



Automated License Plate Readers and the Fourth Amendment

August 2025

Prepared By Katlin Cooper and Michael Lindamood, Legal Research Associates
Division of Legislative Services

Overview

The Fourth Amendment to the United States Constitution protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."¹ This amendment, which "protects individual privacy against certain kinds of governmental intrusion," has gained renewed significance in light of recent technological developments.² One such innovation is the introduction and implementation of automated license plate readers (ALPRs) and their coordinated use by law-enforcement agencies across the country. As ALPR technology becomes more advanced and widespread, it raises a foundational constitutional question: does the collection and utilization of location data by law enforcement constitute an unreasonable search under the Fourth Amendment?

ALPRs are "camera systems that capture the license plate data of passing vehicles, along with related information."³ An algorithm then detects the license plate within the photo or video and reads the numbers.⁴ ALPRs are also able to detect additional information, such as vehicle type and color, global positioning system location data, and date and time.⁵ There are generally two types of ALPRs: fixed or mobile.⁶ Fixed ALPRs are installed in a specific location, oftentimes on infrastructure such as light poles, traffic lights, buildings, or bridges.⁷ Mobile ALPRs, however, are often mounted on police vehicles or privately contracted vehicles.⁸ ALPRs are utilized by law enforcement for a variety of purposes. After capturing and cataloguing license plate data, ALPRs can compare the data against various databases, including hot lists.⁹ Hot lists contain various license plates linked to vehicles of interest.¹⁰ If the ALPR determines that its license plate data matches an entry on the hot list, the ALPR will alert a police officer in real

¹ U.S. Const. Amend. IV.

² *Katz v. United States*, 389 U.S. 347, 350 (1967).

³ Kristin Finklea, *Law Enforcement and Technology: Use of Automated License Plate Readers 1*, Cong. Rsch. Serv., R48160 (2024), <https://www.congress.gov/crs-product/R48160>.

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

⁷ *Id.*

⁸ *Id.*

⁹ *Id.*

¹⁰ *Id.*

time.¹¹ Law enforcement also uses ALPRs to gather intelligence and evidence, help identify potential suspects, and facilitate crime scene analysis.¹²

There is little federal law that directs or prohibits specific tools and technologies that are used by federal law enforcement to aid investigations, including ALPRs.¹³ Additionally, no specific federal legislative framework exists that governs use of ALPRs.¹⁴ However, use of ALPRs is incredibly popular nationwide. Nearly 90 percent of sheriffs' offices with 500 or more sworn deputies use ALPR technology, and 100 percent of police departments that serve over one million people use ALPR technology.¹⁵

Law enforcement's use of ALPR technology has sparked nationwide debate over its constitutionality. Critics are particularly concerned about the privacy ramifications and potential infringement on individuals' Fourth Amendment protections. These debates have increasingly made their way into courtrooms, where judges must determine whether such surveillance practices constitute an unreasonable search.

In Virginia, the use of ALPRs has only recently come under formal regulation through the passage of HB 2724 (Herring, 2025).¹⁶ The bill establishes clear legal parameters around law enforcement's access to and use of ALPR data.¹⁷ However, constitutional questions remain concerning the implementation and use of ALPR data. As a result, federal courts across the country and in Virginia continue to hear cases related to the constitutionality of ALPR technology's use.

To explore that legal question, this brief traces how courts apply the Fourth Amendment standard to ALPR technology. It begins by outlining the legal framework used to determine whether government action constitutes a search and, if so, whether it is unreasonable under the Fourth Amendment. The brief then analyzes how that framework has been applied to ALPR technology in lower courts, specifically how courts have begun to treat ALPR tracking differently depending on its duration, scope, and access policies. Finally, the brief reviews recently enacted ALPR legislation, HB 2724 (Herring, 2025), and considers how existing doctrine may continue to evolve as courts confront unique challenges posed by automated, location-based surveillance.

Fourth Amendment Doctrine and Supreme Court Foundations: Katz v. United States and Carpenter v. United States

Primarily rooted in common law trespass, the Fourth Amendment historically protected against the government obtaining information by physically intruding on a constitutionally protected area.¹⁸ For much of its history, the Fourth Amendment has shaped how courts evaluate alleged violations of personal privacy. In recent decades, the emergence of advanced surveillance

¹¹ *Id.*

¹² *Id.*

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ HB 2724, Reg. Sess. (Va. 2025).

¹⁷ *Id.*

¹⁸ *United States v. Martin*, 753 F. Supp. 3d 454, 461 (E.D. Va. 2024) (*United States v. Jones*, 565 U.S. 400, 405-06 (2012)).



technologies has pushed courts to revisit and refine the scope of those protections. As these technologies continue to evolve, so too does the legal understanding of what constitutes a violation of privacy.

Courts addressing ALPR use must apply the Fourth Amendment's two-step analysis, determining whether the surveillance constitutes a search and, if so, whether such a search is unreasonable.¹⁹ Under current doctrine, a search occurs when there is an invasion of one's reasonable expectation of privacy."²⁰ A search becomes unreasonable when it (i) is executed without a legal search warrant signed by a judge or magistrate, (ii) is executed without probable cause, or (iii) exceeds the authorized scope of a search.²¹

The Supreme Court's landmark decision in 1967 with *Katz v. United States* "articulated a new, complementary two-faceted standard to assess whether a search occurred under the Fourth Amendment."²² To determine whether a search has occurred, courts apply the "*Katz* test," which asks the following questions:

1. Did the person exhibit an actual (subjective) expectation of privacy?²³
2. Is that expectation of privacy one that society is prepared to recognize as "reasonable"?²⁴

Only if there is a subjective expectation of privacy and that expectation is objectively reasonable is there a Fourth Amendment violation of privacy.²⁵ In this way, *Katz* marked a shift from the earlier trespass-based framework to one centered on privacy expectations.

Carpenter v. United States addressed how courts should apply the *Katz* test to modern surveillance technologies.²⁶ In *Carpenter*, the petitioner was charged with six counts of robbery and six counts of carrying a firearm during a federal crime of violence.²⁷ In order to prove its case, the government applied for court orders to obtain the petitioner's cell phone records.²⁸ The government obtained 129 days of cell-site records, which produced 12,898 location points, creating an average of 101 points per day.²⁹ With that data, the government could know the location of Carpenter's cell phone whenever he made or received calls.³⁰ Despite additional nuances to this case, namely the element of third-party doctrine, the Court deemed the government's acquisition of cell-site location information (CSLI) to be a search.³¹

¹⁹ U.S. Const. Amend. IV.

²⁰ *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 344 (4th Cir. 2021).

²¹ *Unreasonable Search and Seizure*, Legal Information Institute (May 2022), https://www.law.cornell.edu/wex/unreasonable_search_and_seizure.

²² *United States v. Martin*, 753 F. Supp. 3d 454, 461 (E.D. Va. 2024) (quoting *Katz v. United States*, 389 U.S. 347 (1967) (Harlan, J., concurring)).

²³ *Id.*

²⁴ *Id.*

²⁵ *Id.*

²⁶ *Carpenter v. United States*, 585 U.S. 296 (2018).

²⁷ *Carpenter*, 585 U.S. at 302.

²⁸ *Id.*

²⁹ *Id.*

³⁰ *Id.* at 306.

³¹ *Id.* at 316.



In deciding that the government engaged in a search, the *Carpenter* Court relied on the dichotomy of short-term tracking of public movements and prolonged tracking that can reveal intimate details through habits and patterns.³² To support its position, the *Carpenter* Court relied on *United States v. Knotts*, in which government officers tracked a suspect using a beeper attached to the suspect's car and traditional visual surveillance methods.³³ Because law enforcement was essentially following an automobile on public streets and highways, the *Knotts* Court deemed there to be no objective expectation of privacy.³⁴ The *Knotts* Court stated:

When [an individual] traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.³⁵

The *Knotts* Court asserted that because the beeper revealed no information that was not otherwise visible to the naked eye, no unconstitutional search had occurred.³⁶

In contrast to *Knotts*, the *Carpenter* Court also relied on *United States v. Jones*.³⁷ In this case, FBI agents installed a GPS tracking device on Jones's vehicle and remotely monitored the vehicle's movements for four weeks.³⁸ Because GPS monitoring tracks a person's every move, the *Jones* Court concluded that long-term GPS tracking likely impinges on a person's expectation of privacy, regardless of whether those movements were disclosed to the public at large.³⁹ As a result, the *Carpenter* Court found *Jones* to be most similar to the petitioner's case.

The *Carpenter* Court also held that, in addition to engaging in a search, the government must generally obtain a warrant supported by probable cause before acquiring records like CSLI.⁴⁰ Warrantless searches are typically unreasonable when a search is undertaken by law enforcement to discover evidence of criminal wrongdoing.⁴¹ Warrantless searches are only reasonable if they fall within a specific exception to the warrant requirement.⁴²

In making its decision, the *Carpenter* Court emphasized the consideration of historical understandings "of what was deemed an unreasonable search and seizure when the Fourth Amendment was adopted" to determine whether one's privacy has been violated.⁴³ The *Carpenter* Court stated that the Fourth Amendment "seeks to secure the privacies of life against

³² *United States v. Martin*, 753 F. Supp. 3d 454, 465 (E.D. Va. 2024) (*Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330 (4th Cir. 2021)).

³³ *United States v. Martin*, 753 F. Supp. 3d 454, 462 (E.D. Va. 2024) (*United States v. Knotts*, 460 U.S. 276, 278-79 (1983)).

³⁴ *United States v. Martin*, 753 F. Supp. 3d 454, 462 (E.D. Va. 2024) (quoting *United States v. Knotts*, 460 U.S. 276, 281-82 (1983)).

³⁵ *Id.*

³⁶ *United States v. Martin*, 753 F. Supp. 3d 454, 462 (E.D. Va. 2024) (*United States v. Knotts*, 460 U.S. 276, 285 (1983)).

³⁷ *Carpenter v. United States*, 585 U.S. 296, 307 (2018) (*United States v. Jones*, 565 U.S. 400 (2012)).

³⁸ *Carpenter v. United States*, 585 U.S. 296, 307 (2018).

³⁹ *Carpenter v. United States*, 585 U.S. 296, 307 (2018) (*United States v. Jones*, 565 U.S. 400, 430 (2012)).

⁴⁰ *Carpenter v. United States*, 585 U.S. 296, 316 (2018).

⁴¹ *Id.*

⁴² *Id.* at 316-17.

⁴³ *Carpenter v. United States*, 585 U.S. 296, 296 (2018) (quoting *Carroll v. United States*, 267 U.S. 132, 149 (1925)).

arbitrary power" and that the framers wanted "to place obstacles in the way of a too permeating police surveillance."⁴⁴ In relation to innovative surveillance tools, such as CSLI, the judicial system is wary of the government's ability to encroach upon areas normally guarded from inquisitive eyes.⁴⁵ Thus, the *Carpenter* Court made its decision, in part, because it wanted to preserve the same historic degree of privacy that existed when the Fourth Amendment was adopted.⁴⁶

Though *Carpenter* involved CSLI data, like CSLI, ALPR data has the potential to be used to reveal detailed patterns of a person's movements over time. As such, *Carpenter's* reasoning offers an analytical pathway by which courts may consider ALPR use as a Fourth Amendment search.

Early Doctrinal Origins of License Plate Checks: United States v. Ellison

United States v. Ellison, a 2006 decision from the Sixth Circuit, offers a limited but instructive perspective on how courts can assess the Fourth Amendment implications of license plate checks.⁴⁷ Though it predates the widespread use of ALPR technology, this case addresses a foundational threshold issue: whether law enforcement's act of running a vehicle's license plate number through a police database before stopping the vehicle or interacting with its occupants can constitute a search under the Fourth Amendment.⁴⁸

In *Ellison*, a police officer observed a van idling in a fire lane near a shopping center.⁴⁹ Without engaging with the driver or issuing a citation, the officer ran the vehicle's license plate through a law-enforcement database and discovered an outstanding warrant for the registered owner.⁵⁰ That information led to the officer pulling over the vehicle and indicting the owner with a charge of being a felon in possession of a firearm.⁵¹ Even though a lower court later found that the vehicle had not been illegally parked, the key question on appeal was whether entering a license plate into a database under these circumstances violated Ellison's right to Fourth Amendment privacy.⁵² The Sixth Circuit approached the issue using the *Katz* test.

The Sixth Circuit ultimately held that motorists do not have a constitutionally protected expectation of privacy in their license plates.⁵³ Relying on *Katz*, the *Ellison* Court reasoned that because license plates are displayed publicly and used for identification, any expectation of privacy is inherently unreasonable.⁵⁴ The *Ellison* Court stated, "The VIN's mandated visibility makes it more similar to the exterior of the car than to the trunk or glove compartment. The

⁴⁴ *Carpenter v. United States*, 585 U.S. 296, 305 (2018) (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886); *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

⁴⁵ *Carpenter v. United States*, 585 U.S. 296, 305 (2018) (*Kyllo v. United States*, 533 U.S. 27, 34 (2001)).

⁴⁶ *Carpenter v. United States*, 585 U.S. 296, 296 (2018) (*Carroll v. United States*, 267 U.S. 132, 149 (1925)).

⁴⁷ *United States v. Ellison*, 462 F.3d 557 (6th Cir. 2006).

⁴⁸ *Id.* at 559.

⁴⁹ *Id.*

⁵⁰ *Id.*

⁵¹ *Id.*

⁵² *Id.* at 561.

⁵³ *Id.*

⁵⁴ *Id.*



exterior of the car is . . . thrust into the public eye, and thus to examine it does not constitute a search."⁵⁵

The Sixth Circuit further emphasized that simply entering a license plate number into a database, without stopping the car or engaging the driver, did not transform the action into a Fourth Amendment search.⁵⁶ Because there was no privacy interest in the license plate information and the information was available to the public, the *Ellison* Court found such action acceptable.⁵⁷ As a result, the *Ellison* Court held that "so long as the officer had a right to be in a position to observe the [individual's] license plate, any such observation and corresponding use of the information on the plate does not violate the Fourth Amendment."⁵⁸

However, this case's reasoning is limited to infrequent tracking, such as a one-time database inquiry based on a visible license plate, not ongoing or systematic surveillance.⁵⁹ The distinction between isolated checks and persistent surveillance becomes especially important in the context of ALPR systems. Unlike the one-time database inquiry in *Ellison*, ALPRs operate continuously and automatically, collecting, storing, and analyzing large volumes of license plate data. Additional case law is needed to determine the qualities or situations that transform the use of public data into a form of surveillance that implicates Fourth Amendment protections.

Federal District Court Applications of Fourth Amendment Principles to ALPR Use: United States v. Martin and Schmidt v. City of Norfolk

United States v. Martin, a 2024 decision from the United States District Court for the Eastern District of Virginia, squarely addresses the central question of whether reviewing stored license plate data from an ALPR system without a warrant constitutes a Fourth Amendment search.⁶⁰ This case presents a modern example of how law enforcement uses ALPR technology not just to identify a single vehicle, but also to link individuals to a series of criminal events across time and geography.

In *Martin*, law-enforcement officers investigating a string of armed robberies across the City of Richmond and Chesterfield County used private security (Flock) footage to identify a suspect's vehicle: an Acura with unique rear-window stickers.⁶¹ An officer then searched Flock's ALPR database, which returned the system's maximum 2,500 images.⁶² After manually reviewing the results, the officer identified two photographs showing the vehicle near one of the robbery locations.⁶³ These images helped police tie the vehicle to the broader investigation and ultimately led to a Global Positioning System (GPS) tracking warrant and the suspect's arrest.⁶⁴

⁵⁵ *Id.*

⁵⁶ *Id.* at 562–63.

⁵⁷ *Id.* at 562.

⁵⁸ *Id.* at 563.

⁵⁹ *United States v. Martin*, 753 F. Supp. 3d 454, 465 (E.D. Va. 2024).

⁶⁰ *Id.*

⁶¹ *Id.* at 457.

⁶² *Id.* at 459.

⁶³ *Id.*

⁶⁴ *Id.* at 460.



The defendant moved to dismiss the charges, arguing that the evidence was gathered in violation of the Fourth Amendment.⁶⁵ Specifically, the defendant claimed that law enforcement's access to previously collected, stored license plate data without a warrant constituted an unconstitutional search.⁶⁶

The *Martin* Court utilized *United States v. Knotts* and *Leaders of a Beautiful Struggle v. Baltimore Police Department*, a case decided by the United States Court of Appeals for the Fourth Circuit in 2020, in its analysis.⁶⁷ The *Martin* Court quoted *Knotts*, stating that "a car has little capacity for escaping public scrutiny" and that "a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."⁶⁸ The *Martin* Court found that there was no reasonable objective expectation of privacy related to ALPR data since the Flock cameras provided no greater information than is otherwise available to the naked eye.⁶⁹ "The cameras merely augment the same inherent sensory faculties of law enforcement that have existed since the Founding."⁷⁰

Unlike *Knotts*, *Leaders of a Beautiful Struggle* involved the Baltimore Police Department employing Aerial Investigation Research (AIR) to conduct a pilot program.⁷¹ The program was six months in duration and was intended to monitor crime in the city.⁷² AIR's planes surveilled city residents during almost all daylight hours, weather permitting, and captured an estimated 12 hours of total coverage of around 90 percent of the city each day.⁷³

Despite AIR's planes only capturing photographs at a resolution of one pixel per person or vehicle, the *Leaders of a Beautiful Struggle* Court found that Baltimore Police Department's warrantless use of AIR's images violated the Fourth Amendment and constituted a search.⁷⁴ As stated in *Carpenter*, "A person does not surrender all Fourth Amendment protection by venturing into the public sphere."⁷⁵ The Fourth Circuit deemed AIR's data to be an "intimate window" into a person's associations and activities.⁷⁶ Even though the aerial photographs were not taken all day, every day, most people tend to do their moving during the daytime, not overnight.⁷⁷ As a result, law enforcement would be easily able to deduce the people behind the pixels by tracking

⁶⁵ *Id.* at 461.

⁶⁶ *Id.*

⁶⁷ *United States v. Martin*, 753 F. Supp. 3d 454 (E.D. Va. 2024) (*United States v. Knotts*, 460 U.S. 276 (1983); *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330 (4th Cir. 2021)).

⁶⁸ *United States v. Martin*, 753 F. Supp. 3d 454, 462 (E.D. Va. 2024) (quoting *United States v. Knotts*, 460 U.S. 276, 281–82 (1983)).

⁶⁹ *United States v. Martin*, 753 F. Supp. 3d 454, 476 (E.D. Va. 2024).

⁷⁰ *Id.*

⁷¹ *United States v. Martin*, 753 F. Supp. 3d 465 (E.D. Va. 2024) (*Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 334 (4th Cir. 2021)).

⁷² *Id.*; *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 333 (4th Cir. 2021).

⁷³ *United States v. Martin*, 753 F. Supp. 3d 465 (E.D. Va. 2024) (*Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 334 (4th Cir. 2021)).

⁷⁴ *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 334, 346 (4th Cir. 2021).

⁷⁵ *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 341 (4th Cir. 2021) (*Carpenter v. United States*, 585 U.S. 296, 310 (2018)).

⁷⁶ *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 342 (4th Cir. 2021).

⁷⁷ *Id.* at 343.



people's habits and patterns.⁷⁸ Such data collection threatens to expose an individual's "familial, political, professional, religious, and sexual associations," which violates an individual's right to privacy under the Fourth Amendment.⁷⁹

Because of the similarities between *Knotts* and *Martin* and the differences between *Martin* and *Leaders of a Beautiful Struggle*, the *Martin* Court rejected the argument that accessing the Flock ALPR database constituted a Fourth Amendment search.⁸⁰ The District Court ruled that the data usage by law enforcement was not unconstitutional largely because the ALPR search did not generate a continuous or detailed chronology of the defendant's location.⁸¹ Thus, it fell short of surveillance that would violate a reasonable expectation of privacy under the Fourth Amendment.⁸²

In *Schmidt v. City of Norfolk*, a case pending in the United States District Court for the Eastern District of Virginia, the complaint challenges the City of Norfolk's use of Flock Safety's ALPR system, which includes at least 172 cameras across Norfolk that are linked to a centralized database.⁸³ According to the plaintiffs, this "web of unblinking eyes" captures detailed vehicle information, such as color, make, model, type of plate, damage or alterations to the car, and whether the vehicle is registered to a resident or non-resident, and stores such data for a minimum of 30 days.⁸⁴ The plaintiffs' complaint alleges that: "(1) [the City of Norfolk's Chief of Police] stated that it would be difficult to drive any distance in the city of Norfolk without running into one of the Flock cameras[;] (2) there are more than 170 Flock cameras around Norfolk [;] (3) there are four cameras directly outside [one plaintiff's] neighborhood and he cannot leave his neighborhood without the [Norfolk Police Department] knowing; (4) [the other plaintiff's] car has been photographed on a near daily basis by the ALPRs; (5) the Flock system creates a searchable database of digital fingerprints of specific cars, and retains that data for 30 days allowing for long term tracking; and (6) the stated purpose of the Flock system is to 'archive evidence' of a vehicle's movements 'for evidence gathering.'"⁸⁵

Additionally, data is pooled with surrounding jurisdictions, creating what police officials described as a "nice curtain of technology" that enables extended surveillance beyond city limits.⁸⁶ The two plaintiffs argue that the ALPR system's operation constitutes pervasive surveillance in violation of their Fourth Amendment rights.⁸⁷

Schmidt has not been decided, but the *Schmidt* Court did deny a motion to dismiss filed by the defendants, finding that there are potentially two valid arguments that deserve their time in court.⁸⁸ The first is following the case law set by *United States v. Martin*, which would stipulate that the use of ALPRs, including use other than by law enforcement, does not violate the Fourth

⁷⁸ *Id.*

⁷⁹ *Id.* at 341 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012)).

⁸⁰ *United States v. Martin*, 753 F. Supp. 3d 454, 468 (E.D. Va. 2024).

⁸¹ *Id.* at 476.

⁸² *Id.*

⁸³ *Schmidt v. City of Norfolk*, 2025 U.S. Dist. LEXIS 21096, at 2 (E.D. Va. Feb. 5, 2025).

⁸⁴ *Id.*

⁸⁵ *Id.* at 15.

⁸⁶ *Id.* at 3.

⁸⁷ *Id.* at 4.

⁸⁸ *Id.* at 18–19.

Amendment. The other argument, which particularly appealed to the Court, is that the use of ALPRs in Norfolk specifically could be violating the plaintiffs' privacy rights under the Fourth Amendment.⁸⁹ The Court stated:

Because the facts as alleged in the complaint suggest that [d]efendants can discern intimate information about the [p]laintiffs, such as where they go, for how long, who they associate with, and because [p]laintiffs point to statements by the Chief of Police stating that it would be difficult to drive any distance in Norfolk without running into one of the Flock cameras, [p]laintiffs have, at least at this early stage, plausibly alleged that their subjective and reasonable objective expectations of privacy have been violated.⁹⁰

As of August 2025, the case is set to go to trial.⁹¹ As the case unfolds, there is a chance that the *Schmidt* Court will expand the case law landscape regarding which circumstances of ALPR usage by law enforcement could violate the Fourth Amendment.

Virginia General Assembly Legislation Background: HB 2724 (Herring, 2025)

HB 2724, a bill patroned by House Majority Leader Charniele Herring, was enacted during the 2025 legislative session and represents Virginia's current legislative approach to regulating ALPR technology.⁹² As introduced, the bill was a recommendation of the Virginia State Crime Commission following their study of HB 775 (Herring, 2024), a prior bill related to the use of ALPRs that failed to pass.⁹³ The legislation touches on several issues, including data retention, reporting, and system approval, but for the purposes of this brief, the most relevant provision is its restriction on when law enforcement may use ALPR data.⁹⁴ Though not framed in constitutional terms, the enacted legislation signals a growing legislative awareness of the privacy implications surrounding ALPR use.

As enacted, the statute limits the use of ALPR systems by law enforcement to specific investigative contexts.⁹⁵ The law provides that "[a] law-enforcement agency may use a system only (i) as part of a criminal investigation into an alleged violation of the Code of Virginia or any ordinance of any county, city, or town where there is a reasonable suspicion that a crime was committed; (ii) as part of an active investigation related to a missing or endangered person, including whether to issue an alert for such person, or a person associated with human trafficking; or (iii) to receive notifications related to a missing or endangered person, a person with an outstanding warrant, or a person associated with human trafficking, a stolen vehicle, or a stolen license plate."⁹⁶ System data is required to be purged "after 21 days of the date of its capture" and audit trail data is required to be purged "after two years of the date of its capture."⁹⁷

⁸⁹ *Id.* at 19.

⁹⁰ *Id.* at 18–19.

⁹¹ *Case: Schmidt v. City of Norfolk*, Civil Rights Litigation Clearinghouse (July 26, 2025), <https://clearinghouse.net/case/46035/>. A settlement conference is scheduled for November 10, 2025, a final pretrial conference is scheduled for January 16, 2026, and a bench trial is scheduled for February 3, 2026.

⁹² HB 2724, Reg. Sess. (Va. 2025).

⁹³ *Id.*

⁹⁴ *Id.*

⁹⁵ Va. Code Ann. § 2.2-5517 (2025).

⁹⁶ *Id.*

⁹⁷ *Id.*



However, if such system data is part of an ongoing investigation, prosecution, or civil action, the statute states that the data "shall be retained by the law-enforcement agency until (i) the investigation concludes without any criminal charges or (ii) the final disposition of any criminal or civil matter related to the data, including any direct appeals and any writs of habeas corpus . . . in accordance with applicable records retention law and policy."⁹⁸ While the statute restricts when law enforcement may query ALPR data, it does not require a search warrant or court order prior to release of such data.⁹⁹ However, as this brief has discussed, courts continue to hear cases¹⁰⁰ related to whether accessing ALPR data, particularly when it is without a warrant and there is a plethora of data over time, amounts to a search under the Fourth Amendment.¹⁰¹

Conclusion

The question of whether the collection and utilization of location data by law enforcement through ALPRs constitutes an unreasonable search under the Fourth Amendment will continue to be debated. While the federal courts' recent Fourth Amendment jurisprudence has demonstrated various factors that are considered when determining whether an unreasonable search has occurred and whether an individual's subjective and objective privacy expectations have been violated, courts are continuing to analyze these factors in various contexts. As demonstrated by *Schmidt v. City of Norfolk*, this area of the law will continue to evolve.¹⁰² Even though there have been several federal cases related to ALPR technology, *Schmidt* demonstrates that how a particular locale uses ALPR technology and how such data is obtained is crucial to determining whether a Fourth Amendment violation has occurred.¹⁰³

Specifically for Virginia, HB 2724, creating § 2.2-5517 of the Code of Virginia, imposes procedural limits on the use of ALPR data but cannot address the constitutional question of whether long-term location tracking via license plate scans constitutes a search.¹⁰⁴ As ALPR technology continues to spread around the country and throughout Virginia, courts and lawmakers will likely continue to face the following question: at what point does access to data revealing a person's movements over time cross the line into constitutionally protected privacy?

For more information, contact the Division of Legislative Services staff:

Taylor Mey, Senior Attorney, DLS
tmey@dls.virginia.gov
804-698-1870

Emma Buck, Legal Section Chief, DLS
ebuck@dls.virginia.gov
804-698-1818

⁹⁸ *Id.*

⁹⁹ *Id.*

¹⁰⁰ See, e.g., *Commonwealth v. Robinson*, 113 Va. Cir. 494 (2024); *Commonwealth v. Adams*, 113 Va. Cir. 505 (2024); *Commonwealth v. Robertson*, 113 Va. Cir. 565 (2024) (resulting in opinions denying the defendant's motion to suppress a warrantless search of ALPR data); *Commonwealth v. Bell*, 113 Va. Cir. 316 (2024) (resulting in an opinion granting the defendant's motion to suppress a warrantless search of ALPR data).

¹⁰¹ *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330 (4th Cir. 2021).

¹⁰² *Schmidt v. City of Norfolk*, 2025 U.S. Dist. LEXIS 21096, at 9 (E.D. Va. Feb. 5, 2025).

¹⁰³ *Id.* at 18–19.

¹⁰⁴ HB 2724, Reg. Sess. (Va. 2025); Va. Code Ann. § 2.2-5517 (2025).

