EYES ON THE ROAD:
Strengthening Fourth Amendment Protections Against Law Enforcement's Accelerating Use of Automated License Plate Readers

Alyssa Archuleta Stolmack

Abstract

Automated License Plate Readers (ALPRs) have become a critical tool to help law enforcement locate stolen cars and cars sought in connection with other crimes. ALPRs capture images of license plates, accompanied by timestamps and location data, to generate real-time alerts and support the investigation of crimes after the fact. Because vehicles are a nearly inevitable fact of American life, the widespread use of ALPR technology raises profound privacy concerns.

Lower courts have begun to address the privacy risks posed by expansive and long-term ALPR surveillance, at times drawing parallels to the cell-site location data in *Carpenter v. United States*. Accordingly, this Comment explores the constitutional implications of warrantless ALPR data collection and use, analyzing the technology's potential to infringe on the rights guaranteed by the Fourth Amendment.

With privacy in mind, this Comment proposes a judicial rule consistent with *Carpenter* that would require a warrant to access ALPR data that is older than six days. This would limit the retention of data about vehicles not tied to criminal investigations while balancing individual privacy interests with law enforcement's needs. As ALPR technology evolves, so too must the legal frameworks governing its use to ensure that privacy rights are not unduly compromised in the name of public safety.

About the Author

J.D., 2025, UCLA School of Law. B.A., 2018, University of Chicago. Thank you to my mom for inspiring and nurturing my interest in criminal justice, my family and friends for their unwavering love and support, and Professor John Villasenor and the wonderful team at the UCLA Criminal

Justice Law Review for their feedback throughout the editorial process.

Table of Contents

Introduction

In a nation where over ninety percent of commuters drive to work, it is unreasonable to argue that operating a vehicle is truly optional for the average American.[1] Like the now-ubiquitous cell phone at issue in *Riley v. California*,[2] vehicles are such a "pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[3] Cars are indisputably required for participation in contemporary society and, whether parked or in motion, can reveal where someone lives, works, or prays.[4]

Just as cars feature prominently in daily life, cars feature prominently in the commission of crime. Law enforcement thus maintains a special interest in monitoring vehicles because it "estimate[s] that over 70 percent of crimes

1. *Why We Ask Questions About Commuting*, U.S. CENSUS BUREAU, [https://perma.cc/ZTQ2–93ZQ].
2. Riley v. California, 573 U.S. 373 (2014) (holding that the Fourth Amendment exception for warrantless searches incident to lawful arrest does not extend to a warrantless search of a cell phone's digital contents).
3. *Id.* at 385.
4. About ninety-two percent of U.S. households had at least one vehicle in 2022. *See* Ashlee Valentine, *Car Ownership Statistics 2024*, FORBES ADVISOR (Mar. 28, 2024, 8:00 AM), [https://perma.cc/ZD6F-MKG9]. Of the 8 to 8.6 percent of American households without a car, most are below the poverty line. *See* Bailey Schulz, *Is It Possible to Live Without a Car? Why Some Americans Are Going Car-Free*, USA TODAY (July 22, 2024, 5:00 AM), [https://perma.cc/XXT7-BFY6].

committed are associated with the use of a vehicle."[5] Consequently, to more efficiently pinpoint and analyze information about cars on the road, police now rely on Automated License Plate Readers (ALPRs) to aid investigations.[6] The Bureau of Justice Statistics' 2020 Law Enforcement Management and Administrative Statistics Survey revealed that "larger law enforcement offices were more likely to use ALPR technology than smaller offices; nearly 90% of sheriffs' offices with 500 or more sworn deputies reported using the technology, and of police departments serving over 1 million residents, 100% used ALPRs."[7] As technology has advanced over the last twenty years, ALPRs have grown more popular and more powerful; modern systems deposit billions of records in AI-powered commercial databases,[8] defying the growing calls for data minimization by privacy advocates and policymakers nationwide.[9]

Law enforcement's reliance upon ALPRs has triggered concern among criminal justice and privacy advocates alike. Because license plates are required to legally operate a vehicle in all fifty states, driving may reveal sensitive information to law enforcement, private entities, and bad actors about a driver's faith, employment, and more.[10] The risks associated with collecting such sensitive information are heightened by the fact that "99.9% of [ALPR] data is unrelated to any public safety interest when it's collected. If accessed by malicious actors, the information may be used to harass, stalk, or even extort innocent people."[11] Indeed, in 2019, hackers accessed over 100,000 license plate images collected at United States Customs and Border Patrol checkpoints, some of which were later found on the dark web.[12]

Hackers do not have a monopoly on the illegal exploitation of ALPR data, however. Illegal use of ALPR data by the state, whether an agency's

5. *Automated License Plate Readers*, Culver City Police Dep't, [https://perma.cc/93DW-EK7R].
6. *See generally* Bryce Clayton Newell, *Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy and Access to Government Information*, 66 Me. L. Rev. 397 (2014). ALPR may also stand for "automated license plate recognition," which refers to the same technology.
7. Kristin Finklea, Law Enforcement and Technology: Use of Automated License Plate Readers, Cong. Rsch. Serv. 1 (Aug. 19, 2024).
8. Dave Maass & Cooper Quintin, *New ALPR Vulnerabilities Prove Mass Surveillance Is a Public Safety Threat*, Elec. Frontier Found. (June 18, 2024), [https://perma.cc/QA46–2X7S] (finding that "just 80 agencies in California," for example, "collected more than *1.6 billion* license plate scans in 2022.").
9. Helena Engfeldt & Elisabeth Dehareng, *Data Minimization: An Increasingly Global Concept*, Int'l Ass'n. Priv. Pros. (May 7, 2024), [https://perma.cc/2EQM-F4NE].
10. *See* Shawn Furman, *Which States Require a Front License Plate in 2024?*, AutoList (June 5, 2024), [https://perma.cc/B4YT-SCR3] ("Every state requires at least one license plate to be mounted and visible on a vehicle," though only 29 states require both front and rear license plates.); *see also Street Level Surveillance: Automated License Plate Readers*, Elec. Frontier Found. (Oct. 1, 2023), [https://perma.cc/83AA-ZC7D].
11. Maass & Quintin, *supra* note 8 (citing data from a 2021 EFF study); *see also* Cal. St. Auditor, *Report 2019–118: Automated License Plate Readers* 1 (2020) ("99.9 percent of the 320 million images Los Angeles stores are for vehicles that were not on a *hot list* when the image was made.") [https://perma.cc/JNH3-UGDR].
12. Maass & Quintin, *supra* note 8.

practice or abuse by a single actor, similarly puts individuals in harm's way.[13] For instance, U.S. Immigration and Customs Enforcement (ICE) obtains driver location data from local police departments to target individuals for deportation despite local privacy laws and sanctuary policies that prohibit such practices.[14] In Kansas, the Kechi Police Department lost its access to its ALPR system after one of its lieutenants was arrested for abusing the system to stalk his ex-wife.[15] While the specific ALPR company at issue in Kechi claimed that the episode marked its "first report of an officer abusing the system," law enforcement departments may enable abuse within their own ranks by failing to proactively ensure that ALPR data is only accessible by authorized individuals for appropriate uses.[16] More recently, a Florida police officer was arrested and charged for stalking an ex-partner by repeatedly querying the department's ALPR database to keep tabs on her location for roughly seven months.[17] When confronted

13. *See* Sadie Gurman & Eric Tucker, *Across US, Police Officers Abuse Confidential Databases*, Assoc. Press (Sept. 27, 2016, 9:28 PM), [https://perma.cc/QZ83–4HUN] ("A Mancos, Colorado, marshal asked co-workers to run license plate checks for every white pickup truck they saw because his girlfriend was seeing a man who drove a white pickup, an investigative report shows. In Florida, a Polk County sheriff's deputy investigating a battery complaint ran driver's license information of a woman he met and then messaged her unsolicited through Facebook . . . . Officers are only occasionally prosecuted, and rarely at the federal level."); *see also* C.J. Ciaramella, *Los Angeles Sheriff Misused Confidential Database Thousands of Times to Run Concealed Carry Background Checks*, Reason (Jan. 29, 2025, 2:41 PM), [https://perma.cc/FFD7-YRDE] (In 2023 alone, California police departments self-reported more than 7,000 misuses of a single database. While not an ALPR-specific database, this revelation highlights the vulnerability of law enforcement databases to abuse).
14. Vasudha Talla, *Documents Reveal ICE Using Driver Location Data from Local Police for Deportations*, ACLU (Mar. 13, 2019), [https://perma.cc/CC2A-R8EA] (describing how ICE obtains ALPR data, including by circumventing its own privacy rules by informally seeking information from friendly local police departments); Dave Maass & Jennifer Pinsof, *VICTORY! California Department of Justice Declares Out-of-State Sharing of License Plate Data Unlawful*, Elec. Frontier Found. (Oct. 31, 2023), [https://perma.cc/YQ9W-HZJK] (discussing a lawsuit against the Marin County Sheriff for "violating SB 34 by sending its ALPR data to federal agencies including ICE and CBP," which settled favorably for the plaintiffs).
15. Shawn Loging & KWCH Staff, *Kechi Police Lieutenant's Arrest Puts Flock Technology Under Scrutiny*, 12 News (Nov. 4, 2022, 3:15 PM), [https://perma.cc/5B5U-WBEL]; Michael Stavola, *Former Kechi PD Supervisor Who Abused Wichita Police Cameras Loses Certification*, Wichita Eagle (Aug. 30, 2023, 1:18 PM), [https://perma.cc/K2JB-DXRD] (The offending officer was convicted of two misdemeanors in connection with his ALPR abuse and lost his officer certification as a result.).
16. Stavola, *supra* note 15; Dave Maass & Hayley Tsukayama, *California Auditor Releases Damning Report About Law Enforcement's Use of Automated License Plate Readers*, Elec. Frontier Found. (Feb. 13, 2020), [https://perma.cc/NAX7-W8TT]; Cal. St. Auditor, *supra* note 11, at iii ("[T]he agencies we reviewed either did not have ALPR policies or their policies were deficient, and they had not implemented sufficient safeguards. For example, none had audited searches of the ALPR images by their staff and thus had no assurance that the searches were appropriate. Furthermore, three of the four agencies have shared their ALPR images widely, without considering whether the entities receiving them have a right to and need for the images.").
17. Anthony Talcott, *'Dumb as Hell': Orange City Officer Accused of Stalking Woman Using License Plate Readers*, Click Orlando (Feb. 5, 2025, 6:00 PM), [http://perma.

by detectives about his abuse of the system, the officer lied and claimed that his victim had been acting suspiciously, perhaps to conceal his improper conduct under the guise of legitimate police work.[18] In sum, "license plate reader databases provide the opportunity for institutionalized abuse by allowing anyone who has access to the information to snoop into an individual's daily activities, habits, or present and past relationships."[19]

Improper use of ALPR data is enabled, in part, by insufficient laws and poor enforcement at the local, state, and federal levels. There are no federal regulations currently governing the use of ALPR technology.[20] Many states, however, already regulate the use of ALPRs and the retention of ALPR data.[21] As of December 2024, eighteen states have passed laws to address the use of ALPRs, and several states are contemplating new or improved ALPR legislation.[22] For example, if passed, a Rhode Island House bill would impose guidelines on the collection, retention, and use of ALPR data, setting a 30-day limit on the retention of data not needed for investigation and prohibiting the sale of ALPR data to third parties.[23] Taking a different approach, a bill in the New Jersey Assembly would impose annual reporting requirements for agencies that use ALPRs and make unauthorized use or access of ALPR data by law enforcement agency employees punishable by imprisonment or fine.[24] In Virginia, where courts have heard both civil and criminal cases involving ALPR technology, the House of Delegates passed legislation that would restrict the storage and use of ALPR data and authorize the state's Department of Transportation to issue permits for certain ALPR installations.[25] A Missouri bill, if passed, would prohibit automated red light cameras and license plate

cc/D79N-D586].

18. *Id.*
19. Samuel D. Hodge Jr., *Big Brother Is Watching: Law Enforcement's Use of Digital Technology in the Twenty-First Century*, 89 U. Cin. L. Rev. 30, 40 (2020).
20. Justin Klawans, *The Pros and Cons of License-Plate Reader Technology*, The Week (Dec. 17, 2023), [https://perma.cc/AJ9L-GLQF].
21. Charlotte Rene Woods, *Virginia Lawmakers Considering Regulating Police Use of Automated License Plate Readers*, Va. Mercury (Nov. 14, 2024, 5:37 PM), [https://perma.cc/JB3F-6FEC] (summarizing existing state-level ALPR laws while addressing efforts in Virginia to pass their own such ALPR regulations).
22. *Automated License Plate Readers: State Statutes*, NCSL (Feb. 3, 2022), [https://perma.cc/FD25-C8HQ*J*; *see also Automated License Plate Readers Widely Used, Subject to Abuse*, U. Mich. Ford Sch. of Pub. Pol'y (Feb. 22, 2023), [https://perma.cc/W7Q6-SXUA] (noting that only sixteen states had ALPR laws on the books as of 2023); *see also* Becky Budds, *SC House Considers License Plate Reader Bill*, News 19 (Mar. 26, 2024, 6:10 PM), [https://perma.cc/27F3-ZZYS] (discussing a bill in the South Carolina House to "restrict ALPR usage to law enforcement agencies only"); *see also* Woods, *supra* note 21.
23. H.B. 7749, 2024 Gen. Assemb., Jan. Sess. (R.I. 2024) (held by committee for further study).
24. A.B. 3297, 221st Leg. (N.J. 2024) (awaiting fiscal analysis by the Office of Legislative Services).
25. Critics of the bill argue that it serves to benefit major ALPR vendors more so than civilian privacy interests. The bill is currently headed to the Virginia Senate. Charlotte Rene Woods, *License Plate Reader Bill Clears the House, but Privacy Concerns Persist*, Va. Mercury (Feb. 4, 2025, 6:12 PM), [https://perma.cc/27KZ-DBDU].

readers alike and limit access to license plate data collected by vehicles traveling over public roads.[26] And, in Oklahoma, lawmakers have begun to study ALPRs in order to draft legislation that prevents "uncontrollable" abuse of the technology.[27]

While some state legislation has helped clarify how law enforcement may use the technology, ALPR regulation still primarily consists of a "bad mix[] of piecemeal ordinances" imposed within each state by municipalities, counties, law enforcement agencies, and ALPR providers themselves.[28] In South Carolina, accessing the "Back Office," the expansive law enforcement database containing ALPR scans, requires only that an officer have a "legitimate law enforcement purpose" or "public safety-related mission," neither of which is defined by the state's ALPR policy or existing legislation.[29] Often, policies governing the storage, use, and transfer of ALPR data conflict even though agencies tend to rely on the same multijurisdictional ALPR databases.[30] Data retention periods are inconsistent as well, so drivers traveling from one city to the next cannot reliably evade the risks associated with long-term storage. For example, a road trip through the three largest cities in California's Bay Area, Oakland, San Jose, and San Francisco, will subject a driver to three different ALPR data retention policies. The City of Oakland, absent cause for suspicion, will retain a driver's plate for just 28 days.[31] But drive across the Bay Bridge to neighboring San Francisco, or head south to San Jose, and that plate will remain in each city's system, available for law enforcement scrutiny and vulnerable to breach, for a full twelve months.[32] California did pass a law

26. Joey Schneider, *Missouri Bill Would Ban Red Light Cameras and License Plate Readers*, Fox 4 KC (Feb. 8, 2025, 2:52 PM), [https://perma.cc/25FA-RSPT] (discussing Senate Bill 540, introduced by State Senator Mike Moon (R-Ash Grove)). The bill provides an exception for law enforcement vehicle-mounted ALPRs. Keith Goble, *Seven States Pursue Rules for License Plate Readers*, Land Line (Feb. 7, 2025), [https://perma.cc/8DUV-RQNU].

27. Oklahoma law currently allows police to use ALPRs *only* to prosecute uninsured drivers. Following *State of Oklahoma v. Ifabiyi*, discussed *infra*, Part IV, lawmakers have expressed concern that police use of ALPR technology that exceeds the narrow scope of the current law will "jeopardize viable criminal prosecutions." Lionel Ramos, *Oklahoma Lawmaker Warns Against AI License Plate Tech Helping Criminals*, KOSU (Oct. 9, 2024, 5:32 AM), [https://perma.cc/3H8F-2F6V].

28. Jonathan Hofer, *The Pitfalls of Law Enforcement License Plate Readers in California and Safeguards to Protect the Public*, Indep. Inst. (Aug. 16, 2022), [https://perma.cc/7BWK-FPSY]; *see also California Automated License Plate Reader Policies*, Elec. Frontier Found. (2019), [https://perma.cc/P8KW-2CZ8] (showing 191 unique ALPR policies among public and private entities within California).

29. William K. Rees, *Survey of South Carolina Law: Enhancing Law Enforcement or Compromising Privacy? The Problem with South Carolina's Use of Automated License Plate Readers*, 75 S.C. L. Rev. 727, 744–46 (2024).

30. Ángel Díaz & Rachel Levinson-Waldman, Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use, Brennan Ctr. For Just. (2020), [https://perma.cc/J55G-7SSZ].

31. Nollyanne Delacruz, *To Curb Crime, Accidents, San Jose Will Expand ALPRs*, Gov. Tech. (Apr. 25, 2024), [https://perma.cc/9QX6-R72Z] (noting that, unlike San Jose, Oakland stores ALPR data for only twenty-eight days).

32. *Id.*; *see also* Surveillance Technology Policy: Automated License Plate Reader, City

in 2011 limiting ALPR data retention to 60 days in the absence of a felony investigation, but the law applies narrowly to retention by a single law enforcement agency: California Highway Patrol.[33] A 2021 state senate bill that would have limited most ALPR data retention to just 24 hours died in committee.[34] At present, the patchwork of local ordinances and state law will not protect our Bay Area driver from prolonged ALPR data retention and its associated risks.

This Comment begins by describing ALPR technology and its uses. Next, the Comment analyzes warrantless use of ALPR data by the police under the Fourth Amendment's rules governing physical trespass, open fields, third-party disclosure, and historical data. The Comment then summarizes the lower court decisions that most directly address the use of ALPR data in criminal cases. Drawing on *Carpenter v. United States*,[35] the Comment concludes by proposing a judicial rule based on data type and retention to balance individual privacy interests with time-sensitive law enforcement needs, speculating as to how the United States Supreme Court would rule on this issue today.

I. What is an ALPR?

ALPRs are "high-speed, computer-controlled camera systems" typically mounted on streetlights, overpasses, utility poles, or police squad cars.[36] ALPRs use optical character recognition to detect and capture any license plate number that comes into view along with the location, date, and time of the image.[37] Some ALPRs also determine the make and model of the vehicle associated with a particular license plate.[38] ALPR systems comprise a growing network of GPS-enabled cameras that funnel vehicle data into massive databases.[39] While private entities like commercial buildings use ALPRs to manage

---

& Cnty. of San Francisco 7, 14 (Dec. 19, 2023) (San Francisco Police Department "defers to the NCRIC retention standard: ALPR records are maintained for 12 months from capture" unless a record "is connected to a criminal investigation or criminal intelligence file," in which case it may be retained for five years.) Note, however, that this report mischaracterizes the Northern California Regional Intelligence Center (NCRIC) retention standard, which "supports a *maximum* retention period of 365 days for ALPR data" but urges that "other factors may supersede this, resulting in a shorter retention period." NCRIC Automated License Plate Reader Policy, N. Cal. Reg. Intel. Ctr 4 (last visited Sept. 3, 2024).

33. Cal. Vehicle Code § 2413 (2011). As its name suggests, the California Highway Patrol's primary patrol jurisdiction is largely limited to the state's highways, as well as roads that run outside of city and county limits. *See, e.g.*, *Understanding the Reach of the California Highway Patrol: What You Need to Know*, Chambers L. Firm, [https://perma.cc/79AG-AY6G]. Thus, the bulk of the ALPRs with which this article is concerned are not subject to the sixty-day retention limit in California because they are operated by individual cities, counties, and private operators. *See California Automated License Plate Reader Policies*, *supra* note 28.
34. *2022 – Senate Bill 210 (Wiener, Scott), Automated License Plate Recognition Systems: Use of Data (Dead)*, Cal. Air Res. Bd., [https://perma.cc/FDR8–9G98].
35. 585 U.S. 296 (2018).
36. *Street Level Surveillance: Automated License Plate Readers*, *supra* note 10.
37. *How ALPR Works*, Senstar, [https://perma.cc/DY2W-TRLM].
38. *Street Level Surveillance: Automated License Plate Readers*, *supra* note 10.
39. Díaz & Levinson-Waldman, *supra* note 30.

parking and control access, for example,[40] this paper focuses on ALPR use by law enforcement for purposes including threat detection and surveillance.[41]

License plate readers (LPRs) have improved dramatically since their adoption by American law enforcement agencies beginning in the early 2000s.[42] Early LPRs, first used in the United Kingdom in the 1970s, lacked the artificial intelligence capabilities of their modern equivalents.[43] Made up of a camera and an external CPU capable of optical character recognition (OCR), these LPRs captured low-resolution images and often struggled to read different license plate styles.[44] Today, ALPRs capture high-definition images and video from which license plate numbers and other attributes can be clearly discerned, including the contents of a bumper sticker and a driver's face.[45] Using artificial intelligence, ALPRs are increasingly used to detect crime, for example, by flagging vehicles that are associated with known trafficking routes.[46] Consequently, this Comment employs the term "ALPR" rather than "LPR" to reflect the technological capabilities of the license plate cameras used today, though in practice the acronyms are often used interchangeably. Modern ALPRs are usually installed in existing traffic cameras and body-worn cameras, reducing the difficulty and cost of implementation.[47] Law enforcement agencies have also installed ALPR technology directly into police car dash cameras and, more creatively, in phony Saguaro cacti.[48]

40. *ALPR Common Use Cases,* Senstar, [https://perma.cc/A8HG-YZ23].
41. The Fourth Amendment applies equally to non-law enforcement state actors. U.S. Const. amend. IV.
42. David Griffith, *12 Things You Need to Know About LPR*, Police Mag., (Apr. 3, 2018), [https://perma.cc/V2BZ-X4U4].
43. Úrsula González, *License Plate Recognition: Past, Present and (a Great) Future*, Quercus Techs. (Feb. 4, 2022), [https://perma.cc/E94A-JWN4].
44. *Id.*; *How ANPR Systems Have Evolved over the Years*, Britannia Parking (Nov. 16, 2023), [https://perma.cc/FA7U-ZEZR] (ANPR refers to "Automatic Number Plate Recognition," terminology used more commonly in the U.K.).
45. William Parker, *The Evolution of ANPR Technology: From Traditional Cameras to AI-Powered Systems*, Medium (Jan. 31, 2024), [https://perma.cc/TS5A-AQAK].
46. *See* Kewei Zhan, *Revolutionizing Law Enforcement: The Role of Artificial Intelligence in License Plate Recognition*, Proc. of 5th Int'l Conf. on Computing & Data Sci. 32, 34 (2023) ("One of the primary applications of ALPR in law enforcement is in the detection and prevention of criminal activity. ALPR cameras can be strategically placed in high-crime areas, at border crossings, or in areas where specific criminal activities are known to occur. This allows law enforcement to monitor the license plates of vehicles passing through these areas and quickly identify those that are associated with criminal activity."); *see also* Motion to Suppress at 4, United States v. Zayas, 2023 U.S. Dist. LEXIS 155355 (S.D.N.Y. Mar. 10, 2023) (No. 00178–01), ("[W]ithout any reason to suspect any individual, and without connection to any particular criminal investigation," officers "searched the RTC's massive location database to identify travel patterns they believed to be 'consistent with interstate narcotics trafficking.").
47. Thomas Brewster, *This AI Watches Millions of Cars Daily And Tells Cops If You're Driving Like A Criminal*, Forbes (July 17, 2023, 6:30 AM), [https://perma.cc/LZ3D-H5FZ]; Kelcey Hook, *AI-Driven ALPR: Accelerating Investigations and Saving Lives*, Rekor (Oct. 19, 2023), [https://perma.cc/KKU4-YBX5].
48. *See, e.g.*, Chelsea Hylton & Denise Whitaker, *Seattle City Council Approves Expansion of License Plate Readers for all Police Vehicles*, Komo News (June 21, 2024, 9:23 AM), [https://perma.cc/GE3V-3N2R] (documenting the addition of ALPR technology

ALPRs collect data in real time and store data for subsequent retrieval.[49] Real-time data helps law enforcement track vehicles of interest that are already placed on a "hot list," perhaps because the vehicle is stolen or associated with a specific crime scene or outstanding warrant.[50] Today, some ALPR systems are configured to automatically alert law enforcement upon detecting a vehicle on a hot list.[51] As the following Part explores, this use of real-time ALPR data likely withstands Fourth Amendment scrutiny due to the existing suspicion associated with these vehicles at the time law enforcement is notified of their whereabouts.

Historical data, on the other hand, is generated over time, stored in a database, and accessed by searching within the database.[52] Historical data may include all detections and locations associated with a particular plate as well as the vehicle's make, model, color, and visible characteristics like significant damage or bumper stickers.[53] Additionally, data collected by an ALPR may reveal the movements of a driver and their passengers or cargo in and out of the car.[54] In 2019, the then-largest private ALPR database in the country contained over 6.5 billion license plate scans and corresponding location data, all accessible to paying law enforcement agencies.[55] The total volume of ALPR data has only exploded since. By 2022, vendor Flock Safety boasted one billion plate scans *per month*.[56] "[R]egardless of whether [someone is] suspected of criminal activity," ALPR databases catalog "expansive and sensitive accounts of [their] movements."[57] Indeed, only 0.05 percent of license plate scans collected by California law enforcement agencies from 2018 to 2019 matched a hot list.[58]

---

to 360 police vehicles); *see also* Weldon B. Johnson, *Paradise Valley Hides License-Plate Reading Cameras in Cactuses*, AZ Central (May 11, 2015, 4:03 PM), [https://perma.cc/NLL3-N86E].

49. *Street Level Surveillance: Automated License Plate Readers*, *supra* note 10.
50. *Id.*
51. Fourth Amendment Ctr., ALPR Primer, Nat'l Ass'n Crim. Def. Laws. 1 (2016).
52. *Id.*
53. *Street Level Surveillance: Automated License Plate Readers*, *supra* note 10. Newer, AI-powered license plate cameras use Optical Character Recognition (OCR) to capture text displayed not only on vehicles, but also in other places like yard signs and t-shirts. This text is then stored in massive, searchable databases that can be accessed by public and private actors alike. One search for Delaware license plates containing the word "Trump" revealed over 150 time-stamped, geolocated images that included homes and bumper stickers, reinforcing that ALPR data may be abused to monitor individuals on the basis of protected speech activity. *See* Matt Burgess & Dhruv Mehrotra, *License Plate Readers Are Creating a US-Wide Database of More Than Just Cars*, Wired (Oct. 3, 2024, 6:30 AM), [https://perma.cc/DC7P-G2TD].
54. *Street Level Surveillance: Automated License Plate Readers*, *supra* note 10.
55. United States v. Yang, 958 F.3d 851, 855 (9th Cir. 2020).
56. Jay Stanley, ACLU, Fast-Growing Company Flock is Building a New AI-Driven Mass-Surveillance System 2 (2022), [https://perma.cc/AH5G-QYVA] (citing to an archived page from Flock Safety's website).
57. Díaz & Levinson-Waldman, *supra* note 30.
58. Maass, *Data Driven 2: California Dragnet–New Data Set Shows Scale of Vehicle Surveillance in the Golden State*, Elec. Frontier Found. (Apr. 22, 2021), [https://perma.cc/4YD5-X6AE].

Law enforcement agencies routinely contract with large vendors that collect and aggregate ALPR scans into multijurisdictional databases, greatly expanding the scope of an individual agency's access to license plate data.[59] One vendor, Rekor, aggregates 150 million plate scans from 30 states into one centralized database each month.[60] Motorola advertises a database containing over 44 billion plate scans that generates 600,000 hot list alerts every day.[61] Flock Safety, which has spent more than seven years deploying tens of thousands of cameras in over 5,000 American cities, markets a "searchable, nationwide database" that is "accessible to police departments across the country."[62] While these databases generally do not contain personal information like a driver's name, law enforcement can cross-reference available databases with the captured images themselves to associate individuals with their license plate numbers.[63]

Police may also gain access to ALPR data volunteered by non-state actors like businesses and homeowners' associations.[64] Thus, while many law enforcement agencies limit their own ALPR installations to capture cars traveling over public roads, they may nevertheless gain access to data collected in private locations, including residences and garages.[65]

Beyond pure data retrieval, ALPR data is also mined and used to perform analytics that identify trends in a vehicle's whereabouts, behavior, and associations with other vehicles.[66] Over the past few years, artificial intelligence has deepened the impact of ALPR data by enabling predictive analytics that anticipate the routes and locations of specific vehicles based on past trends in their behavior.[67]

ALPR technology has evolved significantly since its early days and continues to improve as increasing law enforcement demand drives investment in performance upgrades.[68] For instance, some of the newest ALPRs advertise

59. *See* Bryan Polcyn, *Mapping Flock Cameras, Police 'Secrecy' Varies by Department*, Fox6 Milwaukee (Oct. 24, 2023, 10:09 PM), [https://perma.cc/4BE8-ASX5]; Díaz & Levinson-Waldman, *supra* note 30.

60. Brewster, *supra* note 47.

61. *License Plate Recognition*, Motorola Sols., [https://perma.cc/T8FF-QHJK].

62. Flock Safety, *Flock Safety Announces Partnership With MS2 to Bring AI Traffic Analytics to State Transportation Agencies* Yahoo! Fin., (Jan. 6, 2025), [https://perma.cc/FFK8-PATX] ("Flock Safety's leading camera network [is] present in over 5,000 communities across 49 states"); Polcyn, *supra* note 59.

63. *Id.*

64. *Id.*; *see also* Brewster, *supra* note 47 (discussing the use of ALPR technology by McDonalds and White Castle to improve the drive-through experience).

65. *See, e.g.*, Cal. ALPR FAQs, N. Cal. Reg'l Intel. Ctr. 3, [https://perma.cc/L9D5-LB8F].

66. Nicole K. McConlogue, *Discrimination on Wheels: How Big Data Uses License Plate Surveillance to Put the Brakes on Disadvantaged Drivers*, 18 Stan. J. C.R. & C.L. 279, 282, 303 (2022) (examining the use of ALPR data-driven analytics by insurers, among others, to algorithmically set rates).

67. Díaz & Levinson-Waldman, *supra* note 30. For hypothetical scenarios about ALPR data mining and analysis, *see* ACLU, You Are Being Tracked: How License Plate Readers are Being Used to Record Americans' Movements 30 (2013) (explaining how data mining techniques cannot reliably distinguish between innocuous and suspicious reasons for certain driving habits).

68. *See* Haje Jan Kamps, *Flock Safety's Solar-Powered Cameras Could Make Surveillance*

the ability to scan the license plates of cars driving 140 miles per hour.[69] These improvements have not rendered the technology failproof, however. In early 2025, researcher Matt Brown discovered that more than 170 ALPRs produced by Motorola Solutions streamed drivers' sensitive vehicle data onto the open Internet rather than their intended private servers, which Motorola attributed to a "potential technical issue."[70] Using a search engine, Brown "accessed live color and infrared video and captured data including the license plate number, make, model, and a photo of every vehicle he viewed."[71] As law enforcement adoption of ALPRs accelerates, simultaneously exposing the technology's pitfalls, so too must awareness of the true costs and benefits associated with widespread vehicle surveillance.

II. The Effects of ALPR Technology on American Policing

At present, there exists a fierce debate between ALPR advocates and civil rights organizations about the appropriate role of license plate scanners in modern policing. ALPRs are now incredibly common among American law enforcement agencies,[72] meaning that inaccuracy and other errors associated with the technology threaten grave consequences for individuals sought by police. At the same time, proponents of the technology believe that it increases public safety and enables more efficient policing.[73] One vendor, Flock Safety, advertised in 2024 that ten percent of all reported crime in the United States is solved using Flock devices,[74] though researchers have challenged the valid-

More Widespread, TechCrunch (May 16, 2024, 7:29 AM), [https://perma.cc/2TQC-6RF6] ("Flock Safety is an extraordinarily well-funded startup. PitchBook reports that the company has raised more than $680 million to date, at a valuation of close to $5 billion.").

69. Nicole Stoffman, *New Police Tech can Read Plates of Cars Going 140 mph*, Timmins Daily Press (Nov. 8, 2024), [https://perma.cc/55UG-RZWF].

70. Shawn Mulcahy, *On Display*, Chi. Reader (Jan. 8, 2025), [https://perma.cc/VY9B-FCLA].

71. *Id.*

72. Finklea, *supra* note 7, at 1 (As of mid-2024, "nearly 90% of sheriffs' offices with 500 or more sworn deputies reported using the technology, and of police departments serving over 1 million residents, 100% used ALPRs.") (internal citation omitted); Robert Spinks, *What You Need to Know About Automatic License Plate Readers*, Am. Police Beat (Oct. 20, 2023, 6:00 AM), [https://perma.cc/627L-S3YG] (As of 2023, "[i]n cities with populations of 100,000 or more, 75% of police departments use[d] ALPR systems . . . .").

73. *See, e.g.*, Bruce Taylor, Christopher Koper, & Daniel Woods, Police Executive Research Forum, Combating Auto Theft in Arizona: A Randomized Experiment with License Plate Recognition Technology vi (2011) ("Experimental results showed that LPR use considerably enhanced the productivity of the auto theft unit in checking license plates, detecting stolen vehicles and plates, apprehending auto thieves, and recovering stolen vehicles. Combining results across both phases, the use of LPRs resulted in 8 to 10 times more plates checked, nearly 3 times as many 'hits' for stolen vehicles, and twice as many vehicle recoveries.").

74. Flock Safety, How Many Crimes Do Automated License Plate Readers (ALPRs) Solve, Anyway? (Feb. 8, 2024), [https://perma.cc/T3S4-HWER] ("[O]ver 700,000 crimes each year are solved using Flock Safety technology. This represents roughly

ity of Flock's research methodology and findings.[75] Anecdotally, the benefits of ALPR use are impressive, helping police departments large and small to capture individuals wanted for sexual assault,[76] murder,[77] insurrection,[78] kidnapping,[79] terroristic threats,[80] mass shooting,[81] attempted assassination,[82] and more. The technology is also used by some cities to assist with more mundane

10% of reported crime nationwide.").

75. One of two academic researchers who cosigned the study later said that the police department-generated data used to complete this study "are too varied and incomplete for us to do any type of meaningful statistical analysis," calling into question the legitimacy of the claim that Flock technology is used to solve ten percent of all reported crime in the United States. The study was not subject to peer-review, either. Jason Koebler, *Let's Talk About the Flock Study That Says It Solves Crime*, 404 Media (Mar. 20, 2024, 11:03 AM), [https://perma.cc/6J6B-NZ85].
76. Rhea Caoile, *Suspect Arrested After Sexual Assault of Teen Girl in North County*, Fox 5 San Diego (Nov. 8, 2024, 4:16 PM), [https://perma.cc/CFF5-FF57] ("Detectives from the SDSO sexual assault unit were able to identify the suspect and his vehicle using automated license plate reader (ALPR) technology.").
77. Tim Pulliam, *Beverly Hills License Plate Reader Used in Capture of Murder Suspect Draws Mixed Reviews*, ABC 7 (Dec. 4, 2023), [https://perma.cc/238S-EDGL] (Police credited ALPR technology with identifying an individual accused of murdering three homeless men in Beverly Hills, California.); Erin Mathews, *Maine Man Bound Over for Trial in Connection with Tescott Man's Murder*, Salina J. (Jan. 29, 2018, 8:30 PM), [https://perma.cc/8EXX-QNXZ] (ALPR technology helped police to track down a Maine resident wanted for murder in Kansas).
78. Jenni Fink, *FBI Traced NYC Sanitation Worker to Capitol Riot with License Plate Readers*, Newsweek (Jan. 22, 2021, 1:09 PM), [https://perma.cc/7URS-4C5S].
79. Danielle Smith, *Mission Valley Mall Kidnapping Arrestee Also Charged in Second Kidnapping*, ABC 7 San Diego (June 21, 2024, 4:31 PM), [https://perma.cc/FF6W-GTVU]; Erika Esquivel, *NMSP Finds 5 Kidnapped Children from Texas Using License Plate Reader*, KFOX 14 (Nov. 19, 2024, 6:01 PM), [https://perma.cc/PVL8–2L7N] ("New Mexico State Police successfully located and rescued five kidnapped children from Texas after an automatic license plate reader identified the vehicle they were traveling in.").
80. ALPRs helped police to intercept Kurt James Cofano with "30 improvised bombs in his vehicle along with numerous weapons, homemade detonators and chemicals used in making explosives" after he was observed on social media threatening to "blow up" the Treasury Department and CIA headquarters. *Mt. Lebanon, PA Police Used ALPR Technology to Proactively Locate Terrorist and His Vehicle Containing Multiple Weapons and 30 Bombs in Real Time Just Prior to Intended Attacks*, Police1 (July 21, 2020, 3:00 PM), [https://perma.cc/FLQ7–9976].
81. Joe Fisher, *Raleigh Police Chief, Nash County Sheriff Advocate for License-Plate Readers After They Helped Catch Suspected Atlanta Mass Shooter*, WRAL News (May 4, 2023, 3:11 PM), [https://perma.cc/M2PT-GVH9].
82. *See* Shaila Dewan, *Technology That Helped Catch Trump Suspect is Proliferating*, N.Y. Times (Sept. 17, 2024), [https://perma.cc/7CJV-7R86] (explaining how an ALPR hot list alert helped police to apprehend the suspect in a September 2024 assassination attempt on Donald Trump in West Palm Beach, Florida).

tasks like parking enforcement,[83] distracted driving,[84] and noise pollution.[85] Given these claims, local governments may face pressure from constituents and law enforcement agencies alike for declining to adopt the technology.[86]

While ALPRs are easily understood to help investigate crimes that have already occurred, their role in deterring crime is less clear. Some law enforcement agencies, such as Illinois State Police, credit ALPRs with preventing crime like Chicago-area expressway shootings, which decreased dramatically following the installation of cameras on every expressway in Cook County.[87] Critics, on the other hand, assert that "[c]orrelation does not equal causation" because the statistics do not show that the cameras effectively reduced the number of these particular shootings.[88]

While law enforcement agencies assert that ALPR technology greatly improves policing ability, privacy advocates warn that the risks associated with the use of the technology outweigh the benefits, even when the technology is used properly. For instance, in 2015, a security lapse compromised the entire ALPR system covering Boston, Massachusetts, exposing years of records to the public.[89] As recently as 2019, ALPR scans were accurate only ninety percent of the time.[90] With ALPRs registering billions of scans each year, these

83. *See* Marian Davidson, *You Asked: License Plate Readers*, KTVH (Jan. 17, 2025), [https://perma.cc/A697-A6WH] (While "[l]icense plate readers are largely banned in Montana," the law has exceptions including one that permits incorporated cities to use ALPRs "in a regulated parking system, but only to identify a vehicle's location and license plate number to enforce parking restrictions.") (citation omitted).

84. Laura Neitzel, *Outside-the-Box Uses for ALPR*, Police1 (Jan. 29, 2025, 3:04 PM), [https://perma.cc/3GU6–7MNH] ("Jenoptik's ALPR technology uses advanced cameras, infrared (IR) lighting (which is not distracting for the driver) and machine learning to produce clear photographic evidence of distracted driving behaviors. 'The technology can see through the windshield and detect if someone is holding their cellphone or if their attention is taken away from the operation of the motor vehicle.'").

85. *Id.* (explaining that Jenoptik ALPRs now feature noise detection capabilities that can automatically alert law enforcement "[w]hen a predefined noise threshold is exceeded or an abnormal sound is detected").

86. *See, e.g.*, Kendall Ashman, *Wilson County Sheriff Calls Out Metro for Not Having LPRs; 'Fusus' Deferred During Metro Council Meeting*, WKRN (Feb. 5, 2025, 6:11 PM), [https://perma.cc/G6ER-4YYD] (highlighting tensions between Nashville, Tennessee and law enforcement from surrounding jurisdictions over Nashville's failure to install ALPR technology to date).

87. Robert McCoppin, *License Plate Cameras Help Solve Crimes, But Are Creating a Backlash Over Privacy Concerns*, Chicago Trib. (June 17, 2024, 5:00 PM), [https://perma.cc/ELN8–6RUH].

88. *Id.* (internal quotations omitted) (quoting an attorney who filed suit to challenge Illinois's installation of more than 300 ALPRs statewide).

89. Kearston Wesner & Katie Blevins, *Restraining the Surveillance Society: Comparing Privacy Policies for Automated License Plate Readers in the United States and the United Kingdom*, 18 Ohio St. Tech. L. J. 99, 105 (2021) (citing Kenneth Lipp, *License to Connive: Boston Still Tracks Vehicles, Lies About It, and Leaves Sensitive Resident Data Exposed Online*, DigBoston (Sept. 8, 2015), [https://perma.cc/PM3M-QNZ9]).

90. Lisa Fernandez, *Privacy Advocate Sues CoCo Sheriff's Deputies After License Plate Readers Target His Car Stolen*, KTVU Fox 2 (Feb. 19, 2019, 11:12 AM), [https://perma.cc/2SCD-X4LL].

errors accumulate and undermine the overall integrity of the databases relied upon by law enforcement, though the downstream effects of these errors may evade Fourth Amendment scrutiny under the good faith exception to the exclusionary rule.[91]

As AI and other technological developments improve ALPR accuracy, there still remains the possibility of human error when officers and staff enter and retrieve license plate numbers.[92] Even when the license plate retrieval system works as intended, officers may nevertheless disregard on-screen guidance about how to act on data about a particular license plate, giving rise to legally dubious traffic stops and automobile searches.[93] These factors can result in severe consequences if license plate numbers and vehicle attributes are not properly confirmed and on-screen warnings are not properly heeded before law enforcement acts. Take, for instance, Robbie Tolan, who was shot by police in his own yard after an officer entered the wrong plate number into his system, as officers often do to review a vehicle's ALPR data history, resulting in the belief that Tolan's vehicle was stolen.[94] Denise Green of San Francisco narrowly avoided the same fate when officers pulled her from her car with guns drawn after failing to perform "the most basic, visual check" to realize that the stolen car sought was a gray GMC truck and not Green's burgundy Lexus.[95] Finally, consider Zach Norris, former director of the Ella Baker Center for Human Rights, who was detained at gunpoint after an individual stole his license plate and replaced it with one used in an armed robbery.[96]

In Norris's and Green's cases, the ALPRs worked properly by alerting officers to the presence of wanted license plates. However, the aggressive and/or careless behavior of the officers acting on the plate information presented by the ALPR system resulted in avoidable, life-threatening

91. *See* Herring v. United States, 555 U.S. 135 (2009) (holding no Fourth Amendment violation occurs when introducing evidence seized by police during the execution of a defunct arrest warrant negligently allowed to remain active in their database).

92. *See* Arizona v. Evans, 514 U.S. 1 (1995) (permitting evidence seized by police during the execution of an arrest warrant that had been quashed but remained on the defendant's record due to a judicial staffer's clerical error).

93. In one case, a New York State Trooper conducted a traffic stop of the defendant based only on a license plate check that returned the following instruction: "THE FOLLOWING HAS BEEN REPORTED AS AN IMPOUNDED VEHICLE——IT SHOULD NOT BE TREATED AS A STOLEN VEHICLE HIT——NO FURTHER ACTION SHOULD BE TAKEN BASED SOLELY UPON THIS IMPOUNDED RESPONSE." The officer disregarded the instruction and proceeded with the traffic stop, ultimately recovering marijuana and a loaded gun. Indeed, the car had been impounded, but the defendant had timely paid to have it released. The system had not yet been updated to reflect the payment. Because the state trooper lacked both reasonable suspicion that a crime had occurred and probable cause that a traffic violation had occurred, the court held that the stop was unlawful. People v. Hinshaw, 156 N.E.3d 812, 813 (N.Y. 2020).

94. Yamiche Alcindor, *Supreme Court Reignites Robbie Tolan Police Shooting Case*, USA Today (May 24, 2014, 7:00 AM), [https://perma.cc/HUL3-XE59].

95. Kade Crockford, *San Francisco Woman Pulled Out of Car at Gunpoint Because of License Plate Reader Error*, ACLU (May 13, 2014), [https://perma.cc/84G7-NF4M].

96. Zach Norris, *At Gunpoint, Police Handcuffed Me After License-Plate Reader Error*, Mercury News (June 23, 2021, 5:00 AM), [https://perma.cc/6WN2-CC7X].

situations for individuals not connected to any crime.[97] These errors are costly to taxpayers and dangerous for civilians caught in the crosshairs.[98]

In addition to the high-level implications of mass surveillance for free society, the consequences of faulty ALPR data and human error at the individual level solidify the need for proper regulation through a combination of legislation, judicial remedies, and enforcement, especially as it becomes clear that ALPR technology is here to stay across American police departments.[99]

III. Fourth Amendment Frameworks

The Fourth Amendment safeguards the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[100] This language was designed to strike a balance between the government's interest in law enforcement and the individual's right to privacy and autonomy.[101] The framers of the United States Constitution included the Fourth Amendment, in part, as a rejection of pre-Revolution general warrants and writs of assistance, which British authorities used to search homes, businesses, and personal effects without specificity as to "person, crime, or place to be searched."[102] These instruments were despised by the colonists for their broad and invasive nature, empowering officials to search indiscriminately for as long as the King who issued them lived.[103] Modern surveillance tac-

97. In a similar episode in the United Kingdom, police shot and killed Chris Kaba after an ALPR system alerted police that the vehicle he was operating was linked to a firearms incident, leading officers to act as though he was armed and dangerous. Police "rammed and blocked Kaba's car" before killing Kaba with a single shot. The car was not registered to Kaba. Griff Ferris, *Automated Policing Helped Kill Chris Kaba*, Novara Media (Sept. 14, 2022), [https://perma.cc/2NVR-MLZB].

98. *See* Adam Schwartz, *The Human Toll of ALPR Errors*, Elec. Frontier Found. (Nov. 1, 2024), [https://perma.cc/F4EB-ZZZ8] (accounting for at least $2.5 million in settlements paid out to victims wrongfully detained as a result of ALPR data and alerts).

99. "At the Federal level, regulation of ALPRs is nonexistent, and only [eighteen] states have enacted some form of regulation. As most jurisdictions have zero laws regarding ALPRs, law enforcement and private actors can use the technology however they wish." *Automated License Plate Readers Widely Used, Subject to Abuse*, *supra* note 22. (revising the number of states with ALPR regulations to reflect current totals). However, several private parking companies, including ABM, have been sued for violating the 1994 Driver's Privacy Protection Act (DPPA) by using ALPRs to track down drivers' contact information without their consent. Kelly Mehorter, *ABM, FlashParking, Parkpliant Hit with Class Action Over Alleged Parking Fee 'Scheme'*, ClassAction.org (Jan. 18, 2024), [https://perma.cc/D66S-LVCY]. But the DPPA was not enacted with modern surveillance technology in mind, is "full of loopholes," and "may not be sufficient to protect customers' privacy." Hannah Harris Green, *Parking Lot Companies May Be Violating Privacy Laws to Fine Drivers. It's Only the Beginning.*, Slate (Sept. 24, 2024, 11:30 AM), [https://perma.cc/3KR4-MJAV].

100. U.S. Const. amend. IV.

101. *What Does the Fourth Amendment Mean?*, U.S. Cts., [https://perma.cc/DZ62-T9GX].

102. Laura K. Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181, 1190, 1192 (2016).

103. David Snyder, *The NSA's "General Warrants": How the Founding Fathers Fought an 18th Century Version of the President's Illegal Domestic Spying*, Elec. Frontier

tics, particularly those which involve digital data, have drawn comparisons to general warrants because they allow police to "rummage indiscriminately through our private data for any cause (or no cause at all) and without judicial oversight."[104] The growth of tech-driven policing will increasingly "have an inverse and inimical relationship with individual privacy from government intrusion, presenting serious concerns for Fourth Amendment protections."[105] The use of ALPRs by law enforcement to aid investigations represents one such surveillance technology that is often at odds with the constitutional rights against unreasonable searches and seizures.[106]

This Part explores current Fourth Amendment jurisprudence and its relevance to the admissibility of ALPR evidence in court. It first examines the applicability of the *Jones* physical trespass test before analyzing ALPR data under the open fields and third-party doctrines that are embedded in the *Katz* reasonable expectation of privacy test. This Part ultimately concludes that the Supreme Court's reasoning in *Carpenter v. United States* provides the strongest basis for limiting the admissibility of ALPR data as evidence in criminal cases.

A. *Physical Trespass & GPS Surveillance*

In *United States v. Jones*,[107] the Supreme Court ruled unanimously that police violated the Fourth Amendment under a physical trespass theory. Before obtaining a warrant, police manually attached a GPS tracker to a suspect's vehicle while it was parked on private property to monitor the suspect's location for a month as part of a narcotics trafficking investigation.[108] The suspect was ultimately convicted on a conspiracy charge, but a panel of the U.S. Court of Appeals for the D.C. Circuit overturned the conviction on Fourth Amendment grounds based on the admission of evidence obtained through the warrantless use of the GPS tracker.[109] In its case before the Supreme Court, the government argued that the defendant had no reasonable expectation of privacy in his movements over public roads, however, the Court rejected this argument due to the Fourth Amendment's historical emphasis upon strong property rights.[110] The Court ultimately held that the means through which police installed the

FOUND. (2007) (citing Nelson B. Lasson, *The History and Development of the Fourth Amendment to the United States Constitution*, 54 (1937)), [https://perma.cc/PU6D-QS8M].

104. *The Warrant Clause in the Digital Age*, ACLU (May 3, 2023), [https://perma.cc/WM8F-Q2PF].

105. United States v. Tuggle, 4 F.4th 505, 528 (7th Cir. 2021) (upholding the constitutionality of warrantless surveillance of the exterior of the defendant's home using three stationary pole cameras that operated 24/7 for eighteen months but cautioning that more expansive surveillance technology may demand a different outcome).

106. U.S. CONST. amend. IV.

107. 565 U.S. 400, 405 (2012).

108. *Id.* at 402–03.

109. *Id.* at 404.

110. *Id.* at 405–06 ("The text of the Fourth Amendment reflects its close connection to property [. . .] Consistent with this understanding, our Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century" when *Katz v. United States* introduced the "reasonable expectation of privacy" test.).

GPS tracker, rather than the prolonged period of surveillance that followed, created the Fourth Amendment violation.[111] Because ALPRs function by scanning license plates, conventional use of the technology is unlikely to violate the Fourth Amendment under a physical trespass theory because, unlike in *Jones*, police are not manually attaching a device to a suspect's vehicle.[112]

The Court in *Jones* relied on physical trespass to find that the attachment of a GPS tracker to a suspect's car violated the Fourth Amendment.[113] At the same time, a plurality also expressed concern about the ability of virtual and long-term GPS tracking to jeopardize important privacy interests.[114] While no physical trespass can be said to occur when a license plate is scanned by a camera from afar, the justices warned that long-term GPS surveillance, enabled by modern technology, may nevertheless infringe upon one's reasonable expectation of privacy.[115] In her concurrence, for example, Justice Sotomayor warned that the trespass doctrine would soon grow obsolete as physical intrusion became less essential for police surveillance.[116] And, in his concurrence, Justice Alito cautioned that "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[117] Thus, while the *Jones* physical trespass theory may not directly render the use of ALPR technology unconstitutional under the Fourth Amendment, the case offers insight into the Court's likely approach to a case involving extensive ALPR surveillance, as opposed to individual, isolated cameras.[118] Only when an ALPR network becomes pervasive enough to

111. *Id.* at 412 ("Thus, even assuming that the concurrence is correct to say that '[t]raditional surveillance' of Jones for a 4-week period 'would have required a large team of agents, multiple vehicles, and perhaps aerial assistance,' our cases suggest that such visual observation is constitutionally permissible. It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question." (internal citations omitted)).
112. Property-based Fourth Amendment arguments against the use of ALPRs are further weakened by the fact that license plates may technically be considered state property. *See* Isabella Vanderheiden, *Eureka City Council Tables Decision on Police Surveillance Cameras, Citing Privacy Concerns*, Lost Coast Outpost (Oct. 2, 2024, 5:27 PM), [https://perma.cc/YB5G-4N52].
113. 565 U.S. 400 (2012).
114. *Id.*
115. *Id.* at 430 (Alito, J., concurring) ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. . . . We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.").
116. *Id.* at 414–15 (Sotomayor, J., concurring) ("[P]hysical intrusion is now unnecessary to many forms of surveillance. . . . In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance.").
117. *Id.* at 430 (Alito, J., concurring) (ostensibly referring to the reasonable expectation of privacy required by the two-part test articulated in *Katz*, discussed below).
118. The court in *Virginia v. Bell* addresses this concern in its June 2024 order on a motion to suppress ALPR evidence, discussed *infra*, Part IV.

thoroughly catalog an individual's movements does it become analogous to the plurality's concerns in *Jones*.

Ultimately, the *Jones* trespass test provides an incomplete framework for analyzing police use of ALPRs. While it is effective for addressing cases involving physical intrusion, it fails to fully capture the privacy concerns posed by modern surveillance technologies that operate without physical trespass. For this reason, courts have increasingly turned to privacy-based analyses under the "reasonable expectation of privacy" test articulated in *Katz v. United States*.

B. *Reasonable Expectation of Privacy Under Katz*

Justice Harlan's concurrence in *Katz v. United States* established a two-pronged test that requires both subjective and reasonable expectations of privacy for a search to violate the Fourth Amendment.[119] Departing from the traditional physical trespass test explored in *Jones*, the Court clarified that the Fourth Amendment protects people, not just their property.[120]

In *Katz*, federal agents placed a recording device on the exterior of a public phone booth to eavesdrop on defendant Charles Katz, who was suspected of illegal gambling activity.[121] The agents did not have a warrant, and Katz was convicted based on the contents of his recorded conversations.[122] On appeal, Katz challenged the admissibility of this evidence, contending that law enforcement violated his Fourth Amendment rights by recording his conversations without a warrant.[123] Nevertheless, the Court of Appeals rejected Katz's argument because "[t]here was no physical entrance into the area occupied by [Katz]."[124] Taking up the issue, the Supreme Court held that the government "violated the privacy upon which [Katz] reasonably relied while using the telephone booth, and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[125]

Katz's legacy derives from Justice Harlan's concurring opinion, which articulated the two-pronged "reasonable expectation of privacy test."[126] To have a "constitutionally protected reasonable expectation of privacy" such that intrusion may constitute a Fourth Amendment violation, the person must first have exhibited "an actual (subjective) expectation of privacy," such as by using a phone booth to speak or by encrypting communications.[127] Once an individual has established a subjective expectation of privacy, they must next demonstrate that the expectation was one that "society is prepared to recognize as 'reasonable'" in light of prevailing norms.[128] Under this test, Harlan

119. Katz v. United States, 389 U.S. 347, 361 (1967).
120. *Id.* at 351 ("[T]he Fourth Amendment protects people, not places.").
121. *Id.* at 354.
122. *Id.* at 348, 356–57.
123. *Id.* at 348.
124. *Katz*, 389 U.S. at 349 (internal quotations omitted).
125. *Id.* at 353.
126. *Id.* at 360 (Harlan, J., concurring).
127. *Id.* 360 –61
128. *Id.* at 360.

suggested, one could reasonably expect that their home would remain private, whereas conversations made in public could not reasonably be expected to remain private.[129]

The following analysis considers how the use of ALPR technology may violate an individual's reasonable expectation of privacy under *Katz* and its progeny, which established the open fields and third-party doctrines.

1. Traveling Over Public Roads in Plain View

In his *Katz* concurrence, Justice Harlan stipulated that individuals do not have a reasonable expectation of privacy over what they expose in plain view, including when traveling over a public road.[130] The Court illustrated this principle in *Knotts*, holding that police did not conduct a search in violation of the Fourth Amendment by warrantlessly tracking a suspect's vehicle.[131] Without obtaining a warrant, police first placed a radio beeper inside a barrel of chloroform to track its location as it exchanged hands in connection with suspected illegal activity.[132] Using the beeper, police followed a car containing the chloroform to the defendant at a rural cabin, which the police used to obtain a search warrant that ultimately led to his conviction for conspiring to manufacture controlled substances.[133] On appeal, the Eighth Circuit overturned the conviction, finding that the use of the beeper violated the Fourth Amendment by infringing upon the defendant's reasonable expectation of privacy.[134] The Supreme Court reversed, reasoning that the device merely enhanced what was otherwise observable to the naked eye because it monitored the vehicle only while it traveled over public roads.[135] Because a police car could have reached the same conclusions about the car's whereabouts by following the driver, law enforcement's use of the beeper did not constitute an illegal search within the meaning of the Fourth Amendment.[136]

---

129. Katz v. United States, 389 U.S. 347, 360 (1967).
130. *Id.* at 361. ("[O]bjects, activities, or statements that [one] exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited."). In subsequent case *Oliver v. United States*, the Court concluded that government surveillance conducted from an open field is not an unreasonable search prohibited under the Fourth Amendment. 466 U.S. 170, 177 (1984) (affirming Hester v. United States, 265 U.S. 57 (1924) (holding that Fourth Amendment protections do not extend to open fields).
131. United States v. Knotts, 460 U.S. 276 (1983). Note that Justice Stevens issued a concurring opinion challenging the majority's application of the "open fields" doctrine to the facts of this case. *Id.* at 288. ("[T]he Court implies that the chloroform drum was parading in 'open fields' outside of the cabin, in a manner tantamount to its public display on the highways. The record does not support that implication.") (internal citations omitted). Justice Stevens's concern would ostensibly not apply to detection of a license plate fixed in plain sight on the exterior of a vehicle.
132. *Id.* at 277.
133. *Id.* at 278–79.
134. *Id.* at 279.
135. *Id.* at 282 ("Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.").
136. United States v. Knotts, 460 U.S. 276, 285 (1983).

Considering a literal reading of the open fields doctrine, then, the use of ALPRs to monitor a vehicle on public roads would not violate the Fourth Amendment. The exterior of a car "is thrust into the public eye, and thus to examine it does not constitute a 'search'."[137] Additionally, cameras are not generally thought to exceed the scope of what is ordinarily detectable with the naked eye.[138] However, "AI has the potential to facilitate the recognition of license plates even under challenging conditions. AI-powered license plate recognition systems can quickly and accurately read license plates from a distance, regardless of the lighting or weather conditions that are hard for human eyes to read," suggesting that ALPRs may in some cases amount to sense enhancement, as contemplated in *Kyllo*.[139] While both technologies assist with real-time police surveillance, modern ALPRs are far more sophisticated than the 1980s radio beeper used in *Knotts*, which the Court acknowledged may require "different constitutional principles."[140] One of the primary capabilities of the ALPR is to catalog location data for extended periods of time and, in doing so, generate a written record revealing a car's travel over time that would be nearly impossible to replicate using police manpower alone. At least one ALPR provider advertises that infrared cameras and machine learning allow it to "see through the windshield" to identify distracted drivers and, perhaps more disturbingly, that it can detect wireless signals from devices inside the car "so [a] suspect can be tied to the same place and time" as a vehicle.[141] The transmission of wireless signals, at a minimum, exceeds the scope of what can be perceived by the human eye. Consequently, in the absence of analysis that weighs the nature and scope of the location data collected, as the Court did

137. New York v. Class, 475 U.S. 106, 114 (1986). At the same time, a "citizen does not surrender all the protections of the Fourth Amendment by entering an automobile." *Id.* at 112.

138. *Hill v. State* relied on this reasoning, in part, to affirm the denial of a defendant's motion to suppress evidence seized during a traffic stop initiated because of a hot list alert. "[V]isual surveillance of vehicles in plain view does not constitute an unreasonable search for Fourth Amendment purposes, even if the surveillance is aided by an officer's use of a license plate tag reader, because a defendant does not have a reasonable expectation of privacy in a plainly visible license plate." Hill v. State, 321 Ga.App. 817, 818 (Ga. Ct. App. 2013) (citing Hernandez-Lopez v. State, 319 Ga.App. 662, 664 (Ga. Ct. App. 2013)). Outside of the ALPR context, *see, e.g.*, United States v. McIver, 186 F.3d 1119, 1125 (9th Cir. 1999), *cert. denied* 528 U.S. 1177 (finding that motion-detecting surveillance cameras used to photograph a marijuana growing operation did not violate the Fourth Amendment because the Forest Service could have stationed officers to conduct the same 24-hour surveillance but instead opted for a lower-cost "mechanical eye"); *see, cf.* Kyllo v. United States, 533 U.S. 27 (2001) (holding that a warrantless scan of a greenhouse using sense-enhancing thermal imaging technology constituted an illegal search under the Fourth Amendment because the thermal imaging revealed details about the greenhouse that would have otherwise been unknowable).

139. Zhan, *supra* note 46, at 32; *Kyllo*, 533 U.S. at 27.

140. *Knotts*, 460 U.S. at 284 ("[I]f such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.").

141. Neitzel, *supra*, note 84.

in *Carpenter*, the open fields doctrine does not present the strongest Fourth Amendment case for the regulation of the most cutting-edge ALPRs.

2. The Third-Party Doctrine

Supreme Court cases *United States v. Miller* and *Smith v. Maryland* establish that an individual has no reasonable expectation of privacy in information knowingly and voluntarily revealed to third parties.[142] Law enforcement is therefore permitted to request and obtain such information without a warrant because the act of revealing it forfeits one's reasonable expectation of privacy.

In *United States v. Miller*, the government subpoenaed the bank records of a defendant suspected of operating an illegal distillery.[143] Following his conviction, the defendant argued that the government's warrantless acquisition of his private financial information violated the Fourth Amendment.[144] The Supreme Court rejected the defendant's claim, holding that his bank records were not protected by the Fourth Amendment because he voluntarily shared the information with the bank, a third party.[145] By providing information to the bank, including that which revealed illegal activity, the defendant was thought to have assumed the risk that the bank may share its records with the government.[146]

In *Smith v. Maryland*, a telephone company installed a pen register at law enforcement's request to warrantlessly monitor the phone numbers dialed from a suspect's telephone, without accessing the contents of any phone calls.[147] The defendant, convicted of robbery after placing a series of threatening phone calls to his victim within days of the crime, argued that the phone company's use of the pen register violated his Fourth Amendment rights because it revealed private information about his communications.[148] Rejecting the argument, the Supreme Court affirmed the police's use of the pen register to collect evidence that helped to convict the defendant.[149] First, the Court explained, individuals have no reasonable expectation of privacy in the numbers dialed from their phones because phone companies are generally known to record this information for billing, fraud detection, and other purposes.[150] In addition, the Court found that the limited scope of the data collected by a pen register weighed against a finding that the technology was so intrusive as to violate the Fourth Amendment prohibition against unreasonable searches.[151]

Proponents of ALPR technology may argue that the decision to operate a vehicle is a choice that involves the knowing and voluntary exposure of license plate information to privately-operated cameras, including those equipped

142. *See, e.g.*, John Villasenor, *What You Need to Know about the Third-Party Doctrine*, Atlantic (Dec. 30, 2013), [https://perma.cc/66HV-PACA].
143. United States v. Miller, 425 U.S. 435, 436 (1976).
144. *Id.* at 97.
145. *Id.* at 444.
146. *Id.* at 443.
147. Smith v. Maryland, 442 U.S. 735, 737 (1979).
148. *Id.* at 742.
149. *Id.*
150. *Id.*
151. *Id.*

with ALPR technology or Ring doorbells.[152] Like the bank in *United States v. Miller* and the phone company in *Smith v. Maryland*, ALPR companies are private entities that may share or sell information to law enforcement.[153] *Miller* and *Smith* defined "knowingly" and "voluntarily" broadly to describe the use of essential services like banking and telephone communications. Given these broad definitions, courts may also hold that driving constitutes a knowing and voluntary exposure of vehicle information to third parties, whether ALPRs or other entities. This interpretation would weigh against a finding that ordinary ALPR use violates the Fourth Amendment.

Alternatively, courts may distinguish ALPR cases from *Miller* and *Smith* because drivers are not directly providing their information to private ALPR companies. Instead, private ALPR companies are collecting and analyzing the information on their own and providing it to paying law enforcement entities. But "there is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected" by modern technology like license plate readers.[154] This is especially true today as individuals increasingly rely on third parties for digital services that dubiously obtain informed consent to share and sell user data.[155] Therefore, if applied without regard for the unique attributes of ALPR data, the third-party doctrine does not present the strongest argument that ALPR use either violates the Fourth Amendment or withstands Fourth Amendment scrutiny.

In any case, Congress and the courts have signaled their concern about law enforcement's access to large volumes of third-party data. On April 17, 2024, the House approved The Fourth Amendment is Not For Sale Act, which would require a warrant for police to purchase third party data.[156] As initially drafted, the bill ostensibly would have applied to the sale of ALPR data from private companies to law enforcement, however, the bill was later amended to explicitly exempt "data generated by a public or private ALPR system."[157] While the bill expired at the end of the 118th Congress, the purchase of ALPR

152. *See* Tom Kertscher, *Watch Out*, Marquette Today (July 15, 2024), [https://perma.cc/3D6X-FKYL] ("Most everyone I told about my case was taken aback to hear that I received a traffic ticket based on a homeowner's video" captured using a Ring doorbell.).

153. United States v. Miller, 425 U.S. 435, 444 (1976); Smith v. Maryland, 442 U.S. 735, 742 (1979).

154. Carpenter v. United States, 585 U.S. 296, 314 (2018).

155. *See, e.g.*, Scott Berinato, *"Stop Thinking About Consent: It Isn't Possible and It Isn't Right"*, Harv. Bus. Rev. (Sept. 24, 2018), [https://perma.cc/DNL2-SY52] (interviewing scholar Helen Nissenbaum about the harms of massive consent agreements that users must navigate in order to access digital services).

156. Rebecca Beitsch, *House Passes Bill Requiring Warrant to Purchase Data From Third Parties*, Hill (Apr. 17, 2024, 6:25 PM), [https://perma.cc/FFX5-DKUL].

157. The Fourth Amendment is Not for Sale Act, H.R. 4639, 118th Cong. § 2(e)(1)(C)(ii)(IV), (2023–2024); Press Release, Clay Higgins, U.S. Congressman for Louisiana's 3rd District, Higgins Amendment to Clarify Constitutional Protections, Preserve Law Enforcement Capabilities Passes House (Apr. 22, 2024), [https://perma.cc/77W9–45PD].

data by law enforcement departments would have remained federally legal even if the Fourth Amendment is Not For Sale Act became law.[158]

3. *Carpenter*: Requiring a Warrant to Gather Cell-Site Location Data

In *Carpenter v. United States*,[159] the Court declined to mechanically apply the third-party doctrine to historical cell-site location information (CSLI) provided by cell service providers. Instead, the Court focused on the nature of the data at issue, including its volume and duration. Decided in 2018, *Carpenter* involved a defendant sought by the FBI in connection with several robberies.[160] Without first obtaining a warrant, agents gained access to 127 days of Carpenter's CSLI, revealing 12,898 location points: "an average of 101 data points per day."[161] The CSLI placed Carpenter near the scenes of several robberies, which prosecutors used during trial to convict him.[162] The Sixth Circuit affirmed the conviction, holding that Carpenter did not have a reasonable expectation of privacy in his CSLI because he "shared that information with his wireless carriers."[163] Reversing the Sixth Circuit in a 5–4 decision, the Supreme Court reasoned that because cell phones constantly transmit location information, CSLI is not truly shared voluntarily for the purposes of the third-party doctrine.[164] As a result of the Court's ruling, police now need a warrant to obtain more than six days of historical CSLI to comply with the Fourth Amendment.[165]

Consequently, *Carpenter* probably does not apply to real-time ALPR data that is collected by police based on existing suspicion and acted upon within a relatively short period of time.[166] However, historical CSLI provides the closest Fourth Amendment analogue to historical ALPR data.[167] The majority opinion expressed concern about "the retrospective quality" of CSLI data, which gives police access to "a category of information otherwise unknowable."[168] In other words, CSLI enables law enforcement to "travel back in time to retrace a person's whereabouts, subject only to the retention policies of the wireless

158. The Fourth Amendment Is Not For Sale Act, H.R. 4639, 118th Cong. (2023–2024).
159. Carpenter v. United States, 585 U.S. 296, 320 (2018).
160. *Id.* at 296.
161. *Id.*
162. *Id.*
163. *Id.*
164. *Id.* at 298.
165. *Carpenter*, 585 U.S. at 322.
166. *Id.* at 310 n.3 (declining to "decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and, if so, how long that period might be.").
167. *See* Jennifer Lynch, *Courts Issue Rulings in Two Cases Challenging Law Enforcement Searches of License Plate Databases*, ELEC. FRONTIER FOUND. (May 5, 2020), [https://perma.cc/8T4M-4ZXN] ("Like CSLI, the aggregation of ALPR data can paint a picture of where a vehicle and its occupants have traveled, including to sensitive and private places like homes, doctors' offices, and places of worship . . . And, like CSLI databases, ALPR databases facilitate retrospective searches of cars whose drivers were not under suspicion when the plates were scanned.").
168. *Carpenter*, 585 U.S. at 312.

carriers."[169] The same is true for data collected by private ALPR companies. The billions of records indiscriminately collected by ALPRs grant police long-term access to the daily movements of individuals not sought in connection with any crime.[170] Should an individual subsequently become connected to a crime, police can easily access years of intimate records, highlighting the need for more stringent data retention policies and warrant requirements.[171] Bolstering the comparison between CSLI and ALPR data is the possibility that ALPRs may be able to passively collect communication data, including "information from wireless signals such as Wi-Fi, Bluetooth, and cellular from car communication devices, mobile devices and wearables."[172]

The Fourth Amendment protection against unreasonable searches and seizures constantly requires courts to balance privacy with public safety, a test complicated by the ease with which modern technology grants access to sensitive personal information. As the following lower court decisions explore, *Carpenter* offers the strongest Fourth Amendment framework to address the proliferation of ALPR data and its use by law enforcement.

IV. State & Federal Court Decisions

A handful of lower court decisions have addressed whether the warrantless use of ALPRs by police violates the Fourth Amendment. Many of these cases are summarized in the tables below, organized in order of the year of decision.[173] This list is not exhaustive but aims to present an overview of the conclusions courts have reached based on different factual scenarios involving ALPR data.

Federal Court Decisions					
Case	Court	Year	Holding	Data Type	Data Collection Time Frame
U.S. v. Ellison 462 F.3d 557	6th Circuit	2006	No reasonable expectation of privacy in license plate information retrieved from database	Search of ALPR database revealing outstanding felony warrant	N/A
U.S. v. Yang 958 F.3d 851	9th Circuit	2020	No reasonable expectation of privacy in location of overdue rental car	Database containing a single entry for the vehicle of interest	9 days

169. *Id.*
170. *Id.*
171. *Id.* In Colorado, for instance, surveillance data collected passively must be destroyed after the third anniversary of its collection, unless the data is retained in connection with an incident that might make the data relevant. Colo. Rev. Stat. § 24–72–113(2)(a) (2015).
172. Neitzel, *supra* note 84.
173. Note that many of these decisions stem from motions to suppress ALPR data.

Federal Court Decisions					
Case	Court	Year	Holding	Data Type	Data Collection Time Frame
U.S. v. Rubin 556 F.Supp.3d 1123	N.D. Cal.	2021	Merely accessing ALPR data did not give rise to a Fourth Amendment search	Precise number of database entries revealing defendant's location is unknown: more than one, but not enough to be "detailed" and "encyclopedic"	1 month
U.S. v. Brown 2021 U.S. Dist. LEXIS 206153	N.D. Ill.	2021	No reasonable expectation of privacy in short-term ALPR tracking	Historical data showing about two dozen images of defendant's car over the course of ten weeks	10 weeks
U.S. v. Bowers 2:18-CR-00292-DWA	W.D. Penn.	2021	No Fourth Amendment Violation because the defendant lacked a reasonable expectation of privacy in his license plate, vehicle location, or ALPR data	Two days after offense at issue, law enforcement conducted query of all available ALPR data revealing 106 scans from 33 ALPR cameras	20 weeks
U.S. v. Porter 2022 U.S. Dist. LEXIS 6755	N.D. Ill.	2022	No reasonable expectation of privacy in short-term ALPR tracking	At least two images relevant to the investigation over the course of eight weeks	8 weeks
U.S. v. Zayas 2023 U.S. Dist. LEXIS 155355	S.D.N.Y.	2023	Guilty plea	Historical database with 1.6B records, AI identified suspicious vehicle behavior[174]	2 years
U.S. v. Toombs 671 F.Supp.3d 1328	N.D. Ala.	2023	No Fourth Amendment violation in officers' use of Drug Enforcement Administration System Information License (DEASIL)	One scan of defendant's vehicle reviewed later the same day it was captured	1 day
U.S. v. Jiles 2024 U.S. Dist. LEXIS 34957	D. Neb.	2024	Querying the ALPR database was not a search because the data available was of limited volume and utility to law enforcement	A search of the ALPR database revealed only five or six hits over the course of six months	6 months
U.S. v. Mapson No. 22011159	11th Circuit	2024	Declines to decide whether *Carpenter* requires search warrant for ALPR data due to good-faith exception to exclusionary rule	Reports revealing defendants' location at three locations on the day of shooting	1 day

174. See Brewster, *supra* note 47.

Federal Court Decisions					
Case	Court	Year	Holding	Data Type	Data Collection Time Frame
U.S. v. Martin 2024 U.S. Dist. LEXIS 186377	E.D. Va.	2024	Denies motion to suppress ALPR evidence. No warrantless search because defendant lacked expectation of privacy in license plate number revealed on public roads	188 cameras installed in area spanning 2 cities and 3 counties where robberies occurred. Retention period of 30 days. ALPR search revealed only 3 images of car used by defendant	30 days
U.S. v. Salcido-Gonzalez 2024 U.S. Dist. LEXIS 91349	D. Utah	2024	No Fourth Amendment violation because ALPR database did not operate at the "granular level of detail that would expose the intimate details" of the defendant's life	One ALPR scan at the California-Nevada border and one ALPR scan from the "Denver area," which encompasses the city and many surrounding suburbs	1 to 2 days
U.S. v. Cooper 2025 U.S. Dist. LEXIS 1466	E.D. Louisiana	2025	No Fourth Amendment violation because New Orleans's ALPR system consists of only 60 cameras that revealed limited information about the defendant's travel history	Law enforcement entered the defendant's license plate number into their system, revealing historical reads that placed defendant in the vicinity of two armed robberies	3 to 4 months

State Court Decisions					
Case	Court	Year	Holding	Data Type	Data Collection Time Frame
Hernandez-Lopez v. State 319 Ga. App. 662	Georgia Court of Appeals	2013	No Fourth Amendment violation because hot list alert served same purpose as a manual search for vehicle's plate	Hot list alert from vehicle-mounted ALPR showing wanted person	Instant
Traft v. Commonwealth 539 S.W.3d 647	Kentucky Supreme Court	2018	No Fourth Amendment violation because he defendant lacked both a subjective and objective expectation of privacy in his license plate data displayed while he drove over a public road	Hot list ALPR alert notified police of an active bench warrant, prompting officers to pull over the defendant's car	Instant

State Court Decisions					
Case	Court	Year	Holding	Data Type	Data Collection Time Frame
Uhunmwangho v. State 2020 Tex. App. LEXIS 2466	Texas Court of Appeals	2020	No reasonable expectation of privacy in license plates	Search of ALPR database revealed one image of defendant's car captured on the same day as the traffic stop by one of two ALPR cameras set up on the highway	1 day
Commonwealth v. McCarthy 484 Mass. 493	Mass. Supreme Court	2020	Images captured by four ALPRs posted on two bridges did not give rise to a Fourth Amendment search	Hot list alerts and historical data showing 48 days over the course of three months when the defendant traveled over the bridges	3 months
Commonwealth v. Watkins 304 A.3d 364	Penn. Superior Court	2023	No Fourth Amendment violation because the defendant did not have a reasonable expectation of privacy in his license plate, vehicle exterior, or location on public roads, and no physical trespass occurred	After querying ALPR database and learning that the drug trafficking suspect routinely traveled over a particular road, law enforcement configured the system to issue a hot list alert every time his plate was read in any location. Defendant's car was subsequently scanned over 50 times in nearly 3 months	Nearly 3 months
State v. Patrick 2024 Ohio Misc. LEXIS 325	Cuyahoga Cnty. Ct., Ohio	2024	No Fourth Amendment search because the surveillance network did not create an "exhaustive chronicle" of the defendant's movements	Record of travel down a single street for about 30 blocks and a single snapshot of the defendant's vehicle in another town	1 day
Commonwealth v. Bell Case No. CR23001500–00	Norfolk Circuit Court, Virginia	2024	Grants motion to suppress because Flock's collection and storage of license plate and location data constitutes a Fourth Amendment Search that requires a warrant.	Real-time and historical data collected by 172 cameras installed throughout Norfolk, Virginia with 30-day retention period	N/A
Commonwealth v. Adams 113 Va. Cir. 505	Chesterfield County Circuit Court, Virginia	2024	No Fourth Amendment search because the defendant lacks a reasonable expectation of privacy in license plates displayed while driving over public roads	Search of historical data from 22-camera ALPR system, limited to the 26 hours when a quadruple-homicide occurred, revealing four hits of defendant's car	26 hours

State Court Decisions					
Case	Court	Year	Holding	Data Type	Data Collection Time Frame
State of Oklahoma v. Ifabiyi CF-2023–3	McClain County District Court, Oklahoma	2024	Motion to suppress ALPR data granted. Declines to address Fourth Amendment implications of warrantless ALPR data search because OK law prohibits ALPR data use for any reason other than compulsory insurance law enforcement	ALPR data aggregated by public and private sources revealed that defendants were returning from Houston, TX rather than Dallas, TX, as they had said	N/A
State v. Sidor 558 P.3d 621	Arizona Appeals Court	2024	No Fourth Amendment violation because the limited ALPR data here did not thoroughly catalog the defendant's movements and did not infringe on a reasonable expectation of privacy	Database query showing four ALPR scans of defendant's vehicle in Arizona and Kansas	2 months

The following summaries expand upon several of the cases presented in the charts to reflect the diversity of analysis and outcomes among federal and state courts addressing ALPR issues.

No Fourth Amendment Search, Warning of a *Carpenter*-esque Future for ALPR Technology

While *United States v. Yang* declined to hold that querying an ALPR system constitutes a search, the system at issue contained an average of just four entries for each vehicle identified.[175] In this case, the defendant was observed stealing mail out of collection boxes in a rental vehicle that was six days overdue.[176] The rental company was unable to access the vehicle's location because its GPS system had been disabled, prompting law enforcement to search the Vigilant Solutions LEARN database for license plate hits.[177] The court explained that "the mere expiration of the rental period does not automatically end a lessee's expectation of privacy," but on these facts, the defendant did not establish a reasonable expectation of privacy in his historical location data.[178] Consequently, the Ninth Circuit found that police did not violate the Fourth Amendment by using short-term data from this system to locate the defendant's overdue rental car.[179] Concurring, Judge Bea acknowledged that this particular database did not intrusively catalog the defendant's movements.[180] However, he stressed that ALPRs may eventually present the same problems

175. United States v. Yang, 958 F.3d 851, 862 (9th Cir. 2020).
176. *Id.* at 852.
177. *Id.* at 853.
178. *Id.* at 859.
179. *Id.* at 861–62.
180. *Id.* at 862 (Bea, J., concurring).

addressed in *Carpenter* because they can "effortlessly, and automatically, create voluminous databases of vehicle location information" that allow police to precisely identify details about an individual's life.[181]

No Fourth Amendment Search in Short-Term Tracking but Establishing a Privacy Interest in One Year of Location Data

Similarly, *Commonwealth v. McCarthy*[182] held that no Fourth Amendment search occurred where law enforcement used four ALPRs in two locations to track a defendant over the course of three months.[183] In *McCarthy*, police relied on historical data collected by four total ALPRs to determine how many times a drug trafficking suspect had crossed two bridges in a three-month period.[184] In addition, police received real-time alerts when the suspect passed each ALPR, one of which resulted in his arrest.[185] Addressing whether the use of ALPR technology in this case amounted to a search under the Fourth Amendment, the Massachusetts Supreme Court concluded that the limited use of ALPRs in this case did not invade the defendant's "constitutionally protected expectation of privacy in the whole of his public movements," which "could be implicated by the [more] widespread use of ALPRs."[186] However, the court limited its decision by acknowledging that one year of ALPR data retention was "certainly [] long enough to warrant constitutional protection."[187] The court added that the "surreptitious" nature of ALPR data collection helps it "evade[] the ordinary checks that constrain abusive law enforcement practices."[188]

An AI-Assisted Fishing Expedition Through Billions of Plate Scans Results in a Guilty Plea

Unlike many of the other lower court decisions that have directly addressed ALPR use to date, the breadth and duration of the surveillance in *United States v. Zayas*[189] appeared to present clear dragnet-style abuse of years-old ALPR data that would be ripe for a successful Fourth Amendment challenge. Here,

181. *Yang*, 958 F.3d at 863.
182. Commonwealth v. McCarthy, 484 Mass. 493, 512 (2020).
183. *McCarthy* is considered the first (and possibly the only) appellate case in the country to directly address whether ALPR use constitutes a Fourth Amendment search. *See* Patrick McDonald, *Illinois License Plate Cameras Are Violating People's Constitutional Rights, Says New Suit*, Reason (June 14, 2024, 4:18 PM), [https://perma.cc/EMP5-GPEW]; *see also* Commonwealth v. McCarthy, 134 Harv. L. Rev. 2887 (2021).
184. *McCarthy*, 484 Mass. at 494.
185. *Id.*
186. *Id.* at 502; *McCarthy* acknowledges an "aggregation principle for the technological surveillance of public conduct, sometimes referred to as the mosaic theory." *Id.* at 503; Mosaic theory involves the application of the Fourth Amendment to "government conduct as a collective whole rather than in isolated steps." Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311, 320 (2012).
187. *McCarthy*, 484 Mass. at 506.
188. *Id.* at 500.
189. No. 7:22-cr-178, 2023 U.S. Dist. LEXIS 155355 (S.D.N.Y. Mar. 10, 2023), Mot. to Suppress at 8–9; Nico DeMattia, *AI Traffic Surveillance Can Link Your Driving Patterns to Criminal Behavior*, The Drive (July 18, 2023), [https://perma.cc/Q89Z-TQJE].

the defendant was indicted on federal drug trafficking charges after AI-driven ALPR technology from vendor Rekor Scout flagged him for habitually driving routes known to be popular among drug traffickers.[190] In his motion to suppress, the defendant alleged that Westchester, New York police first queried their massive ALPR database, which collected roughly 16.2 million plate scans per week from nearly 500 cameras in the area.[191] To hone in on the defendant, the motion to suppress asserted, officers conducted a search of more than 1.6 billion ALPR records spanning a period of more than two years.[192] After examining this vast expanse of ALPR data, police identified just two trips that seemed suspicious and placed the defendant on a hot list as a result.[193] Police subsequently pulled the defendant over based on a real-time alert generated by the hot list.[194] The defendant argued that the investigation into his drug trafficking activity began with a "suspicionless search of his ALPR location," therefore, all evidence in the case amounted to fruits from a poisonous tree that should be excluded.[195] However, because the defendant pled guilty, he likely waived his right to appeal the use of this evidence.[196]

Avoiding the Fourth Amendment Issues Raised by ALPRs Entirely

In *United States v. Mapson*,[197] the Eleventh Circuit Court of Appeals declined to consider whether the warrantless use of ALPR data to pinpoint the defendants' vehicle near the location of an attempted homicide shooting was an unconstitutional search. Acknowledging the dearth of case law and legal scholarship about the use of ALPR data as evidence, the court upheld the trial court's ruling in favor of the police based on law enforcement's good faith reliance on then-binding prior precedent.[198] The court found that without "any cases addressing the constitutionality of warrantless acquisition of ALPR data,"[199] it was reasonable for the officer to rely on *United States v. Davis*,[200] which allowed officers to obtain cell-site location data without a warrant.[201] However, the *Mapson* ruling was issued just one day before the Supreme Court decided that police would need a warrant for more than six days of CSLI

190. Zayas, No. 7:22-cr-178, 2023 U.S. Dist. LEXIS 155355 (S.D.N.Y. Mar. 10, 2023), Indictment, ECF No. 5; Mot. to Suppress at 4, 19; Mot. to Suppress at 5; DeMattia, *supra* note 189.
191. Zayas, No. 7:22-cr-178, 2023 U.S. Dist. LEXIS 155355, Mot. to Suppress at 3–4.
192. *Id.* at 4–5.
193. *Id.* at 5.
194. *Id.*
195. *Id.* at 5–6.
196. Zayas, No. 7:22-cr-178, 2023 U.S. Dist. LEXIS 155355, Change of Plea Hr'g, ECF No. 45; Sentencing Submission, ECF No. 58.
197. 96 F.4th 1323, 1334–35 (11th Cir. 2024).
198. *Id.*
199. *Id.* at 1335.
200. 785 F.3d 498, 513 (11th Cir. 2015) (en banc), *abrogated by* Carpenter v. United States, 585 U.S. 296, 316–17 (2018).
201. *Id.*; Davis v. United States, 564 U.S. 229, 241 (2011) ("Evidence obtained during a search conducted in reasonable reliance on binding precedent is not subject to the exclusionary rule.").

in *Carpenter*.[202] As a result, the Eleventh Circuit joined a rich tradition of "Supreme Court and lower court rulings [that] have failed to directly address ALPR technology and whether aggregation of one's public travels implicates Fourth Amendment rights."[203]

Suppressing ALPR Data Due to the Pervasive Nature of Surveillance by 172 Cameras in One City

In *Commonwealth v. Bell*, the trial court addressed the Norfolk Police Department's warrantless use of ALPR data in its ruling on a motion to suppress evidence.[204] The defendant, facing robbery charges, was identified after an independent witness to one robbery provided law enforcement with a plate number, leading officers to search the plate in their ALPR database and discover a "hit" related to another robbery.[205] The defendant argued that "vehicles in the current technology age are akin to cellular telephones as they reveal the continued location of civilians."[206] The court agreed.[207] Granting the motion to suppress evidence of the defendant's vehicle, the court held that the collection and storage of license plate and location data collected by ALPRs is analogous to the CSLI at issue in *Carpenter*, meaning that accessing the data amounts to a Fourth Amendment search that requires a warrant.[208] In 2023, Norfolk, Virginia had installed 172 Flock Safety cameras across the city that "track the locations of vehicles within city limits by license plate number and other physical descriptions with the data being kept for 30 days."[209] Considering the scope of the camera system within Norfolk, the court went further, stating in its order that the breadth and storage capabilities of Flock Safety ALPRs are "akin to a GPS device" and thus require a warrant under *Jones*, which prohibited the installation of a physical GPS tracker on vehicles.[210] With this holding, *Bell* became one of the first cases to put the suppression of warrantless ALPR evidence, which *Yang* and *McCarthy* merely contemplated, into practice.[211]

202. *Mapson*, 96 F.4th at 1335.
203. Yash Dattani, Note, *Big Brother Is Scanning: The Widespread Implementation of ALPR Technology in America's Police Forces*, 24 Vand. J. Ent. & Tech. L. 749, 767 (2022).
204. Commonwealth v. Bell, 113 Va. Cir. 316, 316 (Va. Cir. Ct. 2024).
205. *Id.* at 317.
206. *Id.* at 318.
207. *Id.*
208. *Id.*
209. *Id.* at 316–17.
210. Commonwealth v. Bell, 113 Va. Cir. 316, 318 (Va. Cir. Ct. 2024); United States v. Jones, 565 U.S. 400, 404 (2012).
211. Since the ruling in *Bell*, the City of Norfolk, Virginia has been sued in federal court by an organization challenging the city's use of Flock Safety ALPR cameras. *See* Lars Daniel, *Privacy Violated, Warrantless Surveillance Alleges Flock Safety Camera Lawsuit*, Forbes (Oct. 22, 2024, 10:20 AM), [https://perma.cc/BX7D-STYR]. In February 2025, the U.S. District Court for the Eastern District of Virginia rejected the city's motion to dismiss, finding that plaintiffs "adequately alleged that Norfolk conducts unlawful searches when it uses the plate readers." Daniel Seiden, *Virginia City Must Defend Challenge to License Plate Readers*, Bloomberg L. (Feb. 6, 2025, 8:19 AM), [https://perma.cc/G5M5-WNEC].

Suppressing ALPR Data Used by Police in Violation of Oklahoma State Statute

In *Oklahoma v. Ifabiyi*—adjudicated in Oklahoma state court—a police officer pulled over a vehicle for unsafe driving and smelled marijuana while approaching the vehicle.[212] While conducting a subsequent search of the vehicle, the officer recovered a trash bag containing a handgun and nearly $100,000 in cash.[213] During routine questioning, one defendant advised that the vehicle was traveling from Dallas, Texas, to Oklahoma.[214] However, a query of the available ALPR database revealed that the defendants were in fact traveling from Houston, Texas, not Dallas.[215] While the defendants cited *Carpenter* and *Bell* in support of their arguments in favor of suppressing the ALPR data, the court ruled that it "need not address the Fourth Amendment implications of said search because the State of Oklahoma has a statute directly on point which prohibits the use of ALPR data" for any reason other than enforcement of the state's mandatory insurance law.[216] The court suppressed the ALPR evidence accordingly.[217] Following this case, Oklahoma lawmakers have raised concerns that the use of ALPRs by law enforcement, which rarely complies with state law, will jeopardize legitimate criminal investigations.[218] While many arguments in favor of limiting the use of ALPRs appear to prioritize the rights of defendants, Oklahoma lawmakers' concerns post-*Ifabiyi* represent one decidedly pro-law enforcement argument for carefully regulating the use of this technology by police.

Comparing ALPR Data to the Beeper in *Knotts* and Finding No Fourth Amendment Search Occurred

In *United States v. Martin*, police used both private surveillance footage and Flock Safety ALPRs to identify a distinctive gold Acura belonging to a defendant charged with several robbery-related offenses.[219] Based on this information, police were able to obtain a warrant to place a GPS tracker on the vehicle, resulting in a felony traffic stop and an arrest.[220] In denying the defendant's motion to suppress evidence collected using the Flock Safety ALPR system, the court held that law enforcement's use of the system did not constitute a search under the Fourth Amendment.[221] First, the court stated

212. Oklahoma v. Ifabiyi, No. CF-2023–3 (McClain Cnty. Dist. Ct. Sept. 23, 2024), Order Denying, In Part, Defendants' Motion to Suppress Evidence at 1–2 (noting that marijuana is illegal in Oklahoma without a license), [https://perma.cc/99A9-A4P9].
213. *Id.*
214. *Id.*
215. *Id.*
216. *Id.* The Oklahoma statute also provides that ALPR data may be used for any purpose permitted by law to allow latitude if additional applications of ALPR technology are approved in the future.
217. *Id.*
218. *Gann Highlights Suppression of License Plate Scanner Evidence by State Court*, Okla. House of Reps. (Sept. 30, 2024), [https://perma.cc/35FG-QQJG] ("This lazy policing is now putting many potential convictions at risk.").
219. United States v. Martin, 753 F.Supp.3d 454, 459 (E.D. Va. 2024).
220. *Id.* at 460.
221. *Id.* at 476.

that the defendant lacked a reasonable expectation of privacy in his vehicle's exterior attributes, including bumper stickers, because they were visible to anyone on the road.[222] The court compared this case to *Knotts*, arguing that the Flock ALPR system merely augmented law enforcement's ability to perceive what was already in plain view.[223] The court next noted that the ALPR system captured only three photos of the defendant's car during the relevant 30-day period, which did not rise to the invasive level of tracking the whole of defendant's physical movements as contemplated in *Carpenter*.[224] As a result, the District Court declined to rule that the use of ALPR data in this case violated the Fourth Amendment.[225]

As courts have acknowledged in several recent decisions, ALPRs risk revealing the same "intimate window" into one's "familial, political, professional, religious and sexual associations" as the CSLI in *Carpenter*.[226] These decisions demonstrate that the volume of data searched and the time frame and geography over which collection occurs should be central to any Fourth Amendment analysis of ALPR use by law enforcement. As the next Part explores, the sentiments expressed in these cases suggest that the Supreme Court might issue a limited rule, consistent with *Carpenter* and the order in *Bell*, if it hears an ALPR case.

V. A Judicially Created Rule Limiting ALPR Use in Criminal Investigations

If the Supreme Court ruled today on a case involving the warrantless use of ALPR data by police, it would weigh individual privacy interests against the important government aim to enforce the law.[227] Because of the need to strike a delicate balance, the Court typically declines to create sweeping Fourth Amendment rules. Even in *Carpenter*, perhaps the Supreme Court's most privacy-protective Fourth Amendment case in recent memory, the Court employed surgical language to limit the decision's scope to the specific data, technology, and time frame at issue.[228] The Court would likely rule similarly if confronted with a case involving ALPR use and may even defer to existing state use and retention policies, though data sharing across jurisdictions limits the impact of any one department's policies.

The rule proposed in this Comment would differentiate between the use of real-time hot list alerts and historical ALPR data, affording stronger Fourth Amendment protections to historical data associated with individuals who are

222. *Id.* at 469.
223. *Id.* at 472.
224. United States v. Martin, 753 F.Supp.3d at 472.
225. *Id.* at 476.
226. Carpenter v. United States, 585 U.S. 296, 311 (2018).
227. *See, e.g.*, Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 528 (7th Cir. 2018) (holding that a public utility's continuous collection of residential energy use amounted a search given the privacy interest in personal energy collection but was reasonable and therefore constitutionally sound due to the important government interest served by the data collection).
228. *Carpenter*, 585 U.S. at 316.

not suspected in connection with any crime. Like the data collection period proposed in *Carpenter*, this rule would require a warrant to access historical data that is more than six days old regardless of an individual's connection to a crime.[229] This bright-line rule would mitigate the Supreme Court's concern about the "difficulties created for courts, police, and citizens by an ad hoc, case-by-case definition of Fourth Amendment standards to be applied in differing factual circumstances."[230] This rule still invites law enforcement to surveil with impunity up until the seven-day mark, which would leave certain shorter-term yet sensitive circumstances vulnerable, like a visit to an abortion clinic or participation in a protest.[231] Likewise, this approach does not discriminate based on the number of ALPRs used to conduct surveillance over time. This represents one shortcoming of the rule because, while three days of data collected by 200 cameras for a single suspect would likely be more intrusive than data collected by a single camera eight days ago, the rule would permit warrantless access to the former and require a warrant to access the latter. With that said, the rule would not foreclose courts from holding that a shorter surveillance period nevertheless violates the Fourth Amendment.

Under this time-limited approach, without a warrant, law enforcement would need to affirmatively add suspicious license plates to a hot list based on reasonable suspicion[232] to access real-time alerts about the vehicle's whereabouts.[233] Maine and New Hampshire have already statutorily imposed such requirements.[234] Similarly, Indiana State Police policy requires officers to

229. Note that *Carpenter* is not understood to have created a bright line rule requiring a warrant at the seven-day mark. Instead, the Court held that an individual has a reasonable expectation of privacy in CSLI data of seven or more days, so the 127 days of warrantless surveillance at issue violated the Fourth Amendment. *Id.* at 310 n.3, 312–13.

230. Oliver v. United States, 466 U.S. 170, 181 (1984) (collecting cases). For a list of factors that courts may consider when making case-by-case determinations about the constitutionality of ALPR surveillance, *see* Dan Noffsinger, *The New McCarthyism: How the Massachusetts Supreme Judicial Court for Automated License Plate Readers and the Mosaic Theory All Wrong*, 26 J. Tech. L. & Pol'y 1, 24 (2021).

231. One solution to this problem might leave intact the proposed seven-day rule *unless* the data at issue reveals information that ties to a specific state or federal constitutional protection, like First Amendment freedom of speech or freedom of association. U.S. Const. amend. I. Unfortunately, even this approach would leave abortion seekers, for example, vulnerable to surveillance in states where abortion has been criminalized or is otherwise unprotected by the law, highlighting the privacy issues that will persist even under a more privacy-protective ALPR regulatory scheme.

232. Reasonable suspicion is a "less demanding standard" than the probable cause requirement to obtain a warrant. *See* Alabama v. White, 496 U.S. 325, 330 (1990). The standard is met when a police officer has a reasonable suspicion that a person is committing or about to commit a crime based on specific facts and reasonable inferences. Terry v. Ohio, 392 U.S. 1, 21 (1968).

233. *See, e.g.*, Cal. St. Auditor, *supra* note 11, at 2, 9 (showing how ALPRs identify license plate data stored on a hot list and alert law enforcement, a process triggered by just 400,000 of the 320 million license plate images captured by the Los Angeles Police Department during the audit period) (internal citation omitted).

234. N.H. Rev. Stat. Ann. § 236:130.3(g) (2022); Me. Rev. Stat. Ann. tit. 29-A, § 2117-A (West 2022). On the other hand, ALPR data may also be used to help law enforcement

have reasonable suspicion that a crime has occurred before they may query the license plate database at all.[235] "Reasonable articulable suspicion" is also a requirement to access the Department of Justice's Drug Enforcement Administration System Information License (DEASIL) database.[236] Upon adding a vehicle to a hot list, law enforcement would gain the ability to collect historical ALPR data about this vehicle over a reasonable time period for investigation. To define a reasonable time frame, the Court might look to *Carpenter* and *McCarthy*, which reached conclusions based in part on the invasiveness of the technology at issue.[237] The Court should also consider how the nature of different offenses influences what constitutes a reasonable time frame. For example, the pursuit of a single stolen car likely requires less surveillance time than a more complex white collar criminal investigation.[238]

While this rule would not attempt to regulate the data retention period used across jurisdictions, requiring a warrant to query an ALPR database would nevertheless curb law enforcement's ability to use months and years of historical ALPR data about vehicles not connected to any crime.[239] Where it may be reasonable to collect months of historical ALPR data for vehicles sought in connection with a crime, this judicial rule would complement existing regulations that intend to limit the retention and accessibility of historical data about vehicles not sought in connection with a crime. Still, there are compelling reasons for police to hold on to some historical ALPR data about these vehicles, such as to identify witnesses and detect new evidence for criminal investigations.[240] But at present, states have provided for retention periods as short as

---

articulate its reasonable suspicion. *See, e.g.*, Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PENN. L. REV. 327, 378 (2015).

235. Casey Smith, *Indiana Lawmakers Want to Crack Down on Data Privacy. What About License Plate Readers?*, IND. CAP. CHRON. (Feb. 1, 2023, 7:00 AM), [https://perma.cc/Z3UZ-N757] (noting that Indiana lacks statewide ALPR legislation).

236. *See, e.g.*, State v. Sidor, 558 P.3d 621, 623–24 (Ariz. App. Ct. 2024).

237. Carpenter v. United States, 585 U.S. 296, 302, 310 (2018) (seven days of continuous CSLI too invasive for a warrantless search); Commonwealth v. McCarthy, 484 Mass. 493, 494 (2020) (three months of ALPR data collected on just two bridges not so invasive as to constitute a Fourth Amendment search).

238. *See* Jon Regardie, *LAPD Pursuits Lead to More than 1,500 Collisions Over Five Years*, CROSSTOWN, (May 1, 2023), [https://perma.cc/RFK6-LAGR] ("[T]he average duration [of a pursuit] is 5.34 minutes. But 72% last five minutes or less."); *Corporate and White-Collar Prosecutions Hit NewAll-Time Lows in FY 2022*, TRAC-FBI, (Jan. 29, 2023), [https://perma.cc/PZ8D-9JHY] ("White-collar investigations often take years before they result in filing a criminal case.").

239. *Data Driven: What is ALPR?*, ELEC. FRONTIER FOUND., [https://perma.cc/YL3S-TEDU] (noting that historical ALPR data is often stored as long as five years).

240. *See, e.g.*, Leonard L. Hayhurst, *Eubanks to Serve 90 Days, Pay Fine for Reporting Fake Shooting*, COSHOCON TRIB. (Feb. 12, 2018, 3:49 PM), [https://perma.cc/U8VR-GDLS] ("Eubanks' story didn't hold up as he began giving conflicting information, according to officials. Investigators used the license plate reader on Eubanks' cruiser to find witnesses to the event."); *see also* Mark Segraves, *DC Police Have New Clues in Case of Man Who Vanished After Arranging Internet Date*, NEWS4 WASH. (Jan. 19, 2018, 11:54 AM), [https://perma.cc/6MX3-FNUX] ("A license-plate reader provided

three minutes and as long as five years.[241] Consistent with Justice Brandeis's principle that state and local governments act as laboratories of democracy, the Court is unlikely to define uniform nationwide ALPR retention standards that extend beyond the limited scope of the Fourth Amendment protection against unreasonable searches to more generalized privacy or First Amendment concerns, for example.[242]

One counterargument to this proposed judicial rule is that it may counterintuitively encourage police to exercise less discretion when adding license plates to a hot list to monitor a larger number of vehicles. However, as considered above, this concern can be mitigated by requiring police to articulate their grounds for reasonable suspicion to add vehicles to hot lists.

While these direct and indirect limitations on ALPR use may seem overly restrictive to law enforcement, alternative evidence collection methods should help fill any resulting gaps while still protecting individual privacy rights. If the Supreme Court rules on a case involving ALPR technology, it may also urge Congress to pass legislation that more clearly defines acceptable and unacceptable uses of ALPR data in light of the privacy concerns that arise even without a criminal investigation taking place. In his *Jones* concurrence, Justice Alito did the same, explaining that "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative . . . A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[243]

Ultimately, no one legislative or judicial remedy is likely to fully eradicate the privacy harms associated with ALPR technology, in part because of the issues that remain with enforcement.[244] The passage of laws alone is insufficient without robust enforcement mechanisms, evidenced by the current status of California's Senate Bill 34 and the myriad law enforcement agencies

---

one of their first clues in the case. Someone drove McMillan's car on April 28—six days after he disappeared—on East Capitol Street SE near Benning Road NE.").

241. New Hampshire has the nation's shortest retention period for non-hot list data, requiring that it must be purged after just three minutes. N.H. Rev. Stat. Ann. §§ 261.75-b, 236.130 (2024). Alabama lands on the other end of the retention spectrum, requiring state law enforcement agencies to dispose of ALPR data after five years. Ala. Admin. Code r. 265-X-6-.06 (2022). But many states lack retention guidance altogether, instead allowing individual law enforcement departments or municipalities to create their own standards. *See* Fourth Amend. Ctr., *supra* note 51.

242. New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

243. United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring) (internal citations omitted).

244. *See* Stephen Rushin, *The Legislative Response to Mass Police Surveillance*, 79 Brook. L. Rev. 1, 50 (2013) ("The Supreme Court is institutionally limited in its capacity to develop a response to the digitally efficient investigative state"); Cal. Dep't of Justice, Div. of Law Enforcement, *No. 2023-DLE-06, California Automated License Plate Reader Data Guidance* (2023) (urging California law enforcement agencies to begin complying with Senate Bill 34, which passed in 2015 and is supposed to prevent law enforcement agencies from distributing ALPR data to out-of-state agencies, including the federal government).

that habitually fail to comply.[245] For this reason, law enforcement agencies and their respective oversight bodies must continually evaluate and improve upon their ALPR policies *and* ensure compliance with those policies.[246] Alongside these necessary efforts, the proposed judicial rule would act to safeguard criminal defendants from the overzealous, abusive, or illegal use of ALPR data as evidence during trial, when the technology arguably poses its greatest threat to personal liberty.

Increased transparency may also promote accountability among law enforcement agencies.[247] The City of Piedmont, California, claims to have implemented the first Flock ALPR Transparency Portal in the country in 2021.[248] The Denver Police Department (DPD) in Colorado recently followed suit, establishing a "Flock Safety Transparency Portal" that shares metrics like the number of cameras in use, the data retention period, and the 75-plus external agencies that can access ALPR data captured by DPD.[249] Several municipalities throughout California and beyond have since implemented similar measures, though Denver is one of the largest to have adopted Flock's portal to date.[250] Cities including Amarillo, Texas have taken a different approach, commenting publicly on the use of cameras in an effort to "inform[]

245. *See* Andrew J. Campa, *California Cops Illegally Shared License Plate Details, Violating Privacy Laws, Grand Jury Says*, L.A. Times (June 27, 2024, 5:30 PM), [https://perma.cc/AS8W-Z85U] (detailing a grand jury report which found that Sacramento County law enforcement shared records from 1.3 million registered vehicles with out-of-state agencies, in violation of Senate Bill 34); *see also* Nick Hidalgo & Matt Cagle, *Dozens of Police Agencies in California are Still Sharing Driver Locations with Anti-Abortion States. We're Fighting Back.*, ACLU (Feb. 13, 2024), [https://perma.cc/5DAZ-WHCY] ("35 police agencies . . . have refused to comply" with Senate Bill 34).

246. The California State Auditor has already offered this recommendation to the police departments of Fresno, Los Angeles, Marin, and Sacramento. Cal. St. Auditor, *supra* note 11, at 5.

247. In 2017, the California Supreme Court held that license plate data accumulated by ALPR systems does not constitute an "investigative record" for the purpose of the state's public records exemption for police investigations because the data is not collected in connection with any crime. As a result, the data can be made available through public records requests, addressing "'the public's strong interest in understanding how police surveillance impacts privacy.'" Press Release, Elec. Frontier Found., *ACLU Win Court Ruling That Police Can't Keep License Plate Data Secret* (Aug. 31, 2017), [https://perma.cc/4R7S-PA4V].

248. *See Flock Safety and Piedmont Police Launch First-Ever LPR Transparency Portal*, Flock Safety (June 10, 2021), [https://perma.cc/6LDU-KFKU].

249. *Transparency Portal*, Denver Police Dept. (last updated Mar. 4, 2025), [https://perma.cc/G6RW-ZJFS]; *see also* Press Release, *City of Denver, Denver Police Announce License Plate Reader Dashboard Now Available, City and County of Denver* (Sept. 19, 2024), [https://perma.cc/J8G8-F5DE].

250. *See, e.g.*, *Transparency Portal*, San Diego Police Dept. (last updated Mar. 5, 2025), [https://perma.cc/8JEB-HLL7]; *Transparency Portal*, Oakland Police Dept. (last updated Mar. 4 2025), [https://perma.cc/Q55J-CMQG]; *Flock Safety Transparency Portal*, Hazelwood Mo. Police Dept., [https://perma.cc/7HDZ-P33F].

citizens."[251] Other states, including New Jersey, release annual audits of ALPR data collected and used by law enforcement.[252]

As police departments across the country roll out ALPR transparency portals, and as state and local governments pass and amend their own ALPR regulations, a clear judicial rule will help to protect the Fourth Amendment rights of criminal defendants facing an increasingly expansive surveillance landscape.

Conclusion

As was the case in *Jurassic Park*, where scientists reintroduced previously extinct dinosaur species to establish a highly dangerous wildlife park, technology developers have often been "so preoccupied with whether they could, they didn't stop to think if they should."[253] There is perhaps no greater example of this phenomenon than the rapid and largely unchecked spread of technology wielded by the state to monitor civilians. Police surveillance conducted using ALPRs has thus raised diverse concerns about the technology's relationship to the Fourth Amendment.[254]

In the criminal justice context, *Carpenter* offers the strongest case for restricting warrantless access to historical ALPR data without hamstringing more time-sensitive investigative needs. Since 2021, federal appeals courts have similarly applied *Carpenter* to restrict the use of other highly invasive surveillance technologies. In *Leaders of a Beautiful Struggle v. Baltimore Police Department*, the Fourth Circuit Court of Appeals assessed the propriety of the Baltimore Police Department's Aerial Investigation Research (AIR) program under the Fourth Amendment.[255] The AIR program surveilled and retained location data for about ninety percent of Baltimore on a daily basis

251. The mayor of Amarillo insisted that the cameras are "not surveillance technology" and vaguely remarked that they are not "collecting any data on anyone." Instead, "[t]hese cameras have a live feed. They go to storage, and they purge themselves every so often. So [after] roughly 90 days that information gets taken out if it wasn't … needed in a specific event." Caylee Hanna, *City of Amarillo Speaks About License Plate Readers*, My High Plains (Jan. 27, 2025, 10:01 PM), [https://perma.cc/GB5H-AWDQ] (internal quotations omitted). Some Texans may doubt the mayor's statements about the use of ALPRs for surveillance given recent efforts across the state to ban interstate travel for the purposes of undergoing abortions, though Amarillo voters did reject such a measure in the 2024 election. *See* Olivia Aldridge, *Interstate Travel Becomes a Target for the Anti-Abortion Movement With Texas Filing*, Nat'l Pub. Radio (May 17, 2024, 5:59 PM), [https://perma.cc/2VKU-K4Q8]; Jayme Lozano Carver, *Amarillo Voters Reject Abortion "Travel Ban," a Rare Rebuke of Anti-Abortion Movement in Texas*, Tex. Trib. (Nov. 5, 2024, 10:00 PM), [https://perma.cc/B6U9-SGZC].

252. Kevin A. Canessa Jr., *State Releases Audit of Automated License Plate Readers*, Observer (July 16, 2024), [https://perma.cc/WS8E-4348].

253. Jurassic Park (Amblin Entertainment 1993).

254. One purpose of the Fourth Amendment is to "slow down police surveillance." United States v. Brown, No. 19 CR 949, 2021 U.S. Dist. LEXIS 206153, at 9 (N.D. Ill. Oct. 26, 2021).

255. Leaders of a Beautiful Struggle v. Baltimore Police Dep't, 2 F.4th 330, 334 (4th Cir. 2021) (en banc).

using a private contractor's surveillance planes for an estimated 12 hours each day.[256] Consistent with the rule advanced in this Comment, the Fourth Circuit acknowledged that *Carpenter* distinguished between short-term movement tracking and longer-term movement tracking that may allow police to deduce sensitive personal attributes, much like the attributes that may be deduced by analyzing historical ALPR data.[257] The Fourth Circuit continued that longer-term tracking under a program like AIR violates a reasonable expectation of privacy in the whole of one's movements and thus requires a warrant, sounding a death knell for the controversial surveillance program.[258]

More recently, in *United States v. Smith*,[259] the Fifth Circuit Court of Appeals ruled that geofence warrants,[260] which law enforcement uses to identify all mobile devices within a specific geographic area, are "categorically" unconstitutional under the Fourth Amendment.[261] Like ALPRs and Baltimore Police Department's AIR program, geofence warrants involve public-private partnerships between police departments and technology companies, in this case, Google.[262] Here, police struggled to identify a suspect in the armed robbery and assault of a U.S. Postal Service worker, so they obtained a geofence warrant covering a large area physically and temporally near the scene of the crime.[263] In response to the warrant, Google searched "through its *entire* database" and provided police with information on several devices, including the defendants' cell phones.[264] Citing *Carpenter*, the Fifth Circuit held that individuals have a reasonable expectation of privacy in the location data that law enforcement seeks through geofence warrants. Disagreeing with a Fourth Circuit geofence warrant case,[265] the court continued that people do not meaningfully volunteer their data to companies like Google, given the necessity of smartphones in modern society.[266] The Fifth Circuit emphasized in its decision that police reliance upon such intrusive technology too closely resembles the reviled general warrants of yore.[267]

The circuit courts' reliance upon *Carpenter* to rein in the expansion of other police surveillance methods in *A Beautiful Struggle* and *Smith* bodes well for individuals seeking to limit the use of ALPR evidence in criminal cases.

256. *Id.*
257. *Id.* at 344–346.
258. *Id.* at 340.
259. United States v. Smith, 110 F.4th 817 (5th Cir. 2024).
260. For more background information on geofence warrants, see FOURTH AMEND. CTR., GEOFENCE WARRANT PRIMER, NAT'L ASS'N CRIM. DEF. LAWS. (Aug. 29, 2023), [https://perma.cc/U6WE-K5NP].
261. *Smith*, 110 F.4th at 838.
262. *Id* at 822–823.
263. *Id.* at 827.
264. *Id.* at 837 (emphasis in original).
265. The Fourth Circuit has ruled that geofence warrants do not constitute a search because people voluntarily expose their locations to Google and therefore have no reasonable expectation of privacy in that data. United States v. Chatrie, 107 F.4th 319, 339 (4th Cir. 2024).
266. *Smith*, 110 F.4th at 835.
267. *Id.* at 836.

Considering the recent decisions in *A Beautiful Struggle* and *Smith* alongside the cases that have begun to probe the Fourth Amendment implications of ALPR technology, the Supreme Court and lower courts should sharply limit the admissibility of historical ALPR data while preserving law enforcement's ability to use real-time alerts to effectively police ongoing or unresolved crime.

In the meantime, without robust judicial or legislative remedies, practitioners should vigorously challenge the accuracy of ALPR data in case it can be suppressed as evidence prior to a criminal trial.[268] For instance, an attorney may challenge the use of ALPR analytics as a scientific method by filing a *Daubert* motion.[269] Outside of court, advocates may encourage elected officials and local police departments to contract with ALPR vendors that do not engage in the mass surveillance characteristic of Flock and other leading providers.[270] Alternatively, advocates may urge these entities to impose contractual limitations on the far reach of the technology's data sharing and surveillance.[271] Taking matters into his own hands, one privacy advocate has begun an initiative to map ALPR locations worldwide to raise awareness about the use of the technology and to make it easier for individuals to evade digital capture.[272] Recent activity, including pending lawsuits in Virginia, Illinois, and Connecticut[273] and a handful of recent court decisions, suggests that the ALPR privacy question is not going away anytime soon.[274]

---

268. *See* Commonwealth v. Bell, 113 Va. Cir. 316 (Va. Cir. 2024).
269. Fourth Amend.Ctr., *supra* note 51.
270. In February 2025, the City Council of Eureka, California rejected a contract to install 21 ALPRs throughout the city, citing concern about Fourth Amendment privacy protections and public pushback against the potential for ALPR data sharing among law enforcement agencies. Sage Alexander, *Eureka, Calif. Votes No on License Plate Reader Cameras*, Gov. Tech. (Feb. 6, 2025), [https://perma.cc/7RRE-UG6G].
271. Chad Marlow & Jay Stanley, *How to Pump the Brakes on Your Police Department's Use of Flock's Mass Surveillance License Plate Readers*, ACLU (Feb. 13, 2023), [https://perma.cc/8VFS-FLQH].
272. DeFlock, [https://perma.cc/4JV2–7PZQ]; *see* Heather Gann, *Huntsville-Born Software Engineer Mapping License Plate Readers Nationwide: 'I Don't Like Being Tracked'*, AL.com (Nov. 15, 2024, 11:11 AM), [https://perma.cc/PZN6-UWTU] ("So far, nearly 2,000 cameras have been reported in the United States and more than 5,500 have been reported around the world."). ALPR-averse individuals will likewise delight in the commercial availability of license plate covers that thwart recognition by license plate cameras, though they may be illegal in some jurisdictions. *See, e.g.*, *IR Invisible-Plate Anti-ALPR / NPR Infrared Filtering Cover*, Sunflex Zone, [https://perma.cc/U962-G5DB]; *see also* Por Jaijongkit, *Is Covering Up License Plates to Avoid Traffic Cameras Illegal in Colorado?*, Colo. Sun (Jan. 29, 2025, 8:51 AM), [https://perma.cc/7HLQ-XUVC] (The answer is yes).
273. Seiden, *supra* note 211; McDonald, *supra* note 183; Katherine Revello, *Lawsuit: License Plate Readers Found in CT Violate 4th Amendment*, Conn. Inside Investigator. (Oct. 23, 2024), [https://perma.cc/ET4A-BRFZ].
274. Challenges to the use of ALPRs are not confined to the United States, either. In New Zealand's Auckland District Court, for example, the month of August 2024 saw "at least four separate cases [] challenging the admissibility of the images [ALPRs] produce." Phil Pennington, *Police Cameras: Multiple Court Challenges to Use of Number Plate Identification*, Radio New Zealand (July 18, 2024, 8:46 AM), [https://perma.cc/9JEW-3FRE].

Beyond the Fourth Amendment, the use of ALPRs may implicate First Amendment rights, including the free exercise of religion and the freedom of association.[275] These chilling effects, though outside the scope of this Comment, present a valuable opportunity for further discussion.[276]

275. *See* Adam Goldman & Matt Apuzzo, *NYPD Defends Tactics Over Mosque Spying; Records Reveal New Details on Muslim Surveillance*, HUFF. POST (APR. 25, 2012), [https://perma.cc/TS6D-8YEK] (revealing collection of license plate data from worshippers parked near a mosque); *see also* INT'L ASS'N OF CHIEFS OF POLICE, PRIVACY IMPACT ASSESSMENT REPORT FOR THE UTILIZATION OF LICENSE PLATE READERS 13 (2009) (acknowledging the risk that individuals "will become more cautious in the exercise of their protected rights of expression, protest, association, and political participation" due to increased LPR surveillance).

276. *See, e.g.*, POLICING FREE SPEECH: POLICE SURVEILLANCE AND OBSTRUCTION OF FIRST AMENDMENT-PROTECTED ACTIVITY, ACLU (2010).