

No. 25-14394

In the United States Court of Appeals
for the Eleventh Circuit

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

ROBERT GLENN SLAYBAUGH,

Defendant-Appellant.

On Appeal from the United States District Court
for the Middle District of Alabama
No. 3:25-cr-00104-BL-SMD-1; Hon. Bill Lewis

**BRIEF OF PROJECT FOR PRIVACY AND SURVEILLANCE
ACCOUNTABILITY, INC. AS *AMICUS CURIAE*
SUPPORTING APPELLANT AND REVERSAL**

GENE C. SCHAERR
ERIK S. JAFFE
JUSTIN A. MILLER
SCHAERR | JAFFE LLP
1717 K Street NW, Suite 900
Washington, DC 20006
Telephone: (202) 787-1060
gschaerr@schaerr-jaffe.com

Counsel for Amicus Curiae

FEBRUARY 13, 2026

USA v. Slaybaugh

**CERTIFICATE OF INTERESTED PERSONS AND
CORPORATE DISCLOSURE STATEMENT**

Under Federal Rule of Appellate Procedure 26.1 and Eleventh Circuit Rules 26.1-1 through 26.1-3, and in addition to those persons and entities identified by the Appellant and the Appellee, *Amicus* identifies all additional attorneys, persons, associations of persons, firms, partnerships, or corporations that have an interest in the outcome of this case:

1. Jaffe, Erik S., *Counsel for Amicus Curiae Project for Privacy and Surveillance Accountability, Inc.*
2. Miller, Justin A., *Counsel for Amicus Curiae Project for Privacy and Surveillance Accountability, Inc.*
3. Project for Privacy and Surveillance Accountability, Inc., *Amicus Curiae*
4. Schaerr, Gene C., *Counsel for Amicus Curiae Project for Privacy and Surveillance Accountability, Inc.*
5. SCHAERR | JAFFE, LLP, *Counsel for Amicus Curiae Project for Privacy and Surveillance Accountability, Inc.*

USA v. Slaybaugh

Amicus states that no publicly traded company or corporation has an interest in the outcome of this case or appeal. Fed. R. of App. P. 26.1; 11th Cir. R. 26.1.

Project for Privacy and Surveillance Accountability, Inc. is a nonprofit corporation headquartered in Washington, D.C., and recognized as a social welfare organization under Section 501(c)(4) of the Internal Revenue Code. It has no parent corporation, has issued no stock, and as such, no publicly held company owns 10 percent or more of its stock.

TABLE OF CONTENTS

CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT	C1
TABLE OF AUTHORITIES.....	ii
INTRODUCTION, INTEREST OF <i>AMICUS CURIAE</i> AND SOURCE OF AUTHORITY TO FILE	1
STATEMENT OF THE ISSUES.....	3
SUMMARY OF ARGUMENT.....	3
ARGUMENT	6
I. The Lower Courts’ Misapplication of <i>Carpenter</i> and Public-Exposure Doctrine Improperly Reduces the Fourth Amendment’s Protection to Visibility and Duration Tests.	7
A. The Fourth Amendment implicates <i>aggregated</i> surveillance power, not individual data points.....	8
B. <i>Carpenter</i> regulates retrospective surveillance power; it does not set a numerical or scale-based threshold.	17
II. ALPR Radically Departs from Founding Era Understandings of Privacy and Threatens Intrusions Far Worse than General Warrants.	21
A. ALPR is a radical departure from historical privacy understandings and threatens everyday freedoms.	22
B. The district court’s rule invites expansive future surveillance.....	27
CONCLUSION.....	31
CERTIFICATE OF COMPLIANCE.....	33

TABLE OF AUTHORITIES

Cases	Page(s)
* <i>Carpenter v. United States</i> , 585 U.S. 296 (2018)	1-5, 7-9, 11-19, 21, 24, 25, 27, 30, 31
<i>Chatrie v. United States</i> , No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026).....	27
<i>Commonwealth v. Kurtz</i> , 348 A.3d 133 (Pa. 2025)	28
<i>Fuqua v. Turner</i> , 996 F.3d 1140 (11th Cir. 2021)	7
<i>Katz v. United States</i> , 389 U.S. 347 (1967)	7, 14
* <i>Kyllo v. United States</i> , 533 U.S. 27 (2001)	7, 20, 22, 23, 25
<i>Oliver v. United States</i> , 466 U.S. 170 (1984)	13
<i>Stanford v. Texas</i> , 379 U.S. 476 (1965)	7
<i>United States v. Davis</i> , 109 F.4th 1320 (11th Cir. 2024)	9
<i>United States v. Di Re</i> , 332 U.S. 581 (1948)	12
<i>United States v. Jones</i> , 565 U.S. 400 (2012)	9, 14
<i>United States v. Karo</i> , 468 U.S. 705 (1984)	7
<i>United States v. Knotts</i> , 460 U.S. 276 (1983)	4, 13, 14

*Authorities upon which we principally rely are marked with an asterisk

Rules

Fed. R. App. P. 26.1 1, 2
Fed. R. App. P. 29 1
11th Cir. R. 26.1 1, 2

Other Authorities

Tyler Arnold,
*FBI Used Undercover Agent To Investigate Catholics,
Says Weaponization Committee Chairman*, EWTN News
(Apr. 11, 2023, 3:30 PM) 16

Ahmad Austin Jr.,
*‘Dystopian’ Super Bowl Ad for Ring Camera Gets
Bipartisan Blowback: ‘Propaganda for Mass Surveillance,’*
Mediaite (Feb. 9, 2026, 11:05 AM)..... 29

Jeremy Bentham,
Panopticon, or the Inspection House (1791) 25

Matt Burgess & Dhruv Mehrotra,
*License Plate Readers Are Creating a US-Wide Database
of More Than Just Cars*, Wired (Oct. 3, 2024, 6:38 AM)..... 15

Flock Safety,
License Plate Readers (LPR)..... 10

Flock Safety,
Privacy & Ethics 10

*John Adams’s Reconstruction of Otis’s Speech in
the Writs of Assistance Case, in Collected Political
Writings of James Otis* (Richard A. Samuelson ed.,
Liberty Fund 2015) 22

Jocelyn Kaiser,
*A Judge Said Police Can Search the DNA of
1 Million Americans Without Their Consent.
What’s Next?* Science (Nov. 7, 2019) 28

Kelly Kazek,
‘Terrifying’ Super Bowl Commercial Has People Vowing To Never Buy This Popular Product, AL.com
 (Feb. 10, 2026, 9:02 PM) 29

Tracey Maclin,
Decline of the Right of Locomotion: The Fourth Amendment on the Streets, 75 Cornell L. Rev. 1257 (1990) 26

PPSA,
A Class-Action Lawsuit Against San Francisco Details How “Vehicle Fingerprints” Are Used in the Mass Surveillance of Drivers (Jan. 5, 2026)..... 10

PPSA,
AI Drones Sharpen the Security/Privacy Tradeoff of a Surveillance State (Oct. 30, 2025) 29

PPSA,
Flock Appears to be Combining Driver Surveillance with Personal Data (Aug. 19, 2025)..... 30

PPSA,
Flock Partners with Ring–“It’s a Warrantless Day in the Neighborhood!” (Oct. 20, 2025) 29

PPSA,
How the Feds Use Our License Plates to Build Dossiers (Nov. 24, 2025) 30

PPSA,
License Plate Readers Create Vast Privacy Breach (Oct. 8, 2024) 15

PPSA,
PPSA Urges Supreme Court to Rein in Geofence Warrants (Jan. 27, 2026) 27

Nicholas Reimann,
FBI Director Subpoenaed By House GOP Over Monitoring ‘Traditionalist’ Catholics, Forbes
 (Apr. 10, 2023, 3:25 PM) 16

**INTRODUCTION, INTEREST OF *AMICUS CURIAE*
AND SOURCE OF AUTHORITY TO FILE¹**

This case presents a pair of exceptionally important Fourth Amendment questions: Can the government, consistent with the Fourth Amendment, use automatic license plate readers (“ALPR”) to systematically collect and retain data that effectively tails every passerby without reasonable suspicion? And if the government can collect and retain that data, can it search those data stores without a warrant? The history and principles underlying the Supreme Court’s Fourth Amendment caselaw compel the conclusion that this increasingly widespread practice violates the Constitution because it is incompatible with “that degree of privacy against government that existed when the Fourth Amendment was adopted.” *Carpenter v. United States*, 585 U.S. 296, 305 (2018) (citation omitted).

Unfortunately, many federal and state courts continue to treat *Carpenter* as the exception rather than the rule. The magistrate judge

¹ All parties have consented to the filing of this *amicus curiae* brief. See Fed. R. App. P. 29(a)(2). No party or counsel for a party authored this brief in whole or in part and no entity or person, aside from *amicus curiae*, its members, or its counsel, made any monetary contribution intended to fund the preparation or submission of the brief.

here refused to apply *Carpenter* and relied on the public-exposure doctrine, ignoring how *Carpenter* has constrained that approach. *See* Doc. 47 at 3–4. And the district court correctly refused to hold that “use of ALPR data could [n]ever amount to a Fourth Amendment search.” Doc. 52 at 2. But it reduced *Carpenter*’s protections to an unexpressed numerical threshold. *Id.* at 3. Not so. *Carpenter* turns on a search’s qualities—“its depth, breadth, and comprehensive reach”—not the quantity of data points at issue in an individual case.

Because of the serious privacy issues raised by automatic license-plate readers and similar mass surveillance, they are of particular concern to *Amicus* Project for Privacy and Surveillance Accountability, Inc. (“PPSA”), a nonprofit, nonpartisan organization dedicated to protecting privacy rights. *Amicus* PPSA submits this brief to urge this Court to hold that Americans have a reasonable expectation of privacy in not being continuously “tailed” by the government and in their aggregated data, and thus to ensure that Fourth Amendment rights are not left “at the mercy of advancing technology.” *Carpenter*, 585 U.S. at 305 (citation omitted).

STATEMENT OF THE ISSUES

Whether Fourth Amendment “searches” occur (1) when the government uses automated license plate readers to collect and aggregate data from all passersby without a warrant, and (2) when it retroactively queries the resulting database of aggregated data.

SUMMARY OF ARGUMENT

Warrantless collection and aggregation of data and retroactive querying of the resulting databases invades profound privacy interests that far outweigh any legitimate government need. The collection, aggregation, and search of ALPR data like that at issue here forms the “too permeating police surveillance” that is incompatible with “that degree of privacy against the government that existed when the Fourth Amendment was adopted.” *Carpenter*, 585 U.S. at 305 (citations omitted). Two core reasons compel reversal.

First, the Fourth Amendment exists to block the kind of pervasive, suspicionless surveillance the Framers despised in general warrants. *Carpenter* reaffirmed that principle: Individuals retain a reasonable expectation of privacy in the “whole of their physical movements” over time—even when individual data points are public. 585 U.S. at 310.

Yet pervasive and systematic collection and aggregation of a person’s movements turn fleeting, public glimpses into intimate, all-encompassing dossiers revealing where people sleep, work, worship, seek medical care, protest, or associate. And ALPR systems deliver precisely this power. They sweep up time-stamped, geolocated scans of *every* passing vehicle, store the data indefinitely, and let officers reconstruct detailed travel histories “with just the click of a button.” *Id.* at 311.

Here, the government mapped Slaybaugh’s movements and those of every other passerby before any alleged crime occurred. That capability dwarfs the short-term, real-time beeper tracking in *United States v. Knotts*, 460 U.S. 276 (1983)—where the Court explicitly warned that future “dragnet” technologies would demand different rules. At the Founding, no government could amass or analyze such records for its entire populace. Today, ALPR makes mass, tireless surveillance routine.

Second, Carpenter targets the qualitative danger of retrospective digital tracking—not some numerical safe harbor for data points or weeks of surveillance. The Court refused to draw duration lines and focused on the “depth, breadth, and comprehensive reach” of stored

location information and the ease of retracing a person's movements. *Carpenter*, 585 U.S. at 309–10, 320.

That is why the district court's focus on whether 72 data points over three weeks crossed an undefined "whole of movements" threshold misreads *Carpenter*. Merely plucking a subset of data points from a far more pervasive dossier of movements does not change the nature of the collection or query. Once a vast, suspicionless database exists, any query to reconstruct travel history exercises the exact retrospective power *Carpenter* forbids—turning every driver into a permanent suspect who has already been tailed for the entire retention period. That is not traditional observation; it is AI-enabled surveillance that generates suspicion rather than responds to it.

Nor is it needed. The government has ample constitutional tools to perform necessary and ordinary policing: real-time visual tailing, brief pursuits, and warrants backed by probable cause for historical data when needed. Absent exigency, warrantless ALPR queries collapse the privacy balance. This Court should reverse the denial of Slaybaugh's motion to suppress and hold that using aggregated ALPR data to retrace an individual's movements without a warrant violates the Fourth

Amendment—preserving the degree of privacy the Framers fought to secure before digital technology makes it impossible.

ARGUMENT

The decisions below rest on two related Fourth Amendment errors. First, the magistrate judge treated the visibility of a license plate on public roads as dispositive under public-exposure doctrine. Doc. 47 at 3. Then, the district judge decided that it “need not, and does not, decide whether warrantless use of ALPR data could ever amount to a Fourth Amendment search.” Doc. 52 at 2. Instead, the district court reframed the issue as one of degree, holding that this level of ALPR tracking was not extensive enough to reveal the “whole of movements” under *Carpenter*. Both approaches misread modern Fourth Amendment doctrine and historical limits on government surveillance power.

The relevant constitutional question is not whether individual plate reads occurred in public, or whether the surveillance lasted long enough to resemble a citywide dragnet. The Fourth Amendment does not turn on camera counts, mileage, or duration thresholds. The relevant constitutional question here is whether the government used surveillance technology to collect and aggregate location records, and

then retrospectively reconstruct a person's movements. ALPR database searches exercise that power.

I. The Lower Courts' Misapplication of *Carpenter* and Public-Exposure Doctrine Improperly Reduces the Fourth Amendment's Protection to Visibility and Duration Tests.

Contrary to the district and magistrate judges' approaches below, the Supreme Court has long recognized that a "search" under the Fourth Amendment is not confined to physically trespassing on a protected area. Government searches also extend to intrusions on a person's reasonable expectation of privacy. *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (citing *Katz v. United States*, 389 U.S. 347, 360–61 (1967)). And any intrusion into that privacy is presumptively unreasonable without a warrant. *See United States v. Karo*, 468 U.S. 705, 714–15 (1984); *see also Fuqua v. Turner*, 996 F.3d 1140, 1151 (11th Cir. 2021).

No government intrusion, moreover, is more offensive to the Fourth Amendment than mass, generalized searches. Indeed, British abuses of the general warrant sparked the American revolution. *Stanford v. Texas*, 379 U.S. 476, 481 (1965). And if Founding Era police dragnets sparked that strong of a response, we can only imagine how Americans of that era

would have reacted to modern surveillance with integrated camera systems linked by AI that can:

- track every American before any crime occurs,
- store and make accessible data that would have dwarfed any Founding Era conception of a library, then
- analyze that data using AI that can make connections beyond the capabilities of the human mind.

Yet these Fourth Amendment abuses have been excused under ill-fitting principles like the public exposure doctrine or a cramped reading of *Carpenter*. Correctly applied, *Carpenter* focuses courts on the nature of the government’s surveillance capability, not on the chance that any given data point was once observable in public or on whether officers monitored a suspect long enough to satisfy some unstated “dragnet” threshold.

A. The Fourth Amendment implicates *aggregated* surveillance power, not individual data points.

The district and magistrate judges’ determinations on the ALPR systems at issue both misapply *Carpenter*. In that case, the Supreme Court held that individuals retain a reasonable expectation of privacy in “the whole of their physical movements,” even though each individual movement may occur in public and be theoretically observable by

passersby or officers on the street. *Carpenter*, 585 U.S. at 310 (citing *United States v. Jones*, 565 U.S. 400, 430 (2012)); see *United States v. Davis*, 109 F.4th 1320, 1329–30 (11th Cir. 2024). The Court stressed that location records become constitutionally sensitive because, when aggregated over time, they supply an “all-encompassing record” of where a person has been, opening “an intimate window into a person’s life” by revealing all associations. *Carpenter*, 585 U.S. at 311.

1. The historical location information in *Carpenter* raised Fourth Amendment concerns not because any one cell-site ping was private in isolation, but because the state could fuse aggregated pings into a detailed, time-stamped map of Carpenter’s movements. ALPR systems serve the same function. Each plate scan is a discrete observation of a car on a public road, little different than an individual cell-site ping. But in contrast to the cellphone company’s collection of data in *Carpenter*, the data collected from ALPR is intended solely for surveillance. Instead of querying a third-party’s database of location data used to enable cellphone communication, the government contracts with companies to build its own surveillance network and database. The plate

scans systematically collected and stored in those databases catalogue the movements of every passerby, without any suspicion.

In 2019 alone, moreover, 1 billion license plate scans were collected, with 99.9% not actively related to any criminal investigation.² The ALPR system that collected Slaybaugh’s information, Flock, works by creating a “vehicle fingerprint” that includes much more than just a license plate number.³ Each passing vehicle’s “fingerprint” includes its color, make, model, and distinctive features, like a political bumper sticker. Flock then provides advanced search and artificial intelligence functions that can be used to list locations a car has been captured, create lists of cars that have visited specific locations, and even track cars that are seen together.⁴ Thus, this “ALPR data” contains much more than just license

² PPSA, *A Class-Action Lawsuit Against San Francisco Details How “Vehicle Fingerprints” Are Used in the Mass Surveillance of Drivers* (Jan. 5, 2026), <https://tinyurl.com/45p9rtea>.

³ Flock data is not available to the general public and is provided to law enforcement on a paid contractual basis. Doc. 31 at 3–4 (citing Flock Safety, *License Plate Readers (LPR)* (last accessed June 12, 2025), <https://tinyurl.com/y5pyyp36>; see also Flock Safety, *Privacy & Ethics* (last accessed Feb. 13, 2026), <https://tinyurl.com/ms7br648> (“[I]n no case is law enforcement data accessible to private customers.”). As such, Flock acts as a state actor for Fourth Amendment purposes.

⁴ PPSA, *A Class-Action Lawsuit*, *supra* note 2.

plate numbers and allows the creation of an intimate map for every American. And those individualized maps emerge from prolonged suspicionless aggregation of data. The type of device (vehicle or phone) used to create it is simply irrelevant for Fourth Amendment purposes.

The map of Slaybaugh's movements created from aggregated ALPR data is precisely the type of all-encompassing record that *Carpenter* prohibits. The 72 images discussed by the district court were only the results of the government's *query*. The fact that 72 images were retrieved says nothing about the size of the surveillance database the government was searching. That database let officers retrace the "location, direction, and route of Slaybaugh's truck" for the three weeks they happened to request. Doc. 47 at 2. They could easily have requested a much longer period.

Even the existing three-week log, however, was extensive enough to suggest to law enforcement that Slaybaugh had changed residences. *Id.* And the unspoken constitutional issue here is that the officers knew the location, direction, and route of *every* passerby, not just the one who would later be charged with a crime.

The Founders would have been alarmed by such dragnet surveillance. And that's why they drafted the Fourth Amendment to "place obstacles in the way of a too permeating police surveillance." *Carpenter*, 585 U.S. at 305 (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)). They were not merely concerned with the rights of the specific defendant who comes into the government's crosshairs as a criminal suspect.

Here, moreover, the fact that law enforcement tracked Slaybaugh's vehicle instead of his cell phone is inconsequential. The critical fact is that officers were able to create a complete, long-term picture of Slaybaugh's movements along public roads. In the same way that escape from this type of "tireless and absolute surveillance" was possible for the "few without cell phones," Slaybaugh and every other passerby could only have avoided this tracking by avoiding driving on public roads. *See Carpenter*, 585 U.S. at 312. But the Fourth Amendment is not concerned with only protecting privacy for the few who opt out of society. *Id.* It is meant to preserve "that degree of privacy against government that existed when the Fourth Amendment was adopted." *Id.* at 305.

2. The suspicionless collection and aggregation of data that ALPR provides flunks that requirement because it makes possible an overly revealing map of a person's location that is at odds with traditional public observation. *See, e.g., Oliver v. United States*, 466 U.S. 170 (1984) (single group of officers did not need warrant to conduct a single search of a public field that contained marijuana). *Knotts* is instructive here. In that case, tracking vehicles using rudimentary beepers to assist officers in following a single trip on public roads was deemed not a search because the beeper merely aided what officers could have done through visual surveillance. *Knotts*, 460 U.S. at 285. Even then, the Supreme Court foresaw the time when “dragnet type law enforcement practices” might “eventually occur,” but left for another day “whether “twenty-four hour surveillance of any citizen” made possible by technology would trigger “different constitutional principles.” *Id.* at 284.

Later, in *Carpenter*, when the Supreme Court addressed suspicionless, aggregated surveillance, it held that a person “does not surrender all Fourth Amendment protection by venturing into the public sphere.” *Carpenter*, 585 U.S. at 310. So, “what one seeks to preserve as private, even in an area accessible to the public, may be constitutionally

protected,” particularly when digital tools enable the state to compile and analyze a comprehensive dossier of public movements over time. *Id.* (quoting *Katz*, 389 U.S. at 351–52).

The Supreme Court thus squarely rejected the notion that the state may freely aggregate public-facing data into an all-encompassing travel log simply because each observation was, at the moment it occurred, theoretically public. *Id.* at 313. Although “a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements *from one place to another*,” *id.* at 306 (emphasis added) (quoting *Knotts*, 460 U.S. at 281), secretly monitoring “*every movement*’ a person makes in [a] vehicle ... impinges on expectations of privacy’—regardless whether those movements were disclosed to the public at large,” *id.* at 307 (citing *Jones*, 565 U.S. at 430 (Alito, J., concurring)).

In essence, the Court held that public observation is permissible in single instances by single officers, but long-term aggregated surveillance does not align with standard public observation. Instead, the Fourth Amendment recognizes a reasonable expectation of privacy in the pattern

formed by those data points when collected, stored, and later queried by the government. *Id.*

3. That principle is directly implicated by ALPR systems as they convert fleeting, isolated exposures of a plate on public roads into a structured, searchable database. ALPR systems automatically: (a) scan every passing plate, (b) time-stamp and geolocate each read, and (c) store data in searchable archives that enable retrospective reconstruction of movement. This database has the capacity to reveal where a person sleeps, works, worships, seeks medical or political counseling, and with whom he regularly associates. *Id.* at 311. Indeed, reports show that ALPR by its very nature collects and stores political or religious messages displayed on cars, nearby homes, or passersby.⁵ One report showed that users could query an ALPR database to reveal “a bright red ‘Trump’ campaign sign placed in front of someone’s garage” in Alabama with “a banner referencing Israel.”⁶

⁵ PPSA, *License Plate Readers Create Vast Privacy Breach* (Oct. 8, 2024), <https://tinyurl.com/jbxt52j>.

⁶ Matt Burgess & Dhruv Mehrotra, *License Plate Readers Are Creating a US-Wide Database of More Than Just Cars*, *Wired* (Oct. 3, 2024, 6:38 AM), <https://tinyurl.com/bdzmkejb>.

If the Fourth Amendment does not apply to ALPR surveillance, nothing but personal restraint or lack of imagination prevents the government from using ALPR to locate every American with a Catholic bumper sticker or a Planned Parenthood sticker. And if integrated with doorbell cameras, the search can be extended to yard signs and pedestrian clothes. Personal restraint is small comfort after the government surveilled traditionalist Catholics, gun owners, and even parents who opposed mask mandates in schools.⁷ The capacity to conduct this surveillance matters under the Constitution, and in our digital age, it matters more than ever if we are to preserve that degree of privacy that the Founders intended to preserve for us.

In short, when the ALPR system here showed law enforcement “the whole of [Slaybaugh’s] movement,” it did something that the government could not have done through traditional public observation—and would not have obtained until he became an active suspect and the government had probable cause for a warrant. *Carpenter*, 585 U.S. at 311. Indeed,

⁷ Nicholas Reimann, *FBI Director Subpoenaed By House GOP Over Monitoring ‘Traditionalist’ Catholics*, *Forbes* (Apr. 10, 2023, 3:25 PM), <https://tinyurl.com/36n9rrsb>; Tyler Arnold, *FBI Used Undercover Agent To Investigate Catholics, Says Weaponization Committee Chairman*, *EWTN News* (Apr. 11, 2023, 3:30 PM), <https://tinyurl.com/2b5ukuxy>.

“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.” *Id.* at 310. When the government collects and aggregates data—whether cell phone location data or ALPR—it conducts a search that is subject to a warrant requirement.

B. *Carpenter* regulates retrospective surveillance power; it does not set a numerical or scale-based threshold.

The suspicionless collection and aggregation of data is only half of the twin Fourth Amendment violation that ALPR presents. The Court’s preeminent concern in *Carpenter* was that cell-phone data was used to “retrace a person’s whereabouts,” create “a detailed log of [a person’s] movements,” and “access each [person]’s deep repository of historical location information.” 585 U.S. at 311–12. There, the Court did not set a numerical or scale-based threshold for surveillance. Instead, it is a search’s qualities that define its constitutionality, not the quantity of data points collected or later accessed.

As discussed above, ALPR systematically collects the data of every passerby before any crime has been committed, let alone before suspicion attaches to any particular suspect. Then, *after* a crime is committed, the

government goes back and searches that database for the person’s vehicle that they tailed (along with every other vehicle).

That approach itself violates *Carpenter*. But the district court instead focused on whether accessing 72 reads over three weeks—from a database containing a vastly larger aggregation of reads on Slaybaugh and everyone else—did or did not reveal Slaybaugh’s “whole of movements.” Doc. 52 at 3. The district court thus misread *Carpenter* as a case about quantitative cutoffs instead of collecting and aggregating data and retrospective digital tracking. *Id.* Yet in *Carpenter*, the Supreme Court expressly declined to define any safe-harbor period of historical location data free from Fourth Amendment scrutiny. 585 U.S. at 309–10. Instead, the Court held only that accessing seven days of such records constitutes a search and left open whether shorter intervals might also qualify. *Id.* at 310 n.3.

Thus, far from announcing duration quotas or a dragnet threshold, the Supreme Court rooted its holding in the “depth, breadth, and comprehensive reach” of the data and in the state’s ability, with “just the click of a button,” to consult a “deep repository of historical location information” and retrospectively reconstruct a person’s whereabouts

subject only to retention policies. *Id.* at 311, 320. Based on those criteria, the constitutional breach arises from the government’s power to “travel back in time” and “retrac[e] a person’s whereabouts” from a stored database of location records. *Id.* at 312. When the government reviews aggregated data in that manner, “whoever the suspect turns out to be, he has effectively been tailed every moment of every day” for as long as the records are kept. *Id.* at 312. So too here. The Supreme Court’s reasoning in *Carpenter* transfers directly to ALPR databases.

These ALPR systems allow the government to build and retain a reservoir of time-stamped plate-location records, and then later search that archive to reconstruct a suspect’s travel history. This unconstitutional retrospective surveillance power is regulated by *Carpenter* and exists regardless of whether the resulting log from a particular query spans three days, three months, or three years.

Therefore, when the presence or absence of a particular numeric threshold is treated as dispositive, it disregards *Carpenter*’s warning that Fourth Amendment rules must account for “more sophisticated systems that are already in use or in development” and the ease and efficiency with which modern systems enable retrospective tracking. *Id.* at 313

(quoting *Kyllo*, 533 U.S. at 36). This approach, which the district court followed below, resembles the proverbial boiling frog. Even if the systematic mass surveillance of America is here, the situation is just not *quite* bad enough for the courts to be concerned. But the “I’ll know it when I see it” approach to mass surveillance may come too little, too late, if it ever comes at all.

Instead of waiting for a constitutional tipping point that never seems to arrive, this Court should hold that the very nature of ALPR systems’ suspicionless collection, aggregation, and retrospective search capability cannot be squared with *Carpenter* and distinguishes ALPR from constitutionally permissible public observation and investigation. These capabilities allow officers to retrace a person’s steps over an extended period, whereas traditional public observation was limited to individual officers at specific instances. So with ALPR, the detective need not trace the clues from the scene of the crime to the suspect; his AI-enabled surveillance has already traced every person who passed through that scene. The detective just needs to pick which ones he wants to investigate. And he does so without the check of a warrant application

to temper any investigative abuse. Instead of using technology to *investigate* suspicion, he uses it to *generate* suspicion.

Accordingly, allowing warrantless use of ALPR systems and the aggregated data they provide substantially departs from tradition and allows officers to create the type of complete, retroactive map—“near perfect surveillance”—that *Carpenter* prohibits. *See Carpenter*, 585 U.S. at 311–12. In short, what matters for the Fourth Amendment is the state’s use of technology to convert innumerable public-facing moments into a searchable log of a person’s life, not the innocuous nature of any single data point taken alone. And with that database, it is not a matter of if its data will be abused or misused, only a matter of when and by whom.

II. ALPR Radically Departs from Founding Era Understandings of Privacy and Threatens Intrusions Far Worse than General Warrants.

These characteristics of ALPR—suspicionless collection and aggregation of data and its retroactive analysis—are unconstitutional searches that break from traditional Fourth Amendment understandings that protect privacy and the right to travel without undue government intervention. Under that original understanding, the systematic long-

term tracking of every American without suspicion far exceeds the intolerable general warrants that the Founding generation declared to be “the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law book.” *John Adams’s Reconstruction of Otis’s Speech in the Writs of Assistance Case*, in *Collected Political Writings of James Otis* 11, 11 (Richard A. Samuelson ed., Liberty Fund 2015), <https://tinyurl.com/2zhmukac>.

ALPR systems are of a kind with those hated general warrants. For purposes of *defining* a Fourth Amendment “search,” whether the government rummages through all your papers *after* you come under suspicion or collects them all through mass surveillance and then rummages through them *before* you come under suspicion, the intrusion is the same or worse. And *both* are properly deemed Fourth Amendment “searches.”

A. ALPR is a radical departure from historical privacy understandings and threatens everyday freedoms.

The district court’s contrary decision to allow warrantless ALPR use grants officers substantially more surveillance power than law enforcement would have had at the Founding. *See Kyllo*, 533 U.S. at 34.

This scale of long-term tracking of every suspect would have been impractical at the Founding, to say nothing of the suspicionless long-term tracking of every American. When the Fourth Amendment was ratified, the government did not have the capacity to record and retroactively reconstruct a person's movements. And the Founders respected the right to travel without undue government intrusion. ALPR technology, however, is a radical departure from historic policing that threatens to undermine everyday privacy and the freedom of travel.

By restricting the government to historic understandings of ordinary policing, of course, no one is suggesting that modern police remain limited to Founding Era technology while modern criminals have no such limitations. To the contrary, the police can use new and emerging technologies to make reasonable searches and seizures, so long as they obtain a warrant from a neutral judge, as the Founders intended.

Until that constitutional blessing occurs, however, ALPR-based tracking is a warrantless search that remains “presumptively unconstitutional.” *Kyllo*, 533 U.S. at 32. To allow ALPR to remain outside the warrant requirement “would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment.” *Id.* at 34. ALPR

creates a permanent, aggregated record of a person’s geolocated and time-stamped locations, along with other identifying details. Each data point exponentially increases the ability of AI to piece together the “near perfect surveillance” that *Carpenter* prohibits. *See Carpenter*, 585 U.S. at 311–12. This aggregation stands in stark contrast to the “dearth of records” available at the Founding. *Id.* at 312. And any historic attempt to reconstruct a person’s movements would have been limited by the “frailties of recollection.” *Id.* The government simply could not physically store the amount of information that it would take to mass surveil an entire city, let alone the entire country.

In contrast, here ALPR let the government reconstruct “the location, direction, and route of Slaybaugh’s truck ... for three weeks,” Doc. 47 at 2, or three months, or three years, if they so desired. This retrospective capability gives “police access to a category of information otherwise unknowable.” *Carpenter*, 585 U.S. at 312. This category of information is traditionally unknowable because it would have required officers to anticipate its need and then pursue a subject for weeks. And that type of long-term pursuit was “difficult and costly and therefore rarely undertaken,” and only if the need for that search was reasonable

enough to justify the cost. *Id.* at 311 (quotation omitted). Yet here, retrospective long-term pursuit was used to determine whether a single person had changed residences but failed to register as a sex offender at his new address, a crime for which Slaybaugh was sentenced to twelve months and a day's imprisonment. Doc. 78.

Such disproportionate deployment of advanced surveillance underscores how far technology has diverged from Founding-era understandings of the Fourth Amendment. No exigency existed here, and a warrant could have been obtained. At the time of the Founding, perhaps only Jeremy Bentham imagined this pervasive level and degree of surveillance. His “Panopticon” was an imagined prison where all inmates would be subject to 24-hour surveillance by an unseen observer. *See* Jeremy Bentham, *Panopticon, or the Inspection House* (1791). But he never suggested such pervasive surveillance for free persons going about their everyday life. ALPR data places drivers “at the mercy of advancing technology,” subjecting them to the quality of surveillance that would have been inaccessible when the Fourth Amendment was written. *Kyllo*, 533 U.S. at 35.

Moreover, this surveillance involving warrantless collection, aggregation, and querying of ALPR data threatens the long-held freedom to travel without unreasonable government intrusion. Tracey Maclin, *Decline of the Right of Locomotion: The Fourth Amendment on the Streets*, 75 Cornell L. Rev. 1257, 1260 (1990). This freedom to travel is “one of the ‘cherished liberties that distinguish this nation from so many others.’” *Id.* at 1259.

Although this cherished liberty protects the right to physically move through public space and be protected from unreasonable search, pervasive ALPR collection makes it virtually impossible to move through any public space without that movement being recorded, time-stamped, and stored. ALPR data effectively requires the public to trade in their privacy rights to enjoy their right to movement—an unconstitutional condition on public access to the public’s roads. With ALPR data, the government can “search” travel in new ways that were unimaginable at the Founding or in the decades since. To prevent officers from intruding on the freedom to travel and “that degree of privacy against the government that existed when the Fourth Amendment was adopted,”

Carpenter, 585 U.S. at 305 (citations omitted), warrantless access to ALPR data must be held unconstitutional under the Fourth Amendment.

B. The district court’s rule invites expansive future surveillance.

By contrast, legitimizing retroactive, long-term, and aggregated surveillance, as the district court did here, invites unreasonable, warrantless surveillance. If courts permit the warrantless retention and querying of retrospective location data because each individual exposure was public, they authorize mass catalogs of movement, searches of entire populations’ historical data, and real-time linking across databases. This type of “tireless and absolute surveillance” is exactly the type of search prohibited in *Carpenter*. *Carpenter*, 585 U.S. at 312.

And ALPR is just the tip of the surveillance iceberg.

The Supreme Court is poised to hear argument this Term in a mass surveillance case involving geofence warrants. *See Chatrie v. United States*, No. 25-112, 2026 WL 120676 (U.S. Jan. 16, 2026). Like ALPR, geofence warrants involve suspicionless, pervasive data collection and retrospective searches.⁸ These so-called “reverse warrants” to identify

⁸ PPSA, *PPSA Urges Supreme Court to Rein in Geofence Warrants* (Jan. 27, 2026), <https://tinyurl.com/4rdbdzk9>.

potential suspects in a crime are not limited to location data. Far from it. The government has used other forms of these “reverse search warrants” to extract other private data, such as identifying anyone who has searched for a specific phrase, *Commonwealth v. Kurtz*, 348 A.3d 133, 138 (Pa. 2025) (government obtained list of every person to Google a specific address where an unsolved rape occurred), or forcing commercial genealogy companies to allow access to their DNA databases.⁹ These broad uses of surveillance will almost certainly lead to a variety of novel contexts, such as tracking political protests, that could implicate Americans’ rights to free speech and freedom of assembly.

Those surveillance techniques do not exist in isolation and are being combined with technologies like ALPR. For ALPR, as with most surveillance technologies, the greatest issue is not the technology itself (although for ALPR, that issue is severe enough), but rather how it is used in a network. Indeed, the Flock company that provided the ALPR surveillance of Slaybaugh has become notorious for its attempts to

⁹ Jocelyn Kaiser, *A Judge Said Police Can Search the DNA of 1 Million Americans Without Their Consent. What’s Next?* Science (Nov. 7, 2019), <https://tinyurl.com/28bxdrns>.

integrate its technology in ever-expanding webs of intrusive data aggregation and retrospective searches.

Recently, Flock partnered with Amazon's Ring to merge data from ALPR with neighborhood video footage from doorbells.¹⁰ And internal Amazon documents show an appetite to integrate artificial intelligence—including, perhaps, video analytics and facial recognition software—into Ring, and by extension, Flock. Those rumors became reality when Ring decided to unveil its AI integration to the American public during the 2026 Super Bowl. The bipartisan blowback showed that Americans and Alabamians like those surveilled here are unsettled with this level of pervasive, dystopian surveillance.¹¹ And Flock is not content to keep its eyes on the streets. It is now also helping police departments take to the skies by enhancing their drone fleets with artificial intelligence.¹² Again,

¹⁰ PPSA, *Flock Partners with Ring—“It’s a Warrantless Day in the Neighborhood!”* (Oct. 20, 2025), <https://tinyurl.com/57re9hfr>.

¹¹ Ahmad Austin Jr., *‘Dystopian’ Super Bowl Ad for Ring Camera Gets Bipartisan Blowback: ‘Propaganda for Mass Surveillance,’* Mediaite (Feb. 9, 2026, 11:05 AM), <https://tinyurl.com/4behp38v>; Kelly Kazek, *‘Terrifying’ Super Bowl Commercial Has People Vowing To Never Buy This Popular Product,* AL.com (Feb. 10, 2026, 9:02 PM), <https://tinyurl.com/y8z72w2w>.

¹² PPSA, *AI Drones Sharpen the Security/Privacy Tradeoff of a Surveillance State* (Oct. 30, 2025), <https://tinyurl.com/yc8x4kar>.

these cameras will all be integrated into the same emerging mass surveillance ecosystem.

That surveillance ecosystem is not limited to just location data. Flock is mashing up its camera surveillance with digital information gathered on Americans by data brokers.¹³ For now, Flock says it has decided not to include stolen dark web data in its network. But only time will tell if that policy remains in place.¹⁴ And the federal government itself is using an app that allows an officer to photograph a license plate, run it through commercial platforms like Flock and instantly retrieve that vehicle's historical sightings. That app also pull ups the vehicle's travel history, ownership records, and associated personal data.¹⁵

This expansive, warrantless data surveillance is not necessary for ordinary policing. Our country has existed for centuries without it. Even with a warrant requirement, law enforcement can still “pursue[] a suspect for a brief stretch.” *Carpenter*, 585 U.S. at 310. And, with a

¹³ PPSA, *Flock Appears to be Combining Driver Surveillance with Personal Data* (Aug. 19, 2025), <https://tinyurl.com/3mw4cu8j>.

¹⁴ *Id.*

¹⁵ PPSA, *How the Feds Use Our License Plates to Build Dossiers* (Nov. 24, 2025), <https://tinyurl.com/ycxm2eu8>.

warrant based on probable cause, a compilation of historical ALPR data is still available. No exigent circumstances existed here where police officers needed to determine Slaybaugh's location and the use of ALPR data without a warrant *might* have been reasonable, *i.e.*, a kidnapping or Amber alert. It was merely a matter of convenience.

The Fourth Amendment does not prevent the government from collecting, storing, and accessing aggregated data. It just needs to articulate individualized probable cause before a neutral judge. That standard is not too high a price to pay to retain the degree of freedom that the Founders intended us to possess when they drafted the Fourth Amendment.

CONCLUSION

This Court should reverse the denial of Slaybaugh's motion to suppress. This case is not just about the threat of surveillance for anybody who dares drive on a public road—as if that were not enough—it goes to the very heart of what kind of society we are going to live in. And if we are to preserve “that degree of privacy against government that existed when the Fourth Amendment was adopted,” *Carpenter*, 585 U.S. at 305 (citation omitted), the Court should prohibit the warrantless use

of aggregated ALPR data—especially now, as artificial intelligence becomes powerful enough to piece together intimate information from seemingly innocuous details about a target’s life and turn the erosion of Americans’ privacy into a total collapse.

Dated: February 13, 2026

Respectfully submitted,

/s/ Gene C. Schaerr

GENE C. SCHAERR

ERIK S. JAFFE

JUSTIN A. MILLER

SCHAERR | JAFFE LLP

1717 K Street NW, Suite 900

Washington, DC 20006

Telephone: (202) 787-1060

gschaerr@schaerr-jaffe.com

ejaaffe@schaerr-jaffe.com

jmiller@schaerr-jaffe.com

Counsel for Amicus Curiae

CERTIFICATE OF COMPLIANCE

The foregoing Brief of Project for Privacy and Surveillance Accountability, Inc. as *Amicus Curiae* in Support of Appellant complies with the type-volume limit of Fed. R. App. P. 29(a)(5), because, excluding the parts of the document exempted by Fed. R. App. P. 32(f), this document contains 5,971 words.

This brief also complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Century Schoolbook font.

/s/ Gene C. Schaerr
Gene C. Schaerr

Dated: February 13, 2026