Case No. 26-1227

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

LEE SCHMIDT; CRYSTAL ARRINGTON,

Plaintiffs - Appellants,

v.

CITY OF NORFOLK; MARK TALBOT, In his official capacity as the Norfolk Chief of Police,

Defendants - Appellees.

BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION, AND AMERICAN CIVIL LIBERTIES UNION OF VIRGINIA IN SUPPORT OF PLAINTIFFS - APPELLANTS AND REVERSAL

On Appeal from the United States District Court
for the Eastern District of Virginia at Norfolk
Case No. 2:24-cv-00621-MSD-RJK
Hon. Mark S. Davis

Brett Max Kaufman
Nathan Freed Wessler
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
bkaufman@aclu.org

Elizabeth Femia
Andrew Crocker
Jennifer Pinsof
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
lfemia@eff.org

Matthew William Callahan
ACLU FOUNDATION OF VIRGINIA
PO Box 26464
Richmond, VA 23261-6464
(804) 523-2146
mcallahan@acluva.org

Counsel for Amici Curiae

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

DISCLOSURE STATEMENT

- In civil, agency, bankruptcy, and mandamus cases, a disclosure statement must be filed by **all** parties, with the following exceptions: (1) the United States is not required to file a disclosure statement; (2) an indigent party is not required to file a disclosure statement; and (3) a state or local government is not required to file a disclosure statement in pro se cases. (All parties to the action in the district court are considered parties to a mandamus case.)
- In criminal and post-conviction cases, a corporate defendant must file a disclosure statement.
- In criminal cases, the United States must file a disclosure statement if there was an organizational victim of the alleged criminal activity. (See question 7.)
- Any corporate amicus curiae must file a disclosure statement.
- Counsel has a continuing duty to update the disclosure statement.

No. 26-1227 Caption: Lee Schmidt, Crystal Arrington v. City of Norfolk; Mark Talbot, In his official capacity as the Norfolk Chief of Police

Pursuant to FRAP 26.1 and Local Rule 26.1,

Electronic Frontier Foundation, American Civil Liberties Union, and
(name of party/amicus)

American Civil Liberties Union of Virginia

who is amici curiae, makes the following disclosure:
(appellant/appellee/petitioner/respondent/amicus/intervenor)

1. Is party/amicus a publicly held corporation or other publicly held entity? ☐ YES ☑ NO

2. Does party/amicus have any parent corporations? ☐ YES ☑ NO
If yes, identify all parent corporations, including all generations of parent corporations:

3. Is 10% or more of the stock of a party/amicus owned by a publicly held corporation or other publicly held entity? ☐ YES ☑ NO
If yes, identify all such owners:

4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation? ☐YES ☑NO
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question) ☐YES ☐NO
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding? ☐YES ☑NO
If yes, the debtor, the trustee, or the appellant (if neither the debtor nor the trustee is a party) must list (1) the members of any creditors' committee, (2) each debtor (if not in the caption), and (3) if a debtor is a corporation, the parent corporation and any publicly held corporation that owns 10% or more of the stock of the debtor.

7. Is this a criminal case in which there was an organizational victim? ☐YES ☑NO
If yes, the United States, absent good cause shown, must list (1) each organizational victim of the criminal activity and (2) if an organizational victim is a corporation, the parent corporation and any publicly held corporation that owns 10% or more of the stock of victim, to the extent that information can be obtained through due diligence.

Signature: /s/ Brett Max Kaufman Date: 04/20/2026

Counsel for: Amici Curiae

Print to PDF for Filing

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

STATEMENT OF INTEREST 1

INTRODUCTION AND SUMMARY OF ARGUMENT 2

ARGUMENT 4

I. Even "Local" ALPR Systems Are Part of a Vast, Interconnected Network That Collects Massive Amounts of Detailed Data With Little Oversight 4

A. ALPRs Are Increasingly Ubiquitous, Automatically and Indiscriminately Collecting a Significant Amount of Data, Including Precise Location Data 4

B. Police Have Real-Time Access to ALPR Data with Few Restrictions on Use and Little Oversight 8

C. ALPR Data Can Be Automatically and Continuously Shared Across Jurisdictions, Including Through Sprawling Statewide and Nationwide Sharing Networks 12

D. Because ALPR Location Data Can Reveal Detailed Private and Personal Details About Individuals, It is Increasingly Used to Surveil Politically Vulnerable Groups 19

II. ALPR Systems Provide the Government with Unprecedented Powers of Surveillance that Upset Traditional Expectations of Privacy 23

CONCLUSION 28

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS 30

CERTIFICATE OF SERVICE 31

TABLE OF AUTHORITIES

Cases

Boyd v. United States,
116 U.S. 616 (1886).....24

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

Commonwealth v. McCarthy,
142 N.E.3d 1090 (Mass. 2020).....7

Katz v. United States,
389 U.S. 347 (1967).....24

Kyllo v. United States,
533 U.S. 27 (2001)..... 23, 24

Leaders of a Beautiful Struggle v. Baltimore Police Department,
2 F.4th 330 (4th Cir. 2021) ..... *passim*

Riley v. California,
573 U.S. 373 (2014).....1, 24

Schmidt v. Norfolk,
No. 2:24CV621, 2026 WL 207513 (E.D. Va. Jan. 27, 2026) 23, 27

United States v. Chatrie,
136 F.4th 100 (4th Cir. 2025) 27

United States v. Jones,
565 U.S. 400 (2012)..... 2, 24, 26, 28

United States v. Karo,
468 U.S. 705 (1984).....24

United States v. Martin,
753 F. Supp. 3d 454 (E.D. Va. 2024) 14

Statutes

Cal. Civ. Code § 1798.90 16

Va. Code Ann. § 2.2-5517 ..... *passim*

Other Authorities

Abigail Velez, *Flock CEO Responds to Austin Backlash as City Contract Nears Expiration*, CBS Austin (June 20, 2025), https://perma.cc/3ERP-QBMP 6

Alex Roever, *Report Reveals Virginia Police Misuse of License Plate Reader Technology*, WRIC (Mar. 2, 2026), https://www.wric.com/news/virginia-news/report-reveals-virginia-police-misuse-of-license-plate-reader-technology/ 16

Ángel Diaz & Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, Brennan Ctr. (Sept. 10, 2020), https://perma.cc/47KL-DVA8 6

Ben Miller, *Flock Safety Gives Users Expanded Vehicle Location Abilities*, Gov't Tech. (Sept. 1, 2025), https://perma.cc/DUS6-GV7X 20

Brian Kerhin, *Menasha Officer Pleads Not Guilty to Misconduct Charge Over Ex-girlfriend Tracking*, Fox11 News (Feb. 10, 2026), https://tinyurl.com/yj4ywctm 11

Cianna Morales, *Norfolk, Va.'s Flock Cameras Spark Privacy Debate*, Gov't Tech. (June 20, 2023), https://perma.cc/2ENS-NFDK 5, 13

Data Sharing, Motorola Sols. (Dec. 16, 2025), https://perma.cc/T6SL-4V48 13

Dave Maass & Rindala Alajaji, *How Cops Are Using Flock Safety's ALPR Network to Surveil Protesters and Activists*, EFF (Nov. 20, 2025), https://perma.cc/WCL4-7C7R 22

Dustin Dorsey, *Santa Clara County to Stop Using Flock Safety Cameras in Several Cities After Privacy Concerns*, ABC 7 News (Feb. 25, 2026), https://perma.cc/V5AA-W49Z 13

Emily Margaretten & Zoe Morgan, *Mountain View Police Turn Off License Plate Cameras After Data Sharing Breach*, Mountain View Voice (Feb. 2, 2026), https://perma.cc/FR6Y-J72D.....17

Evidence at Scale: 6 Benefits of LPR For Law Enforcement, Flock Safety (Nov. 21, 2023), https://perma.cc/SE8N-HYMY.....8

FAQS – ALPR, Axon, https://perma.cc/WPB7-DR96.....13

Flock Freeform, Flock Safety, https://perma.cc/LPT8-5JBT.....8

Flock Implements Enhanced Guardrails Across California to Ensure Lawful and Responsible Use of LPRs, Flock Safety (Mar. 2, 2026), https://perma.cc/A8QQ-SHYF.....17

Flock Safety Launches New AI-powered Tools to Accelerate Police Investigations, Police1 (Feb. 19, 2025), https://perma.cc/6YPQ-JA8H.....8

Gideon Epstein, *Flock Gives Law Enforcement All Over the Country Access to Your Location*, ACLU Mass. Data for Just. Project (Oct. 7, 2025), https://perma.cc/7XRJ-C6KR.....5

Initial Privacy Impact Assessment for Automated License Plate Reader Technology, N. Cal. Reg'l Intel. Ctr., https://perma.cc/42MC-ELWJ.....20

Introducing, Flock's National and Statewide Law Enforcement Search Network, Flock Safety (Aug. 18, 2020), https://perma.cc/4Z4W-CCMC... 12, 13

Jason Koebler & Joseph Cox, *ICE Taps into Nationwide AI-Enabled Camera Network, Data Shows*, 404Media (May 27, 2025), https://www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data-shows/.....21

Jason Koebler, *Home Depot and Lowe's Share Data From Hundreds of AI Cameras With Cops*, 404Media (Aug. 6, 2025), https://www.404media.co/home-depot-and-lowes-share-data-from-hundreds-of-ai-cameras-with-cops/..... 12, 14

Jason Koebler, *Police Told to Be "As Vague as Permissible" About Why They Use Flock*, 404Media (Jan. 27, 2026),

https://www.404media.co/police-told-to-be-as-vague-as-permissible-about-why-they-use-flock/ 11

Jason Koebler, *Wildlife Conservation Police Are Searching Thousands of Flock Cameras for ICE*, 404 Media, (Apr. 6, 2026), https://perma.cc/5LXV-A48L 21

Jay Stanley, *Kansas Town Uses License Plate Readers to Go After Man Who Wrote Op-Ed*, ACLU (Feb. 3, 2026), https://perma.cc/6UPF-DA6X 11

Jennifer Pinsof, *EFF, ACLU to SFPD: Stop Illegally Sharing Data With ICE and Anti-Abortion States*, EFF (Sept. 18, 2025), https://perma.cc/6KMG-YWJZ 16

Joseph Cox & Jason Koebler, *A Texas Cop Searched License Plate Cameras Nationwide for a Woman Who Got an Abortion*, 404Media (May 29, 2025), https://www.404media.co/a-texas-cop-searched-license-plate-cameras-nationwide-for-a-woman-who-got-an-abortion/ 15, 22

Kunle Falayi, *One Sleepy Virginia Town. Nearly 7 Million Hits On Its Surveillance Network*, Va. Ctr. For Investigative Journalism (Sept. 16, 2025), https://perma.cc/LB4W-5V23 18

Kunle Falayi, *Virginia Surveillance Network Tapped Thousands of Times for Immigration Cases*, VPM News (Oct. 9, 2025), https://www.vpm.org/news/2025-10-09/flock-safety-cameras-alprs-federal-immigration-enforcement-lehmann-kochis 10, 21

Leaving the Door Wide Open: Flock Surveillance Systems Expose Washington Data to Immigration Enforcement, Univ. of Wash. Ctr. For Hum. Rts. (Oct. 21, 2025), https://perma.cc/85XY-8265 ..... 13, 21

License Plate Readers (LPR), Flock Safety, https://perma.cc/8NPB-DKT7 13

Matthew Rodriguez, *Flock License Plate Readers Shared Data With Out-of-state Agencies*, *Ventura County Audit Finds*, CBS (Feb. 27, 2026), https://perma.cc/G4EC-3HT2 17

NACDL Fourth Amend. Ctr., *ALPR Primer*, https://perma.cc/6W6D-WVPM 7

National LPR Network, Flock Safety, https://perma.cc/UMZ5-99YV ..... *passim*

Norfolk VA PD, Flock Transparency Portal (Mar. 31, 2026), available at https://www.eff.org/document/norfolk-va-pd-flock-transparency-portal-3312026.....6

Norfolk, DeFlock, https://deflock.org/map#map=12/36.849370/-76.289954/norfolk%2520virginia.....5

Not All License Plate Readers are Equal: When Plate Data Fails, How Do Investigations Continue?, Flock Safety (Feb. 6, 2026), https://perma.cc/3TKC-LH7W 8

Press Release, Cal. Off. of Att'y Gen., Attorney General Bonta Continues Legal Challenge to Stop El Cajon from Illegally Sharing License Plate Data (Jan. 21, 2026), https://perma.cc/4NMX-8ZH2 17

Press Release, Off. of Sec'y State, Giannoulias Cracks Down on Unlawful Use of License Plate Reader Data (June 12, 2025), https://perma.cc/FZ28-CLQK.....22

Privacy Impact Assessment Report for the Utilization of License Plate Readers, Int'l Ass'n of Chiefs of Police (Sept. 2009), https://perma.cc/Y3RS-AM44 23

Rindala Alajaji & Dave Maass, *License Plate Surveillance Logs Reveal Racist Policing Against Romani People,* EFF (Nov. 3, 2025), https://perma.cc/G8PB-PDJF.....12

Solving Cross-Jurisdictional Crime in Real Time: How Flock Safety's Unified Platform Makes It Possible, Flock Safety (May 28, 2025), https://perma.cc/4JBN-RY6L 7

State of N.J., *Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data* (Dec. 3, 2010), https://perma.cc/72PK-NY2L 19

Steve Connor, *Surveillance UK: Why This Revolution Is Only the Start*, The Independent (Dec. 22, 2005), https://perma.cc/GJU3-XXDA 19

Thomas Brewster, *America's Biggest Mall Owner Is Sharing AI Surveillance Feeds Directly With Cops*, Forbes (May 6, 2024) https://www.forbes.com/sites/thomasbrewster/2024/05/06/simon-property-and-flock-safety-feed-ai-surveillance-feeds-to-the-cops.....14

Thor Benson, *The Danger of License Plate Readers in Post*-Roe *America*, Wired (Jul. 7, 2022), https://www.wired.com/story/license-plate-reader-alpr-surveillance-abortion/.....22

Tomo Chien, *California Cops Are Breaking Surveillance Laws. Who's Going to Stop Them?*, S.F. Standard (Jul. 23, 2025), https://perma.cc/S376-YDFX.....17

Va. State Crime Comm'n, *2024 Annual Report* (June 30, 2025), https://perma.cc/PZ3M-VTHB..... 9, 11, 12, 14

Va. State Crime Comm'n, *Law Enforcement Use of Automatic License Plate Recognition (ALPR) Update* (Jan. 2026), https://perma.cc/5Y6A-NGZW..... 15, 16

Virginia, DeFlock, https://deflock.org/map#map=7/37.169819/-78.574219/virginia.....4

With Cameras, Informants, NYPD Eyed Mosques, AP (Feb. 23, 2012), https://perma.cc/UX2Y-W5AW.....11

STATEMENT OF INTEREST[1]

Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that has worked for more than 30 years to protect innovation, free expression, and civil liberties in the digital world. EFF regularly participates both as direct counsel and as amicus in the U.S. Supreme Court and this Court in cases addressing the Fourth Amendment and its application to new technologies. *See, e.g.*, *Carpenter v. United States*, 585 U.S. 296 (2018); *Riley v. California*, 573 U.S. 373 (2014); *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330 (4th Cir. 2021).

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization that since 1920 has sought to protect the civil liberties of all Americans. The ACLU of Virginia is the ACLU's Virginia state affiliate. The ACLU and the ACLU of Virginia have participated as counsel for parties or amici before this Court and the U.S. Supreme Court in many cases concerning the right to privacy under the Fourth Amendment. *See, e.g.*, *Carpenter*, 585 U.S. 296 (counsel); *Riley*, 573 U.S. 373 (amici); *Leaders of a Beautiful Struggle*, 2 F.4th 330 (counsel).

---

[1] Pursuant to Fed. R. App. P. 29(a)(4)(e), counsel for amici curiae certifies that no party's counsel authored this brief in whole or in part. No person other than amici, their members, or their counsel contributed money that was intended to fund the preparing or submitting of this brief. All parties have consented to the filing of this brief.

INTRODUCTION AND SUMMARY OF ARGUMENT

In America, since long before the advent of cell phones, cars have been "such a pervasive and insistent part of daily life" that for many individuals, owning and driving one "is indispensable to participation in modern society." *Carpenter v. United States*, 1585 U.S. 296, 315 (2018) (cleaned up); *see United States v. Jones*, 565 U.S. 400 (2012) (five concurring justices would hold long-term tracking of vehicle unconstitutional under the Fourth Amendment, endorsing the reasoning ultimately adopted by the *Carpenter* majority). Our vehicles take us to sensitive and private places like our homes, doctors' offices, and places of worship. And yet, for many years now, with little-to-no oversight, law enforcement agencies and private companies have been quietly scanning and recording the locations of vast numbers of vehicles across the country, amassing databases of billions of location points reflecting the locations and movements of ordinary people.

This "Automated License Plate Reader" ("ALPR") data is collected on every vehicle, regardless of whether individual drivers are suspected of criminal activity. ALPR data includes not just the plate number but also a photograph of the vehicle, its make, model, color, distinctive features, and detailed location, time, and date information that can later place the vehicle to within feet of the original scan. This data is stored in massive, interconnected databases and retained according to ad hoc arrangements between law enforcement agencies and ALPR system vendors.

Modern ALPR systems, like the one at issue in this case, are supercharged with video capabilities and artificial intelligence, constantly powered through solar cells, abundantly financed with venture capital, and aggressively marketed to local police as a nationally networked surveillance tool. Today, ALPR data can be used not just to identify and locate a particular vehicle, but to identify that vehicle's owner, driver, and who they associate with, as well as phone numbers, criminal records, and even a vehicle's bumper stickers or state of disrepair. And because ALPR data is stored for weeks, months, or sometimes even years, ALPR databases allow for retrospective searches that enable law enforcement to infer driving patterns, associations, and sensitive details about drivers' lives.

Nor does this surveillance stop at jurisdictional lines. ALPR databases are accessible to federal, state, and local law enforcement agencies even where those agencies do not collect their own data or maintain their own databases. These databases are also linked through nationwide and statewide sharing networks that allow agencies to query location data well beyond their own city limits. Some states, like Virginia, have moved to restrict ALPR data sharing across state lines, but those restrictions have time and again proved insufficient. Though Virginia's 2025 ALPR statute prohibits out-of-state and federal sharing, over 20 Virginia law enforcement agencies have already violated the prohibition. Meanwhile, Virginia's sprawling statewide sharing network remains intact, and officers can still *access* out-of-state

data even if they cannot share Virginia data.

At bottom, searches of ALPR databases seriously threaten to undermine the "degree of privacy against government that existed when the Fourth Amendment was adopted," *Carpenter*, 585 U.S. at 305 (cleaned up), because they give police a capability unimaginable in the past—the ability to enter a virtual time machine and view suspects', or anyone else's, past movements (and much more) "[w]ith just the click of a button," *id.* at 311. The Fourth Amendment's warrant requirement exists to prevent this capability from feeding "too permeating police surveillance." *Id*. (cleaned up).

ARGUMENT

I. Even "Local" ALPR Systems Are Part of a Vast, Interconnected Network That Collects Massive Amounts of Detailed Data With Little Oversight.

A. ALPRs Are Increasingly Ubiquitous, Automatically and Indiscriminately Collecting a Significant Amount of Data, Including Precise Location Data.

ALPRs have rapidly proliferated into one of the most commonplace surveillance technologies in American law enforcement. ALPR cameras now blanket most larger towns and highways nationwide and have been widely deployed by police agencies across the state of Virginia.[2] Norfolk's ALPR vendor, Flock

[2] *Virginia*, DeFlock, https://deflock.org/map#map=7/37.169819/-78.574219/virginia.

Safety ("Flock"), alone has nearly 90,000 cameras in 49 states and over 5,000 communities.[3]

The Norfolk Police Department ("NPD") controls a growing network of 176 of these cameras, and many more cameras have been identified in the vicinity.[4] JA31. Though NPD has refused to reveal where it placed its ALPR cameras, a nationwide effort by private citizens has identified many of their locations.[5] *See* Pls.' Mem. in Supp. of Mot. for Partial Summ. J. at 6, *Schmidt v. City of Norfolk*, 2:24-cv-00621-MSD-RJK (E.D.Va. Sept. 15, 2025), ECF No. 108 (hereinafter "Schmidt Br."). Within Norfolk city limits, NPD also has access to the data from 43 additional ALPR cameras that are owned by other entities and businesses. *See id.* at 7. As the Norfolk police chief has stated in describing Norfolk's ALPR network, "it would be difficult to drive anywhere of any distance without running into a camera."[6]

The scale of ALPR data collection is staggering. By scanning every license

---

[3] *See National LPR Network*, Flock Safety, https://perma.cc/UMZ5-99YV; Gideon Epstein, *Flock Gives Law Enforcement All Over the Country Access to Your Location*, ACLU Mass. Data for Just. Project (Oct. 7, 2025), https://perma.cc/7XRJ-C6KR.

[4] *See Norfolk*, DeFlock, https://deflock.org/map#map=12/36.849370/-76.289954/norfolk%2520virginia.

[5] *Id.*

[6] Cianna Morales, *Norfolk, Va.'s Flock Cameras Spark Privacy Debate*, Gov't Tech. (June 20, 2023), https://perma.cc/2ENS-NFDK.

plate that comes into view—for some systems, nearly 2,000 plates per minute[7]—ALPRs collect an enormous volume of detailed information about drivers, all without any human involvement. Flock boasts that it collects over 20 *billion* ALPR scans every month across the United States.[8] In Norfolk, from March 1 through March 31, 2026, alone, NPD's cameras detected over 1 million vehicles.[9]

ALPR systems collect this data regardless of any vehicle's association with criminal activity. During the same March 2026 period, NPD's ALPR system detected a "hotlist" match for less than 1% of vehicles it captured.[10] In other words, nearly everyone whose ALPR information was collected and stored by NPD was under no suspicion whatsoever at the time Norfolk's ALPR system captured their information. Data in Austin, Texas in 2025 similarly showed only 0.2% of scans contributed to arrests.[11]

Despite their name, ALPRs collect far more than just license plate

---

[7] Ángel Diaz & Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, Brennan Ctr. (Sept. 10, 2020), https://perma.cc/47KL-DVA8.

[8] *See National LPR Network*, *supra* note 3.

[9] *Norfolk VA PD*, Flock Transparency Portal (Mar. 31, 2026), available at https://www.eff.org/document/norfolk-va-pd-flock-transparency-portal-3312026.

[10] *Id*.

[11] Abigail Velez, *Flock CEO Responds to Austin Backlash as City Contract Nears Expiration*, CBS Austin (June 20, 2025), https://perma.cc/3ERP-QBMP.

information. ALPR systems also record detailed geolocation data for each plate scanned, including not just the location of the ALPR camera itself, but also the direction and specific lane in which the car was traveling.[12] Because the camera's exact position is known, the vehicle can be geolocated to within feet of its actual location. Once that data is transmitted to the ALPR database, anyone with access can easily run retrospective searches for a full license plate number to locate a specific vehicle, a partial license plate number to locate a group of vehicles, or for all vehicles recorded at a particular location at specific times. *See* JA8.[13] ALPR databases also enable searches across extended time periods. Depending on the data retention period, users can query weeks, months, or years of vehicle location data with a single request.[14]

Newer ALPR systems, like the Flock system used in Norfolk, also employ artificial intelligence ("AI") to collect and extract greater detail about vehicles. Flock's system creates a "Vehicle Fingerprint" that recognizes vehicle features like

---

[12] *See Commonwealth v. McCarthy*, 142 N.E.3d 1090, 1095 (Mass. 2020) (describing ALPR systems).

[13] *See also Solving Cross-Jurisdictional Crime in Real Time: How Flock Safety's Unified Platform Makes It Possible*, Flock Safety (May 28, 2025), https://perma.cc/4JBN-RY6L (Flock platform allows users to search by "time and location" and by "partial plate," among other categories).

[14] *See* NACDL Fourth Amend. Ctr., *ALPR Primer* 1, https://perma.cc/6W6D-WVPM (queries of ALPR databases return "all instances when that plate was detected…over a set time-period.").

paint color, vehicle type, unique characteristics, and even bumper stickers.[15] Flock users can filter their database searches based on those features, allowing them to track movements and locations of vehicles with certain features.[16] Flock also offers an AI-powered plain language search function that allows law enforcement to search for highly specific details such as "blue SUV with a racing stripe" or "white F-150 with a ladder in the back."[17] As Flock describes it: "Just type what you're looking for…and get visual matches instantly."[18]

B. Police Have Real-Time Access to ALPR Data with Few Restrictions on Use and Little Oversight.

Once an ALPR camera scans a passing vehicle, its data becomes almost immediately available to subscribing agencies—not just the local agency whose camera captured the plate. Norfolk police officers have real-time or near-real-time access to the data captured by Flock's network of cameras, and police can log into Flock's system at any time from a web-based interface or mobile application. JA8.

---

[15] *Evidence at Scale: 6 Benefits of LPR For Law Enforcement*, Flock Safety (Nov. 21, 2023), https://perma.cc/SE8N-HYMY.

[16] *Not All License Plate Readers are Equal: When Plate Data Fails, How Do Investigations Continue?*, Flock Safety (Feb. 6, 2026), https://perma.cc/3TKC-LH7W.

[17] *Flock Safety Launches New AI-powered Tools to Accelerate Police Investigations*, Police1 (Feb. 19, 2025), https://perma.cc/6YPQ-JA8H.

[18] *Flock Freeform*, Flock Safety, https://perma.cc/LPT8-5JBT.

After logging in, users can access not only local data, but also any data, nationwide, shared by other law enforcement agencies and any data from private entities that have opted to share with law enforcement.[19] *See infra* I.C.

Despite the volume and sensitivity of the location data flowing into ALPR databases, Norfolk places few restrictions on officer use. Queries are (and always have been) performed without first obtaining a warrant, without the need to document probable cause, and without prior supervisory approval. Schmidt Br. at 12. Until last year, Virginia did not place any restrictions whatsoever on how police could use ALPRs; "therefore, law enforcement could collect and search ALPR data for any purpose, keep data for an indefinite time period, and share data without any restrictions."[20] Though Virginia enacted a statute in 2025 that places some limits on ALPR use, it still does not require a warrant, probable cause, or even an explanation of the connection between the license plate queried and the suspected crime.[21] *See* Schmidt Br. at 12.

Making matters worse, there is little meaningful oversight on law enforcement ALPR use. This issue is endemic to ALPR systems nationwide, including Norfolk.

---

[19] Va. State Crime Comm'n, *2024 Annual Report* 11 (June 30, 2025), https://perma.cc/PZ3M-VTHB.

[20] *Id.* at 14. Some Virginia agencies adopted their own policies, though the Commission found these retention periods varied by agency. *Id.* at 15.

[21] Va. Code Ann. § 2.2-5517(D).

While Virginia's 2025 statute requires agencies to conduct internal audits and submit self-reported annual usage data to the Department of State Police (who must, in turn, share aggregate, statewide data with the Governor, General Assembly, and Virginia State Crime Commission), the statute imposes no independent, external audits or agency-level oversight mechanism, leaving compliance almost entirely self-policed.[22]

Audits also promise far more oversight than they deliver. Flock's system allows agencies to generate and download "network audits"[23] that log every search, but that mechanism only provides meaningful accountability if officers enter genuine, detailed justifications, if agencies actually download and review the records, and if there are real consequences for misuse. NPD struggles on all of these counts. For one, NPD did not even download its own audit files until February 2025, years into its Flock contract, and no one reviewed them until May 2025. Schmidt Br. at 13. By that point, NPD's ALPR system had been searched over 230,000 times. *Id.*

---

[22] Va. Code Ann. § 2.2-5517(H)(6), (I), (J).

[23] *See* Kunle Falayi, *Virginia Surveillance Network Tapped Thousands of Times for Immigration Cases*, VPM News (Oct. 9, 2025), https://www.vpm.org/news/2025-10-09/flock-safety-cameras-alprs-federal-immigration-enforcement-lehmann-kochis (Flock network audits obtained through public records request).

The top three search reasons were vague, boilerplate phrases,[24] and no one verified that case numbers were real or related to the stated search reason, because doing so "would be entirely too time consuming" given the number of entries. Schmidt Br. at 1, 13. In other words, because NPD does not require a warrant or showing of probable cause for queries, its ALPR system is queried so frequently that meaningful review of individual searches is, by the agency's own admission, simply "impossible." *Id*. at 13.

At the individual level, lack of oversight leads to concrete harms. Officers from several agencies across the country have used ALPR data to stalk their wives or girlfriends.[25] Earlier this year, Kansas police used their ALPR system to pursue someone who wrote a critical op-ed about the police department.[26] New York police collected license plate data to track Muslims and identify mosque attendees,[27] and a

---

[24] Some agencies have even encouraged officers to be "as vague as permissible" when using the Flock system. Jason Koebler, *Police Told to Be "As Vague as Permissible" About Why They Use Flock*, 404Media (Jan. 27, 2026), https://www.404media.co/police-told-to-be-as-vague-as-permissible-about-why-they-use-flock/.

[25] *See* Va. State Crime Comm'n, *supra* note 19, at 30–31; Brian Kerhin, *Menasha Officer Pleads Not Guilty to Misconduct Charge Over Ex-girlfriend Tracking*, Fox11 News (Feb. 10, 2026), https://tinyurl.com/yj4ywctm.

[26] Jay Stanley, *Kansas Town Uses License Plate Readers to Go After Man Who Wrote Op-Ed*, ACLU (Feb. 3, 2026), https://perma.cc/6UPF-DA6X.

[27] *With Cameras, Informants, NYPD Eyed Mosques*, AP (Feb. 23, 2012), https://perma.cc/UX2Y-W5AW.

recent investigation showed officers around the country using racist terms for the Romani people in their search reasons.[28] Another officer who was a serial burglar even monitored license plate data "to determine if he had been identified as a suspect for his crimes."[29]

C. ALPR Data Can Be Automatically and Continuously Shared Across Jurisdictions, Including Through Sprawling Statewide and Nationwide Sharing Networks.

When a vehicle is captured by an ALPR camera, its data is unlikely to remain solely with the local agency. Modern ALPR systems, like Flock's, feed ALPR information into cloud-based databases that allow for instantaneous, automatic, and continuous sharing among law enforcement agencies, as well as sharing from private ALPR customers with law enforcement.[30] Vendors like Flock facilitate and encourage this data sharing. Schmidt Br. at 7. As one Norfolk police lieutenant noted, "[e]very jurisdiction that has Flock is able to share data with other

---

[28] Rindala Alajaji & Dave Maass, *License Plate Surveillance Logs Reveal Racist Policing Against Romani People,* EFF (Nov. 3, 2025), https://perma.cc/G8PB-PDJF.

[29] *See* Va. State Crime Comm'n, *supra* note 19, at 30.

[30] *See National LPR Network*, *supra* note 3; *Introducing, Flock's National and Statewide Law Enforcement Search Network*, Flock Safety (Aug. 18, 2020), https://perma.cc/4Z4W-CCMC; Jason Koebler, *Home Depot and Lowe's Share Data From Hundreds of AI Cameras With Cops*, 404Media (Aug. 6, 2025), https://www.404media.co/home-depot-and-lowes-share-data-from-hundreds-of-ai-cameras-with-cops/ (private companies continuously sharing Flock data with law enforcement).

jurisdictions and also see data that's being shared with them."[31] This transforms a discrete local surveillance program into a node in a vast, interconnected network.

While other ALPR vendors also offer data-sharing networks,[32] Flock is notable for operating the largest stationary ALPR network in the country.[33] Flock data sharing takes several forms. Agencies can share on a one-to-one basis with a specific agency partner,[34] or they can open their network to all agencies statewide[35] or to Flock's entire national sharing network.[36] Once a sharing partner or network is selected, agencies automatically and continuously share all ALPR data captured with those partners, as long as sharing remains turned on.[37] Private entities with Flock

---

[31] Morales, *supra* note 6.

[32] *Data Sharing*, Motorola Sols. (Dec. 16, 2025), https://perma.cc/T6SL-4V48 (Motorola's Vigilant Solutions ALPR system); *FAQS – ALPR*, Axon, https://perma.cc/WPB7-DR96 (Axon's ALPR system).

[33] *License Plate Readers (LPR)*, Flock Safety, https://perma.cc/8NPB-DKT7.

[34] *See Leaving the Door Wide Open: Flock Surveillance Systems Expose Washington Data to Immigration Enforcement*, Univ. of Wash. Ctr. For Hum. Rts. (Oct. 21, 2025), https://perma.cc/85XY-8265 (describing one-to-one sharing of ALPR data through Flock's network).

[35] *See Introducing, Flock's National and Statewide Law Enforcement Search Network*, *supra* note 30.

[36] *See National LPR Network*, *supra* note 3.

[37] *See* Dustin Dorsey, *Santa Clara County to Stop Using Flock Safety Cameras in Several Cities After Privacy Concerns*, ABC 7 News (Feb. 25, 2026), https://perma.cc/V5AA-W49Z (Flock statement describing sharing as granting database "access" that customers can choose to "revoke").

cameras, such as homeowners associations, apartment complexes, business districts, schools,[38] national chain stores,[39] and malls across the country,[40] can also choose to share the data they collect with law enforcement. "So long as customers give their consent, other customers can access this data from Flock cameras in different jurisdictions or across the country." *United States v. Martin*, 753 F. Supp. 3d 454, 458 (E.D. Va. 2024). Depending on how long the agency or private entity stores plate data, historical searches could access data dating back years.[41]

This sharing is different in kind from traditional cooperation between agencies collaborating on a specific case. ALPR data sharing involves shared access to a single, giant database, running continuously. Flock boasts that its national network has the ability to "[t]rack suspects across counties and state lines with seamless data sharing and national plate visibility" through "[t]he only network powered by cities,

---

[38] *United States v. Martin*, 753 F. Supp. 3d 454, 458 (E.D. Va. 2024).

[39] Koebler, *supra* note 30.

[40] Thomas Brewster, *America's Biggest Mall Owner Is Sharing AI Surveillance Feeds Directly With Cops*, Forbes (May 6, 2024) https://www.forbes.com/sites/thomasbrewster/2024/05/06/simon-property-and-flock-safety-feed-ai-surveillance-feeds-to-the-cops.

[41] *See* Va. State Crime Comm'n, *supra* note 19, at 16 (state retention periods ranging from three minutes to five years). Virginia now limits ALPR data retention to 21 days, *see* Va. Code Ann. § 2.2-5517(E), but this limit applies only to Virginia law enforcement and its vendors. Little prevents Virginia officers from accessing ALPR data collected by agencies in other states, such as West Virginia or Kentucky, with no retention limits.

neighborhoods, and businesses—all working as one."[42] And as recent reporting has revealed, if an agency accesses Flock's national sharing network, officers are able to search more than 6,800 different "local" camera networks across the country, comprising data from more than 83,000 ALPR cameras.[43]

Virginia's 2025 ALPR law allows data sharing with outside agencies, including "allowing another law-enforcement agency to query system data, provided that the agency receiving such data shall comply with all of the provisions" of the law.[44] Although the law prohibits sharing with out-of-state or federal agencies,[45] statewide sharing within Virginia itself represents a massive potential network. At least 137 Virginia agencies use Flock's ALPR system, according to a 2025 Virginia State Crime Commission survey.[46] The actual number is likely higher, given that about one third of Virginia agencies failed to respond to the survey.[47] Among the

---

[42] *See National LPR Network*, *supra* note 3.

[43] Joseph Cox & Jason Koebler, *A Texas Cop Searched License Plate Cameras Nationwide for a Woman Who Got an Abortion*, 404Media (May 29, 2025), https://www.404media.co/a-texas-cop-searched-license-plate-cameras-nationwide-for-a-woman-who-got-an-abortion/.

[44] Va. Code Ann. § 2.2-5517(F)(1).

[45] *Id*. § 2.2-5517(F).

[46] Va. State Crime Comm'n, *Law Enforcement Use of Automatic License Plate Recognition (ALPR) Update* 7 (Jan. 2026), https://perma.cc/5Y6A-NGZW.

[47] *Id.* at 2, 5, 14–15 ("[A]lmost one-third of law enforcement agencies did not respond to the survey; therefore, their ALPR use is unknown.").

responding agencies with ALPR systems, the majority provide other law enforcement agencies with some type of continuous access to their ALPR data, and most had not denied another agency's request for continuous access.[48]

Additionally, legislative prohibitions on out-of-state and federal sharing are hardly foolproof. Virginia's restriction has already failed to hold: the State Crime Commission's report found that 20 Virginia agencies were providing out-of-state agencies with continuous access to their ALPR data, and 9 reported doing the same for federal agencies—all in violation of the statute.[49] And the problem is not unique to Virginia. California has similarly prohibited out-of-state and federal sharing of ALPR data since 2016;[50] yet, a decade later, agencies throughout the state continue to share in violation of the law. Last fall, for example, the San Francisco Police Department allowed out-of-state and federal agencies to run 1.6 million illegal searches of its Flock database.[51] Investigations by news organizations have found

---

[48] *Id*. at 11, 13.

[49] *Id*. at 11–12; Alex Roever, *Report Reveals Virginia Police Misuse of License Plate Reader Technology*, WRIC (Mar. 2, 2026), https://www.wric.com/news/virginia-news/report-reveals-virginia-police-misuse-of-license-plate-reader-technology/.

[50] Cal. Civ. Code § 1798.90.5–1798.90.55.

[51] Jennifer Pinsof, *EFF, ACLU to SFPD: Stop Illegally Sharing Data With ICE and Anti-Abortion States*, EFF (Sept. 18, 2025), https://perma.cc/6KMG-YWJZ.

apparent violations of the law to be "routine and widespread,"[52] and the California Attorney General is currently suing one agency for its violations.[53]

Concerningly, Flock's continuous sharing features can apparently be activated inadvertently, allowing for broad, unauthorized access to sensitive driver location data without an agency's knowledge. Just this year, several California agencies discovered they were accidentally sharing ALPR data with hundreds of out-of-state agencies, in violation of California law.[54] These agencies claim they were unaware that Flock's nationwide sharing features had been activated, an assertion Flock itself has since confirmed.[55] After investigating, Flock concluded that, "in some cases it is impossible to determine a specific cause" as to why nationwide sharing was activated without an agency's knowledge.[56] This only underscores the privacy risks

---

[52] Tomo Chien, *California Cops Are Breaking Surveillance Laws. Who's Going to Stop Them?*, S.F. Standard (Jul. 23, 2025), https://perma.cc/S376-YDFX.

[53] Press Release, Cal. Off. of Att'y Gen., Attorney General Bonta Continues Legal Challenge to Stop El Cajon from Illegally Sharing License Plate Data (Jan. 21, 2026), https://perma.cc/4NMX-8ZH2.

[54] Emily Margaretten & Zoe Morgan, *Mountain View Police Turn Off License Plate Cameras After Data Sharing Breach*, Mountain View Voice (Feb. 2, 2026), https://perma.cc/FR6Y-J72D; Matthew Rodriguez, *Flock License Plate Readers Shared Data With Out-of-state Agencies*, *Ventura County Audit Finds*, CBS (Feb. 27, 2026), https://perma.cc/G4EC-3HT2.

[55] *Flock Implements Enhanced Guardrails Across California to Ensure Lawful and Responsible Use of LPRs*, Flock Safety (Mar. 2, 2026), https://perma.cc/A8QQ-SHYF.

[56] *Id*.

inherent in an under-regulated system this sprawling and unwieldy.

These sharing arrangements radically expand the comprehensiveness of the surveillance in two directions.

First, a driver's sensitive location data is no longer just visible to local officers. It is available to potentially hundreds, or even thousands, of agencies across the state and country. This also dramatically inflates the number of times an agency's ALPR data is queried. For example, the Virginia Center for Investigative Journalism obtained Flock audit logs from Bridgewater, Virginia, a town of 6,600 people with only five cameras, and found that outside law enforcement agencies across the country accessed Bridgewater's data 6.9 million times over 12 months.[57]

Second, the inverse is equally true: local law enforcement agencies using the Flock network, like NPD, can now track a person's movements far beyond their own city limits, and far beyond the reach of their own cameras. The district court characterized Norfolk's ALPR system as limited by its geographic footprint: 176 cameras covering a small fraction of the city's road miles. JA36. But that framing isolates the city's cameras from the network they feed. Though the 2025 law prohibits Virginia agencies from sharing their own ALPR data across state lines,

---

[57] Kunle Falayi, *One Sleepy Virginia Town. Nearly 7 Million Hits On Its Surveillance Network*, Va. Ctr. For Investigative Journalism (Sept. 16, 2025), https://perma.cc/LB4W-5V23.

they remain free to access out-of-state agencies' ALPR data.[58] A Norfolk officer can easily query ALPR data throughout the entire state or country and see where a vehicle appeared in Richmond, Northern Virginia, or in a different state entirely.

D. Because ALPR Location Data Can Reveal Detailed Private and Personal Details About Individuals, It is Increasingly Used to Surveil Politically Vulnerable Groups.

Even a small amount of ALPR data can reveal a person's identity as well as sensitive information about that person. By storing data for long periods, ALPR databases allow officers to query months' or years' worth of information about a car's past locations. And the more cameras present in a given area, the more granular the data. This allows officers to make inferences about individuals that they could not have made without such historical data. ALPR data can reveal not only where a driver was on a given date and time in the past, but can also suggest where a driver may be in the future.[59] As one regional California agency recognized in its privacy impact assessment, ALPR data "could potentially be misused to infer additional information about an individual that is not relevant to police purposes and potentially

---

[58] *See* Va. Code Ann. § 2.2-5517(F).

[59] State of N.J., *Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data* 4 (Dec. 3, 2010), https://perma.cc/72PK-NY2L; Steve Connor, *Surveillance UK: Why This Revolution Is Only the Start*, The Independent (Dec. 22, 2005), https://perma.cc/GJU3-XXDA.

sensitive for the individual. Such inferences could include, but are not limited to: non-relevant personal relationships; marital fidelity; religious observance; and political activities."[60]

Newer systems, like Flock's, that incorporate AI to create a "vehicle fingerprint," collect even more revealing data. As mentioned above, Flock can track bumper stickers, which may have political statements, and other identifying information about a vehicle. Flock has also added features like "convoy analysis," which will list vehicles that frequently travel with a vehicle that is searched, and "multi-geo search" which will return a list of all cars that have been to a given number of locations.[61] These features make it even easier for law enforcement to track people's social networks and travel habits through ALPR systems.

When coupled with the massive data sharing networks that allow agencies to surveil driver locations across jurisdictions and state lines, ALPR technology poses acute dangers for politically vulnerable groups. Indeed, license plate data is already being used to track and identify immigrants, individuals seeking abortions, and people attending protests.

---

[60] *Initial Privacy Impact Assessment for Automated License Plate Reader Technology* 3, N. Cal. Reg'l Intel. Ctr., https://perma.cc/42MC-ELWJ.

[61] Ben Miller, *Flock Safety Gives Users Expanded Vehicle Location Abilities*, Gov't Tech. (Sept. 1, 2025), https://perma.cc/DUS6-GV7X.

Although Immigration and Customs Enforcement (ICE) does not have a contract with Flock, individual officers can get access through a "side door": federal officers simply ask local law enforcement agencies to search their ALPR databases on the federal agency's behalf.[62] A trove of Flock data obtained by researchers last spring revealed thousands of "nation and statewide lookups by local and state police done either at the behest of the federal government or as an 'informal' favor to federal law enforcement, or with a potential immigration focus."[63] Officers logged reasons including "ICE," "ICE+ERO," and "immigration."[64] Audit logs obtained in October 2025 similarly revealed that Virginia's own Flock sharing networks were accessed for immigration enforcement purposes nearly 3,000 times over a 12-month period, despite Virginia agencies promising to not use their ALPR systems for immigration enforcement.[65] Many of these searches came from out-of-state, via the nationwide sharing network.

Flock's nationwide sharing network has also been used to track at least one

---

[62] Jason Koebler, *Wildlife Conservation Police Are Searching Thousands of Flock Cameras for ICE*, 404 Media, (Apr. 6, 2026), https://perma.cc/5LXV-A48L; *Leaving the Door Wide Open, supra* note 34.

[63] Jason Koebler & Joseph Cox, *ICE Taps into Nationwide AI-Enabled Camera Network, Data Shows*, 404Media (May 27, 2025), https://www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data-shows/.

[64] *Id.*

[65] Falayi, *supra* note 23.

woman who had an abortion. A Texas law enforcement agency was able to access Illinois ALPR data to search for a woman they suspected had self-administered an abortion, even though data-sharing for that purpose was prohibited under Illinois law.[66] Flock's multi-state sharing network poses unique risks for access to reproductive healthcare because individuals in abortion-restrictive states must travel across state lines to receive care.[67]

Flock audit logs have also revealed that, over the course of 10 months, more than 50 federal, state, and local agencies ran hundreds of searches through Flock's nationwide sharing network in connection with protest activity.[68] In some cases, law enforcement specifically targeted known activist groups. It is no wonder that the International Association of Chiefs of Police has cautioned that ALPR technology creates the risk "that individuals will become more cautious in the exercise of their protected rights of expression, protest, association, and political participation

---

[66] *See* Cox & Koebler, *supra* note 43; Press Release, Off. of Sec'y State, Giannoulias Cracks Down on Unlawful Use of License Plate Reader Data (June 12, 2025), https://perma.cc/FZ28-CLQK.

[67] Thor Benson, *The Danger of License Plate Readers in Post*-Roe *America*, Wired (Jul. 7, 2022), https://www.wired.com/story/license-plate-reader-alpr-surveillance-abortion/.

[68] Dave Maass & Rindala Alajaji, *How Cops Are Using Flock Safety's ALPR Network to Surveil Protesters and Activists*, EFF (Nov. 20, 2025), https://perma.cc/WCL4-7C7R.

because they consider themselves under constant surveillance."[69]

II. ALPR Systems Provide the Government with Unprecedented Powers of Surveillance that Upset Traditional Expectations of Privacy.

The district court below correctly recognized that individuals have an expectation of privacy in their movements in public, and that surveillance that reveals these movements can be so intrusive as to constitute an unreasonable search under the Fourth Amendment. *Schmidt v. Norfolk*, No. 2:24CV621, 2026 WL 207513, at *2, *3 (E.D. Va. Jan. 27, 2026) (citing *Carpenter*, 585 U.S. at 310). However, the court erred in holding that Norfolk's ALPR system does not carry out Fourth Amendment searches because the surveillance is not "near continuous" and therefore does not reveal "the whole" of drivers' movements. *Id.* at *14.

The district court's standard is inconsistent with Fourth Amendment case law from the Supreme Court in *Carpenter* and *Jones*, as well as this Court's decision in *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 2 F.4th 330 (4th Cir. 2021) (en banc). These cases teach that courts must closely examine advances in technology to ensure government surveillance does not erode the "degree of privacy against government that existed when the Fourth Amendment was adopted." *Carpenter*, 585 U.S. at 305 (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)).

---

[69] *Privacy Impact Assessment Report for the Utilization of License Plate Readers* 13, Int'l Ass'n of Chiefs of Police (Sept. 2009), https://perma.cc/Y3RS-AM44.

As Justice Alito explained in *Jones*, "[i]n the precomputer age, the greatest protections of privacy were neither constitutional nor statutory, but practical." 565 U.S. at 429 (Alito, J., concurring in judgment). But in the modern era, "technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes," revealing myriad "privacies of life." *Carpenter*, 585 U.S. at 305 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)). Accordingly, the Supreme Court has repeatedly held that the use of technology to collect information that is "otherwise unknowable" triggers constitutional protections. *Id*. at 312; *see also Leaders of a Beautiful Struggle*, 2 F.4th at 341.[70]

Technology, including ALPRs, that "attempts to reconstruct a person's

---

[70] The Supreme Court's approach of looking to historical expectations of privacy to determine current Fourth Amendment safeguards dates back to before the dawn of the Internet age. In *United States v. Karo*, 468 U.S. 705 (1984), for example, it held that using a radio-tracking beeper to monitor an object's location inside a traditionally protected space was a search because police cannot employ advanced technological means to obtain information that they could not have obtained by observation. *Id.* at 715. *See also Kyllo*, 533 U.S. at 36–37, 40 (police use of a thermal imaging device was a Fourth Amendment search, because conducting an equivalent search before the advent of that technology would have required physically entering the home); *Riley v. California*, 573 U.S. 373, 393-94 (2014) (warrant required to search cell phone seized incident to arrest because privacy interest in phone is incomparable to privacy interest in pre-digital items individuals might carry on their person); *Katz v. United States*, 389 U.S. 347, 352 (1967) (electronic eavesdropping on utterances within glass-walled phone booth was a Fourth Amendment search because a person is "entitled to assume that the words he utters into the mouthpiece [in an enclosed booth] will not be broadcast to the world").

movements" presents a particularly acute risk of "erod[ing] Fourth Amendment protections." *Carpenter*, 585 U.S. at 312, 320. In *Carpenter,* for example, the Supreme Court held that a Fourth Amendment search occurs when the government tracks an individual's movements by accessing cell site location information ("CSLI") held by a cellular service provider, at least for a period of days. *Id*. at 310. The Court noted several important qualities of CSLI, including the "detailed" nature of the records; the indiscriminate nature of its collection, which "runs against everyone" who uses a phone; and "the retrospective quality of the data," which "gives police access to a category of information otherwise unknowable." *Id.* at 309, 312. This Court, sitting en banc, subsequently applied this insight in *Leaders of a Beautiful Struggle*, finding that police violated the Fourth Amendment by operating an aerial surveillance program that captured wide-area, low-resolution photographs allowing indiscriminate tracking of people's movements throughout the city of Baltimore. 2 F.4th at 333. The Court wrote that "*Carpenter* solidified the line between short-term tracking of public movements—akin to what law enforcement could do prior to the digital age—and prolonged tracking that can reveal intimate details through habits and patterns," making clear that the prolonged tracking is a Fourth Amendment search. *Id.* at 341 (cleaned up). The Court also emphasized, over the government's strong objection, that the fact that the police collection was not continuous did not affect the analysis. *See id.* at 342 ("We do not suggest that the

AIR program allows perfect tracking of all individuals it captures across all the time it covers. Though data is collected in 12-hour increments, the tracks are often shorter snippets of several hours or less. Still, the program enables photographic, retrospective location tracking in multi-hour blocks, often over consecutive days, with a month and a half of daytimes for analysts to work with. That is enough to yield 'a wealth of detail,' greater than the sum of the individual trips." (quoting *Jones*, 565 U.S. at 415–17 (Sotomayor, J., concurring))).

Particularly in light of the state- and nationwide scope described above, ALPR systems like Norfolk's infringe on individuals' expectations of privacy for much the same reason that the tracking of cell phones in *Carpenter* and the aerial surveillance in *Leaders of a Beautiful Struggle* did: they facilitate prolonged tracking of millions of Americans, before the government has any reason to be interested in them, that reveals previously unknowable intimate details of their lives. And they do so through the preemptive collection of vast repositories of searchable data. In *Leaders*, this Court explained that mass collection of location information on the front-end enabled the very purpose of the City's surveillance program: allowing police to exploit reams of data to "zero in on specific dates and locations related to its investigations." 2 F.4th at 337–38. That kind of database allows police to "travel back in time" to exploit a "newfound tracking capacity [that] runs against everyone." *Carpenter*, 585 U.S. at 312; *see Leaders*, 2 F.4th at 342 ("And here, as [in

Carpenter], the government can deduce [private] information only because it recorded *everyone's* movements.").

The district court erroneously distinguished the ALPR systems at issue here because the record suggests they compile fewer individual data points than technologies at issue in *Carpenter* and *Leaders of a Beautiful Struggle*. 2026 WL 207513, at *12–*13. However, even a small number of ALPR data points facilitate inferences about individuals' travels habits, including the homes, businesses and neighborhoods they frequent, giving the police access to previously unknowable information. After all, "[t]he datasets in *Jones* and *Carpenter* [and *Leaders of a Beautiful Struggle*] had gaps in their coverage, too," but "in [all three] cases, the surveillance still surpassed ordinary expectations of law enforcement's capacity and provided enough information to deduce details from the whole of the individuals' movements." *Leaders of a Beautiful Struggle*, 2 F.4th at 342–43; *see id.* at 343 (discussing how even where location collection has gaps, the sensitivity of certain locations such as the home will often allow police to "deduce identity"); *see also United States v. Chatrie*, 136 F.4th 100, 122–24 (4th Cir. 2025) (per curiam) (en banc) (Wynn, J., concurring in the judgment) (explaining why even two hours of precise location data can infringe on reasonable expectations of privacy), *cert. granted*, No. 25-112. Moreover, the extent to which such a technology captures "the whole" or "less than all" of person's movements was just one factor among several

in *Carpenter* and *Leaders of a Beautiful Struggle*.[71] As discussed above, other factors include the indiscriminate and retrospective nature of the technology, while the ultimate question is whether it allows the deduction of details based on individuals' movements in a way unthinkable at the time of the Fourth Amendment's drafting. The confluence of these factors—detailed location data collection about a vast swath of the American population allowing fundamentally new kinds of retrospective searches—is why ALPR systems violate expectations of privacy under the Fourth Amendment. They are "qualitatively different," from traditional surveillance, *Carpenter*, 585 U.S. at 309, and it is "impossible to think of late-18th-century situations that are analogous." *Jones*, 565 U.S. at 420 (Alito, J., concurring in judgment).

CONCLUSION

For the reasons above, this Court should reverse the ruling of the district court.

---

[71] Although the cell phone location records searched by the government in *Carpenter* contained "an average of 101 data points per day," 585 U.S. at 302, the Court did not set a volumetric threshold for triggering Fourth Amendment protection. Rather, the Court established a bright-line rule protecting historical cell site location information against warrantless search, regardless of how frequently a particular person happens to use their phone, and thus generate location records, over the course of a day. Drivers in Norfolk will vary in their driving habits and the amount of time they spend on the road, but that does not diminish the invasiveness of this "newfound tracking capacity [that] runs against everyone." *Id.* at 312.

Dated: April 20, 2026

Respectfully submitted,

/s/ Brett Max Kaufman

Brett Max Kaufman
Nathan Freed Wessler
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
bkaufman@aclu.org

Elizabeth Femia
Andrew Crocker
Jennifer Pinsof
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
lfemia@eff.org

Matthew William Callahan
ACLU FOUNDATION OF VIRGINIA
PO Box 26464
Richmond, VA 23261-6464
(804) 523-2146
mcallahan@acluva.org

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS

Pursuant to Fed. R. App. P. 32(g)(1), I certify as follows:

1. This Brief of *Amici Curiae* in Support of Plaintiffs-Appellants and Reverasal complies with the type-volume limitation of Fed. R. App. P. 29(a)(5) because this brief contains 6489 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This brief 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 this brief has been prepared in a proportionally spaced typeface using Microsoft Word 365, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: April 20, 2026

/s/ Brett Max Kaufman
Brett Max Kaufman

Counsel of Record for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Fourth Circuit by using the appellate CM/ECF system on April 20, 2026.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: April 20, 2026

/s/ Brett Max Kaufman
Brett Max Kaufman

Counsel of Record for Amici Curiae