No. 26-3426

IN THE UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

UNITED STATES OF AMERICA,
PLAINTIFF-APPELLEE,

v.

LAWRENCE STURDIVANT,
DEFENDANT-APPELLANT

On Appeal from the
United States District Court
for the Northern District of Ohio at Cleveland
Case No. 1:22-CR-00615
The Honorable J. Philip Calabrese

# BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION, AND AMERICAN CIVIL LIBERTIES UNION OF OHIO IN SUPPORT OF DEFENDANT-APPELLANT AND REVERSAL

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

Laura Moraff
Brett Max Kaufman
Nathan Freed Wessler

AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Email: lauramoraff@aclu.org
Telephone: (212) 549-2500

Freda J. Levenson
ACLU OF OHIO FOUNDATION, INC.
4506 Chester Avenue
Cleveland, Ohio 44103
Email: flevenson@acluohio.org
Telephone: (216) 541-1376

David J. Carey
ACLU OF OHIO FOUNDATION, INC.
1108 City Park Avenue, Suite 203
Columbus, Ohio 43206
Email: dcarey@acluohio.org
Telephone: (380) 215-0997

*Counsel for Amici Curiae*

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

# Disclosure of Corporate Affiliations and Financial Interest

Sixth Circuit
Case Number: 26-3426 Case Name: U.S. v. Sturdivant

Name of counsel: Andrew Crocker

Pursuant to 6th Cir. R. 26.1, Amicus Curiae Electronic Frontier Foundation, ACLU, & ACLU of Ohio
*Name of Party*
makes the following disclosure:

1. Is said party a subsidiary or affiliate of a publicly owned corporation? If Yes, list below the identity of the parent corporation or affiliate and the relationship between it and the named party:

No.

2. Is there a publicly owned corporation, not a party to the appeal, that has a financial interest in the outcome? If yes, list the identity of such corporation and the nature of the financial interest:

No.

CERTIFICATE OF SERVICE

I certify that on November 9, 2026 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by placing a true and correct copy in the United States mail, postage prepaid, to their address of record.

s/ Andrew Crocker
Electronic Frontier Foundation

This statement is filed twice: when the appeal is initially opened and later, in the principal briefs, immediately preceding the table of contents. See 6th Cir. R. 26.1 on page 2 of this form.

## TABLE OF CONTENTS

DISCLOSURE OF CORPORATE AFFILIATIONS AND FINANCIAL INTEREST ..... iii

TABLE OF CONTENTS ..... iv

TABLE OF AUTHORITIES ..... vi

STATEMENT OF INTEREST ..... 1

INTRODUCTION ..... 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 AND AUTOMATICALLY AND INDISCRIMINATELY COLLECT 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 PRIVATE AND PERSONAL DETAILS ABOUT INDIVIDUALS, IT IS INCREASINGLY USED TO SURVEIL POLITICALLY VULNERABLE GROUPS ..... 18

II. THE USE OF MODERN ALPR SYSTEMS TO RETROSPECTIVELY TRACK INDIVIDUALS' MOVEMENTS IS A SEARCH UNDER THE FOURTH AMENDMENT. ..... 22

CONCLUSION ..... 29

CERTIFICATE OF COMPLIANCE AND SERVICE ..... 32

# TABLE OF AUTHORITIES

## Cases

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

*Chatrie v. United States*,
609 U.S. 605 (2026) ..... *passim*

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

*Leaders of a Beautiful Struggle v. Baltimore Police Dep't*,
2 F.4th 330 (4th Cir. 2021) ..... 26, 27

*Pennsylvania Coal Co. v. Mahon*,
260 U.S. 393 (1922) ..... 27

*Schmidt v. City of Norfolk*,
819 F. Supp. 3d 492 (E.D. Va. 2026) ..... 1, 8

*United States v. Di Re*,
332 U.S. 581 (1948) ..... 29

*United States v. Jones*,
565 U.S. 400 (2012) ..... *passim*

*United States v. Kyle*,
No. 26-CR-00189-SEH,
2026 WL 2958728 (N.D. Okla. Oct. 1, 2026) ..... 26, 28, 29

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

*United States v. Sturdivant*,
786 F. Supp. 3d 1098 (N.D. Ohio 2025) ..... 4, 5, 23, 25

*United States v. Warshak*,
631 F.3d 266 (6th Cir. 2010) ..... 1

**Statutes**

Cal. Civ. Code § 1798.90.5–1798.90.55 ..... 17

**Other Authorities**

Adam Goldman & Matt Apuzzo, *With Cameras, Informants, NYPD Eyed Mosques*, AP (Feb. 23, 2012) ..... 12

Ángel Diaz & Rachel Levinson-Waldman, *Automatic License Plate Readers: Legal Status and Policy Recommendations for Law Enforcement Use*, Brennan Ctr. (Sept. 10, 2020) ..... 5

*Automatic License Plate Readers*, Cleveland Division of Police General Police Order 4.06.13 (Oct. 23, 2025) ..... 9, 11

Ben Miller, *Flock Safety Gives Users Expanded Vehicle Location Abilities*, Gov't Tech. (Sept. 1, 2021) ..... 19

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) ..... 18

Council of the City of Cleveland, Ordinance No. 683-2026 Section 2 (Jul. 15, 2026), ..... 17

Dave Maass & Rindala Alajaji, *How Cops Are Using Flock Safety's ALPR Network to Surveil Protesters and Activists*, EFF (Nov. 20, 2025) ..... 21

Dustin Dorsey, *Santa Clara County to Stop Using Flock Safety Cameras in Several Cities After Privacy Concerns*, ABC 7 News (Feb. 25, 2026) ..... 13

Emily Margaretten & Zoe Morgan, *Mountain View Police Turn Off License Plate Cameras After Data Sharing Breach*, Mountain View Voice (Feb. 2, 2026) ..... 15

*Flock Freeform*, Flock Safety ..... 8

*Flock Implements Enhanced Guardrails Across California to Ensure Lawful and Responsible*

*Use of LPRs*, Flock Safety (Mar. 2, 2026) ..... 15

*Flock Safety Launches New AI-powered Tools to Accelerate Police Investigations*, Police1 (Feb. 19, 2025) ..... 8

Frank W. Lewis & Cid Standifer, *Cleveland may extend its Flock license plate reader contract*, Signal Cleveland (June 11, 2026) ..... 10, 16, 21

Gideon Epstein, *Flock Gives Law Enforcement All Over the Country Access to Your Location*, ACLU Mass. Data for Just. Project (Oct. 7, 2025) ..... 4

Hannah Drown, *How Flock's license plate surveillance works — and how it can be abused*, Cleveland.com (Jul. 17, 2026) ..... 9, 10

*Initial Privacy Impact Assessment for Automated License Plate Reader Technology* 3, N. Cal. Reg'l Intel. Ctr. ..... 19

*Introducing, Flock's National and Statewide Law Enforcement Search Network*, Flock Safety (Aug. 18, 2020) ..... 12, 13

Jason Koebler & Joseph Cox, *ICE Taps into Nationwide AI-Enabled Camera Network, Data Shows*, 404Media (May 27, 2025) ..... 20

Jason Koebler, *Home Depot and Lowe's Share Data From Hundreds of AI Cameras With Cops*, 404Media (Aug. 6, 2025) ..... 12, 13

Jason Koebler, *Wildlife Conservation Police Are Searching Thousands of Flock Cameras for ICE*, 404 Media (Apr. 6, 2026) ..... 20

Jay Stanley, *Kansas Town Uses License Plate Readers to Go After Man Who Wrote Op-Ed*, ACLU (Feb. 3, 2026) ..... 11

Jennifer Pinsof, *EFF, ACLU to SFPD: Stop Illegally Sharing Data With ICE and Anti-Abortion States*, EFF (Sept. 18, 2025) ..... 18

Joseph Cox & Jason Koebler, *A Texas Cop Searched License Plate Cameras Nationwide for a Woman Who Got an Abortion*, 404Media (May 29, 2025) ..... 14

Kunle Falayi, *Virginia Surveillance Network Tapped Thousands of Times for Immigration Cases*, VPM News (Oct. 9, 2025) ..... 11

*Leaving the Door Wide Open: Flock Surveillance Systems Expose Washington Data to Immigration Enforcement*, Univ. of Wash. Ctr. For Hum. Rts. (Oct. 21, 2025) ..... 13

Matthew Rodriguez, *Flock License Plate Readers Shared Data With Out-of-state Agencies*, *Ventura County Audit Finds*, CBS (Feb. 27, 2026) ..... 15

NACDL Fourth Amend. Ctr., *ALPR Primer* 1 ..... 7

*National LPR Network*, Flock Safety ..... *passim*

*North Royalton OH PD Flock Transparency Portal* (Oct. 27, 2026)..... 6

*Not All License Plate Readers are Equal: When Plate Data Fails, How Do Investigations Continue?*, Flock Safety (Feb. 6, 2026)..... 8

*Ohio*, DeFlock..... 4

Olivia Mitchell, *Cleveland's police commission wants to pause Flock camera use*, Cleveland.com (Oct. 2, 2026)..... 5

Press Release, Off. of Sec'y State, Giannoulias Cracks Down on Unlawful Use of License Plate Reader Data (June 12, 2025) ..... 21

*Privacy Impact Assessment Report for the Utilization of License Plate Readers* 13, Int'l Ass'n of Chiefs of Police (Sept. 2009) ..... 22

Rindala Alajaji & Dave Maass, *License Plate Surveillance Logs Reveal Racist Policing Against Romani People,* EFF (Nov. 3, 2025) ..... 12

Rindala Alajaji & Dave Maass, *The High Crime of "LMAO": How Cops Are Treating Flock's Mass Surveillance As a Joke*, EFF (Sept. 14, 2026) ..... 9

Sean McDonnell, *Cleveland to Keep Flock Safety Cameras After Vote*, Gov't Tech. (July 16, 2026) ..... 5

Sean McDonnell, *Newly released records show nearly 2,000 'immigration' and 'ICE' searches on Cleveland's Flock cameras*, Cleveland.com (Jul. 6, 2026) ..... 17

*Shaker Heights OH PD Flock Transparency Portal* (Oct. 27, 2026) ..... 6

*Solving Cross-Jurisdictional Crime in Real Time: How Flock Safety's Unified Platform Makes It Possible*, Flock Safety (May 28, 2025) ..... 7

State of N.J., *Attorney General Guidelines for the Use of Automated License Plate Readers (ALPRs) and Stored ALPR Data* 4 (Dec. 3, 2010) ..... 18

Steve Connor, *Surveillance UK: Why This Revolution Is Only the Start*, The Independent (Dec. 22, 2005) ..... 18

Thomas Brewster, *America's Biggest Mall Owner Is Sharing AI Surveillance Feeds Directly With Cops*, Forbes (May 6, 2024) ..... 13

Thor Benson, *The Danger of License Plate Readers in Post*-Roe *America*, Wired (Jul. 7, 2022) ..... 21

Tomo Chien, *California Cops Are Breaking Surveillance Laws. Who's Going to Stop Them?*, S.F. Standard (Jul. 23, 2025) ..... 18

Va. State Crime Comm'n, *2024 Annual Report* (June 30, 2025) ..... 11, 12

*Vehicle Recognition Software for Investigation-grade LPR*, Flock Safety (Jul. 23, 2026) ..... 8, 14

## STATEMENT OF INTEREST[1]

The Electronic Frontier Foundation ("EFF") is a non-profit civil liberties organization with more than 30,000 dues-paying members. Founded in 1990, EFF represents technology users' interests in court cases and broader policy debates surrounding the application of law to technology. EFF regularly participates both as counsel and as amicus in the Supreme Court, this Court, and other state and federal courts in cases addressing the Fourth Amendment and its application to new technologies. *See*, *e.g., Chatrie v. United States*, 609 U.S. 605 (2026); *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to the principles of liberty and equality embodied in the Constitution. The ACLU of Ohio Foundation is a state affiliate of the ACLU. The ACLU and its affiliates have frequently appeared before the U.S. Supreme Court and other courts in numerous cases implicating Americans' right to privacy in the digital age, including as counsel in *Carpenter v. United States*, 585 U.S. 296 (2018), and as amicus in *Chatrie v. United States*, 609 U.S. 605 (2026), and *Schmidt v. Norfolk*, Case No. 26-1227 (4th Cir. 2026).

[1] Pursuant to Federal Rule of Appellate Procedure Rule 29(c), *Amici* certify that no person or entity, other than *Amici*, their members, or their counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part. All parties consent to the filing of this brief.

## INTRODUCTION

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 tracking of vehicle unconstitutional under the Fourth Amendment). Our vehicles take us to sensitive and private places like our homes, doctors' offices, and places of worship. And yet, for many years, with little-to-no oversight, law enforcement agencies and private companies have been quietly scanning and recording the locations of vast numbers of vehicles nationwide, 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, and aggressively marketed to local police as a nationally networked surveillance tool. Today, ALPR data can be used not just to track particular vehicles, but also to identify vehicle owners, drivers, and who they associate with, as well as phone numbers, criminal records, and even vehicles' bumper stickers. 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 can also be fed into nationwide and statewide sharing networks that allow agencies to query location data well beyond their own city limits. Some states, like Ohio, where this case took place, have no statewide restrictions on sharing ALPR data across state lines. The lack of restriction allows for sprawling intrastate and interstate data sharing networks.

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*. at 305 (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 and Automatically and Indiscriminately Collect 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 Ohio.[2] One of the ALPR vendors used in this case, Flock Safety ("Flock"), alone has nearly 90,000 cameras in 49 states and over 5,000 communities.[3] *See United States v. Sturdivant*, 786 F. Supp. 3d 1098, 1102 (N.D. Ohio 2025) (officer searched database drawing on Flock and

[2] *Ohio*, DeFlock, https://maps.deflock.org/?lat=40.2254&lng=-82.6881&zoom=7.00.

[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.

ELSAG ALPR systems).

Cleveland operates a network of 100 of these cameras, and many more cameras have been identified in the vicinity.[4] Cuyahoga County has at least 1,717 ALPR cameras operated by government or private entities, which equates to nearly four cameras per square mile of land.[5] Cleveland recently allocated $125,000 and extended its contract with Flock for six months despite pushback from the community.[6]

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

---

[4] Sean McDonnell, *Cleveland to Keep Flock Safety Cameras After Vote*, Gov't Tech. (July 16, 2026), https://www.govtech.com/public-safety/cleveland-to-keep-flock-safety-cameras-after-vote.

[5] Adam Ferrise, *How many license plate readers are in your city? We found out*, Cleveland.com (June 4, 2026), https://www.cleveland.com/metro/2026/06/how-many-license-plate-readers-are-in-your-city-we-found-out.html; *see also Sturdivant*, 786 F. Supp. 3d at 1103 (reporting 1,636 Flock cameras in Cuyahoga County in June 2025).

[6] Olivia Mitchell, *Cleveland's police commission wants to pause Flock camera use*, Cleveland.com (Oct. 2, 2026), https://www.cleveland.com/crime/2026/10/clevelands-police-commission-wants-to-pause-flock-camera-use-will-that-happen.html.

[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.

scans every month across the United States.[8] Examples from Cuyahoga County itself are equally staggering. The North Royalton Police Department detected 201,536 unique plates over the course of a recent 30-day period. In that same time, the Shaker Heights Police Department detected 317,302 unique plates.[9]

ALPR systems collect this data regardless of any vehicle's association with criminal activity. While police departments can place suspect plates on a real-time, suspicionless "hotlist," during the same 30-day period, Shaker Heights' and North Royalton's ALPR systems detected a "hotlist" hit for less than 1% of vehicles captured.[10] In other words, nearly everyone whose ALPR information was collected and stored by these police departments was under no suspicion whatsoever at the time the ALPR systems captured their information.

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

---

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

[9] *North Royalton OH PD Flock Transparency Portal* (Oct. 27, 2026) available at https://www.eff.org/document/north-royalton-oh-pd-flock-transparency-portal-10272026; *Shaker Heights OH PD Flock Transparency Portal* (Oct. 27, 2026), https://www.eff.org/document/shaker-heights-oh-pd-flock-transparency-portal-10272026.

[10] *Id.* (Shaker Heights, 895 hits for 317,302 vehicles captured or 0.3%; North Royalton, 438 hits for 201,536 vehicles captured or 0.2%)

direction and specific lane in which the car was traveling.[11] 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, for a partial license plate number to locate a group of partially matching vehicles, or (through a digital checkpoint technique) for all vehicles recorded at a particular location at specific times.[12] ALPR databases also enable searches and tracking of vehicles 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.[13]

Newer ALPR systems, like the Flock system used in Cleveland, also employ artificial intelligence ("AI") to collect and extract greater detail about vehicles. Flock's system creates a "Vehicle Signature" that recognizes vehicle features like paint color, vehicle type, unique characteristics, and even bumper stickers.[14] Flock

---

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

[12] *See 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 allows search by "time and location" and by "partial plate," among other categories).

[13] *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.").

[14] *Vehicle Recognition Software for Investigation-grade LPR*, Flock Safety (Jul.

users can filter their database searches based on those features, allowing them to track vehicles with certain attributes.[15] Flock also offers an AI-powered plain language search function allowing law enforcement to search for details such as "blue SUV with a racing stripe" or "white F-150 with a ladder in the back."[16] As Flock describes it: "Just type what you're looking for . . . and get visual matches instantly."[17]

### 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. 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 from a web-based interface or mobile application. *See Schmidt v. City of Norfolk*, 819 F. Supp. 3d 492, 499 (E.D. Va. 2026). After logging in, users can decide to search their own agency's cameras or expand searches to every camera

---

23, 2026), https://perma.cc/W4GN-W5LC.

[15] *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.

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

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

network their department has permission to access.[18] This allows access to not only local data, but also any data, nationwide, shared by other law enforcement agencies and any data from private entities that have opted in.

Despite the volume and sensitivity of location data flowing into ALPR databases, Cleveland places few restrictions on officer use. Cleveland police policy permits officers to query the ALPR system without a warrant. And although its policy requires reasonable suspicion to access ALPR data, officers need only self-report a reason or purpose for confirmed searches or hits. [19] Self-reporting requirements in this context have proven ineffective, as officers across the country input self-evidently improper reasons for searches, such as "LOL" "idk" "hehe" and "blah."[20] Officers in the Barberton (Ohio) PD ran numerous searches between March 2024 and May 2026 with "LOL" or "lol" as their listed reason.[21] A

---

[18] Hannah Drown, *How Flock's license plate surveillance works — and how it can be abused*, Cleveland.com (Jul. 17, 2026), https://www.cleveland.com/crime/2026/07/how-flocks-license-plate-surveillance-works-and-how-it-can-be-abused.html.

[19] *Automatic License Plate Readers*, Cleveland Division of Police General Police Order 4.06.13 (Oct. 23, 2025), *available at* https://www.clevelandohio.gov/sites/clevelandohio/files/Public%20Safety/Police/4.06.13%20Automatic%20License%20Plate%20Readers.pdf.

[20] Rindala Alajaji & Dave Maass, *The High Crime of "LMAO": How Cops Are Treating Flock's Mass Surveillance As a Joke*, EFF (Sept. 14, 2026), https://www.eff.org/deeplinks/2026/09/high-crime-lmao-how-cops-are-treating-mass-surveillance-joke.

[21] *Id.*

Columbus (Ohio) police officer ran searches in 2023 for "idiot" and the Belton (Missouri) PD ran searches from August to September 2024 for "d*ckhead." Sometimes, officers mash keys instead of typing a reason—the Lake County (Ohio) Sheriff's Office, for example, ran searches with reasons such as "asdfg" and "ghjkl."[22]

Cleveland law enforcement has engaged in similar misuse. Officers are required to select an offense from drop-down menus before accessing the data.[23] But they regularly circumvent this requirement by using the catch-all "other." "Other" was the third most common reason selected in Cleveland police searches over a four-month period earlier this year.[24]

Making matters worse, there is little meaningful oversight on law enforcement's ALPR use—both nationwide and in Cleveland. The State of Ohio has no audit requirements, leaving compliance with any policies local departments choose to adopt almost entirely self-policed. Cleveland police policy promulgated in October 2025 requires the department to release a report on its ALPR usage annually and also requires the city's Real Time Crime Center to conduct an ALPR

---

[22] *Id.*

[23] Drown, *supra* n.18.

[24] Frank W. Lewis & Cid Standifer, *Cleveland may extend its Flock license plate reader contract*, Signal Cleveland (June 11, 2026), https://signalcleveland.org/cleveland-may-extend-its-flock-license-plate-reader-contract-heres-what-we-know/.

system audit annually.[25] Neither report has been produced to date.

Audits also promise more oversight than they deliver. Flock's system allows agencies to generate and download audit logs of every search.[26] Cleveland Police have not revealed whether they engage in these audits. Even if they do, audit logs only provide meaningful accountability if officers enter genuine, detailed justifications, if agencies actually download and review the records, and if there are consequences for misuse.

At the individual level, lack of oversight leads to concrete harms. Officers from agencies across the country have used ALPR data to stalk their romantic partners.[27] Earlier this year, Kansas police used their ALPR system to pursue someone who wrote a critical op-ed about the police department.[28] New York police collected license plate data to track Muslims and identify mosque

---

[25] *Automatic License Plate Readers*, *supra* n.**Error! Bookmark not defined.**.

[26] *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).

[27] *See* Va. State Crime Comm'n, *2024 Annual Report* 30-31 (June 30, 2025), https://perma.cc/PZ3M-VTHB; Brian Kerhin, *Menasha Officer Pleads Not Guilty to Misconduct Charge Over Ex-girlfriend Tracking*, Fox11 News (Feb. 10, 2026), https://tinyurl.com/yj4ywctm.

[28] 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.

attendees,[29] and a recent investigation showed officers around the country using racist terms for the Romani people in their search reasons.[30] Another officer who was a serial burglar monitored license plate data "to determine if he had been identified as a suspect for his crimes."[31]

### 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.[32] Vendors like Flock facilitate and encourage this data sharing. This transforms a discrete local

---

[29] Adam Goldman & Matt Apuzzo, *With Cameras, Informants, NYPD Eyed Mosques*, AP (Feb. 23, 2012), https://perma.cc/UX2Y-W5AW.

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

[31] *See* Va. State Crime Comm'n, *supra* n.27, at 30.

[32] *See National LPR Network*, *supra* n.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).

surveillance program into a node in a vast, interconnected network.

Flock data sharing takes several forms. Agencies can share on a one-to-one basis with a specific agency partner,[33] or they can open their network to all agencies statewide[34] or to Flock's entire national sharing network.[35] Once a sharing partner or network is selected, agencies automatically and continuously share all ALPR data with those partners.[36] Private entities with Flock cameras, such as homeowners associations, apartment complexes, business districts, schools,[37] national chain stores,[38] and malls across the country,[39] can also share the data they collect with law enforcement. "So long as customers give their consent, other

---

[33] *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).

[34] *See Introducing, Flock's National and Statewide Law Enforcement Search Network*, *supra* n.32.

[35] *See National LPR Network*, *supra* n.3.

[36] *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" customers can choose to "revoke").

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

[38] Koebler, *supra* n.32.

[39] 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.

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 the agency or private entity's data retention practices, historical searches could access data dating back years.[40]

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, updated 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, neighborhoods, and businesses—all working as one."[41] 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.[42]

Alarmingly, Flock's continuous sharing features can apparently be activated

---

[40] *See* Va. State Crime Comm'n, *supra* n.27, at 16 (retention periods ranging from three minutes to five years).

[41] *See National LPR Network*, *supra* n.3.

[42] 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/.

inadvertently, allowing for broad, unauthorized access to sensitive driver location data even without an agency's knowledge or affirmative opt-in. 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.[43] These agencies claim they were unaware that Flock's nationwide sharing features had been activated, an assertion Flock itself has since confirmed.[44] 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.[45] This only underscores the privacy risks inherent in an underregulated 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

---

[43] 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.

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

[45] *Id*.

across the state and country. This also dramatically inflates the number of times an agency's ALPR data is queried. For example, from January to mid-May this year, there were nearly 8 million searches of Cleveland's Flock system.[46] Only 14% of the searches came from departments in Ohio, and around 1% were made by Cleveland police.[47] The vast majority of the searches were conducted outside of the locality and even the state. The state that searched Cleveland's cameras the most was Texas, beating out Ohio.[48] The Houston and Dallas police departments alone made up 9% of the total searches.[49]

Second, the inverse is equally true: local law enforcement agencies using the Flock network, like Cleveland police, can now track a person's movements far beyond their own city limits, and far beyond the reach of their own cameras. Because Cleveland police can access out-of-state agencies' ALPR data, an officer can easily query ALPR data throughout the entire state or country to retrospectively track a vehicle's movements regardless of how far it traveled.

While Ohio places no restrictions on ALPR data-sharing with interstate or intrastate agencies, Cleveland has a checkered history of attempting to limit

---

[46] Lewis & Standifer, *supra* n.24.

[47] *Id.*

[48] *Id.*

[49] *Id.*

sharing. After public records revealed nearly 2,000 searches of Cleveland's ALPR network for immigration enforcement purposes between January and November 2025, the city attempted to use a filter offered by Flock to block searches explicitly tied to immigration enforcement and implemented restrictions on immigration data sharing with outside agencies.[50] This restriction apparently failed, and records revealed 163 immigration-related searches between December 28, 2025, and January 27, 2026.[51] In July 2026, in response to criticism about misuse, Cleveland passed an emergency ordinance extending its contract with Flock and requiring outside agencies to get a warrant to access Cleveland's ALPR data.[52]

In other states, legislative prohibitions on data sharing have been repeatedly circumvented. California has prohibited out-of-state and federal sharing of ALPR data since 2016;[53] yet, a decade later, agencies throughout the state continue to share in violation of the law. Last fall, for example, the San Francisco Police

---

[50] Sean McDonnell, *Newly released records show nearly 2,000 'immigration' and 'ICE' searches on Cleveland's Flock cameras*, Cleveland.com (Jul. 6, 2026), https://www.cleveland.com/news/2026/07/newly-released-records-show-nearly-2000-immigration-and-ice-searches-on-clevelands-flock-cameras.html.

[51] *Id.*

[52] Council of the City of Cleveland, Ordinance No. 683-2026 Section 2 (Jul. 15, 2026), *available at* https://www.clevelandcitycouncil.gov/pdf/web/viewer.html?file=/sites/default/files/2026-07/City%20Record%207-24-26.pdf.

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

Department allowed out-of-state and federal agencies to run 1.6 million illegal searches of its Flock database.[54] Investigations by news organizations have found apparent violations of the law to be "routine and widespread,"[55] and the California Attorney General is currently suing one agency for its violations.[56]

### D. Because ALPR Location Data Can Reveal 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 them. 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, and to predict where a driver may be in the future.[57] As one regional

---

[54] 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.

[55] 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.

[56] 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.

[57] 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.

California agency recognized, ALPR data can be "misused to infer" sensitive information "that is not relevant to police purposes," such as "non-relevant personal relationships; marital fidelity; religious observance; and political activities."[58]

Newer systems, like Flock's, that incorporate AI to create a "vehicle signature," collect even more revealing data. As mentioned above, Flock can track bumper stickers, which may have political statements. Flock has also added features like "convoy analysis," which lists vehicles that frequently travel with a searched vehicle, and "multi-geo search" which returns a list of all cars that have been to a given number of locations.[59] 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, ALPR technology poses acute dangers for politically vulnerable groups. License plate data is already being used to track and identify immigrants, abortion seekers, and people attending protests.

Although Immigration and Customs Enforcement (ICE) does not have a

---

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

[59] Ben Miller, *Flock Safety Gives Users Expanded Vehicle Location Abilities*, Gov't Tech. (Sept. 1, 2021), https://perma.cc/DUS6-GV7X.

contract with Flock, individual officers can get access through a "side door": federal officers simply ask local law enforcement to search their ALPR databases on the federal agency's behalf.[60] A trove of Flock data obtained by researchers this 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."[61] Officers logged reasons including "ICE," "ICE+ERO" (referring to ICE's Enforcement and Removal Operations), and "immigration."[62] Cleveland is no stranger to this practice. In 2025, Cleveland's Flock cameras were searched nearly 2,000 times to assist ICE or enforce immigration laws,[63] and officers gave reasons such as "immigration" "ICE" or "Border Patrol."[64] These searches came from as far away as the Texas Department of Public Safety and as close as the Parma, Columbus, and Port Clinton police departments.[65]

---

[60] 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* n. 34.

[61] 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/.

[62] *Id.(Mark for Jason Koebler & Joseph Cox).*

[63] Sean McDonnell, *supra* n.500.

[64] *Id.*

[65] *Id.*

Flock's nationwide sharing network has also been used to track at least one 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 Illinois law prohibited data-sharing for that purpose.[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] Cleveland's network has been searched for this purpose. From January 1 to May 13 this year, ten searches of Cleveland's ALPR network included the term "protest" as the search reason.[69] Only three of those searches came from the Cleveland police.[70]

---

[66] *See* Cox & Koebler, *supra* n.42; 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.

[69] Lewis & Standifer, *supra* n.24.

[70] *Id.*

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 because they consider themselves under constant surveillance."[71]

## II. THE USE OF MODERN ALPR SYSTEMS TO RETROSPECTIVELY TRACK INDIVIDUALS' MOVEMENTS IS A SEARCH UNDER THE FOURTH AMENDMENT.

The "basic purpose" of the Fourth Amendment is "to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Chatrie v. United States*, 146 S. Ct. 2193, 2204 (2026) (quoting *Carpenter v. United States*, 585 U.S. 296, 303 (2018)). "That purpose is central to decisions about whether a Fourth Amendment 'search' has occurred." *Id.* When the government exploits emerging technologies, the analysis of whether a Fourth Amendment "search" occurred takes account of whether the government's conduct threatens to disrupt the traditional "relationship between citizen and government in a way that is inimical to democratic society." *United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (cleaned up). Indeed, as "'[s]ubtler and more far-reaching means of invading privacy have become available to the Government,'" courts are "obligated . . . to ensure that the 'progress of science'

[71] *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.

does not erode Fourth Amendment protections." *Chatrie*, 146 S. Ct. at 2217 (quoting *Carpenter*, 585 U.S. at 320).

"Prior to the digital age, pursuing a suspect 'for any extended period of time was difficult and costly and therefore rarely undertaken.'" *Id.* at 2206–07 (quoting *Carpenter*, 585 U.S. at 310). "As a result, '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.'" *Id.* (quoting *Carpenter*, 585 U.S. at 310). Much less could they secretly monitor and catalogue the movements of *every* car, just in case one later turned out to be involved in a crime. But now, as discussed above, ALPRs allow officers to do just that, across Cuyahoga County and beyond. "What in the past was 'unknowable'"—for example, everyone who had driven to a particular church a month ago, or everywhere a person drove to in the past month—"suddenly becomes open to view, presenting formerly unimaginable 'privacy concerns.'" *Id.* at 2207 (quoting *Carpenter*, 585 U.S. at 311–12).

The district court below held that the officer's use of the ALPR system in this case was not a search because Mr. Sturdivant had "no reasonable expectation of privacy in the appearance of his vehicle or in his license plate number." *United States v. Sturdivant*, 786 F. Supp. 3d 1098, 1111 (N.D. Ohio 2025). But an officer observing the appearance of a vehicle and its license plate number with his own

eyes is a far cry from searching every record of that vehicle—and all other vehicles on the road—from the last month and then reconstructing its past movements.

The district court's ruling was based on its view that *Carpenter*—in which the Supreme Court held that obtaining a week's worth of one individual's historical cell-site location information is a Fourth Amendment search—was "a narrow decision dependent on the 'unique nature' of historical cell-site location data." *Id.* But less than a month after the district court issued its decision in this case, the Supreme Court clarified that its logic in *Carpenter* was not limited to cell-site location data, nor to searches that involved as many individual data points as that in *Carpenter* did. On the contrary, "[w]here the Fourth Amendment applies, it applies—regardless of 'the quality or quantity of information' the government obtains." *Chatrie*, 146 S. Ct. at 2210.

In *Chatrie*, the Supreme Court held that "an individual has a reasonable expectation of privacy in records about his cell phone's location, and police intrude on that constitutionally protected interest when they demand the information—even though for only a limited time, and from a third-party tech company." *Id.* at 2199. While the *Chatrie* Court was considering a "geofence search," involving location history obtained from Google for all devices in a given area at a given time, its logic applies equally to obtaining information from ALPRs regarding cars in a given area at a given time.

Just like the location history at issue in *Chatrie* and the cell-site location information in *Carpenter*, ALPR data reveals sensitive, intimate information about people's travels, activities, and associations. Searching for a vehicle in an ALPR database gives officers a view into its driver's whereabouts over time, including "trips that a person is apt to think 'indisputably private': to 'the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, [or] the by-the-hour motel.'" *Id.* at 2210 (quoting *Jones*, 565 U.S. at 415 (opinion of Sotomayor, J.)).

The district court rejected Mr. Sturdivant's claims that the ALPR surveillance supplied law enforcement with an "intimate window" into his personal life—for example, by showing on which nights he stayed at his girlfriend's residence—because there was "no evidence in the record" indicating that law enforcement used the data to deduce Mr. Sturdivant's overnight locations and identify his girlfriend. *Sturdivant*, 786 F.Supp.3d at 1112–13. But the Court in *Chatrie* clarified that "[w]hether something is a search does not depend on what it finds." *Chatrie*, 146 S. Ct. at 2212. An officer who conducts a search of a home to find a gun must get a warrant; and his failure to do so violates the Fourth Amendment even if no gun was actually found. So too here. Even if the results of the search in this case did not actually reveal Mr. Sturdivant's overnight locations, law enforcement still conducted a search for that information. When an officer

queries an ALPR system, he "cannot know the fruits . . . in advance." *Id.* But querying an ever-expanding system of cameras that captures every vehicle passing by to uncover every record of a vehicle's location over the past month is a search, regardless of the output.

The fact that individuals travel on public roads to engage in their private activities does not defeat the reasonable expectation of privacy in their movements. *See id.* at 2206. Indeed, in *United States v. Jones*, five Justices agreed that using a GPS device to track a vehicle over a four-week period was a Fourth Amendment search, "even though the movements occurred in public." *Id.*; *United States v. Jones*, 565 U.S. at 430 (Alito, J., concurring); *id.* at 415 (Sotomayor, J., concurring); *see also Leaders of a Beautiful Struggle v. Baltimore Police Dep't*, 2 F.4th 330, 337, 345–346 (4th Cir. 2021) (holding that aerial surveillance of public places was a search). Cell phones, too, "move in public places where people can see you in plain view," yet it still "becomes constitutionally problematic when law enforcement can indiscriminately and passively catalog your whereabouts [using your cell phone] over an extended period of time and then use that information for any purpose whenever convenient." *United States v. Kyle*, No. 26-CR-00189-SEH, 2026 WL 2958728, at *13 (N.D. Okla. Oct. 1, 2026).

Nor does the fact that people leave their vehicles mean no reasonable expectation of privacy inheres in an individual's driving location history. After all,

"[t]he datasets in *Jones* and *Carpenter* had gaps in their coverage, too," but "in both cases, the surveillance still surpassed ordinary expectations of law enforcement's capacity and provided enough information to deduce details from the whole of 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"). And the Court in *Chatrie* flatly rejected the government's argument that accessing location information only for a short period—there, two hours—does not count as a Fourth Amendment search. 146 S. Ct. at 2209. The Court explained that it has "never understood Fourth Amendment protections as kicking in only once an intrusion 'goes too far.'" *Id.* at 2210 (quoting *Pennsylvania Coal Co. v. Mahon*, 260 U.S. 393, 415 (1922)). And "'[e]ven short-term monitoring' of a person's physical movements can provide 'a wealth of detail about [his] familial, political, professional, religious, and sexual associations.'" *Id.* (quoting *Jones*, 565 U.S. at 415 (opinion of Sotomayor, J.)).

Moreover, ALPR surveillance (like location history) "'runs against everyone'—not just those 'under investigation'—and 'travel[s] back in time.'" *Id.* at 2207 (quoting *Carpenter*, 585 U.S. at 312). With ALPRs, "the Government need not decide in advance the kind of surveillance it should undertake" or "who they want to follow and when." *Id.* at 2207-8. Instead, "with no real effort," police can

"reconstruct . . . people's comings and goings in any area." *Id.* at 2208. Thus, "[w]hoever the suspect turns out to be, . . . he has effectively been tailed every moment of every day." *Id.* (quoting *Carpenter*, 585 U.S. at 312). And "wherever a location of interest turns out to be (whether a crime scene or a protest march or even a private home), it has effectively been surveilled for the same boundless time." *Id.*

In one of the first cases after *Chatrie* to consider whether querying an ALPR system constitutes a Fourth Amendment search, the Northern District of Oklahoma held that it did. *See Kyle*, 2026 WL 2958728, at *14. Examining the ALPR system at issue, the court concluded it "credibly invokes concerns raised in both *Carpenter* and *Chatrie*." *Id.* at *13. The court reasoned that, while we might expect someone we know to tell us they saw us driving last week, "we do not expect people we know—let alone strangers, and especially not law enforcement—to randomly approach us to say: 'Hey, I have been following your car for the last 30 days, and here is a detailed log of every place your vehicle has been with supporting photographic evidence. I am also going to share this information with law enforcement throughout the country, so they know your whereabouts, too.'" *Id.* By giving law enforcement the ability to do just that, ALPR systems facilitate "a type of indiscriminate mass surveillance" that the Fourth Amendment forbids. *Id.* "Freedom from persistent, dragnet-style surveillance while in public is not a

foreign concept in our society, and it is a reasonable expectation that society already accepts," as reflected in *Carpenter* and *Chatrie*. *Id.*

Since the Founding, the Fourth Amendment has sought "to place obstacles in the way of a too permeating police surveillance." *Chatrie*, 146 S. Ct. at 2205 (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)). Thus, "[w]hatever the form of an attempted incursion, the Fourth Amendment protects Americans' long-held conviction that no government official should have free access to the most closely kept aspects of their lives." *Id.* Modern ALPR systems give police free access to "a virtual panopticon with which to scrutinize its citizens' activities." *Id.* at 2210. They facilitate prolonged tracking of millions of Americans, before the government has any reason to be suspicious of them, that reveals previously unknowable, intimate details of their lives. ALPRs thus violate reasonable expectations of privacy under the Fourth Amendment. The constitutional line must be drawn, and "[i]t is not too much to draw the line at indiscriminate mass surveillance." *Kyle*, 2026 WL 2958728, at *14.

## CONCLUSION

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

Dated: November 9, 2026

By: /s/ *Andrew Crocker*

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

*Counsel for Amicus Curiae Electronic Frontier Foundation*

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

*Counsel for Amicus Curiae American\ Civil Liberties Union*

Freda J. Levenson
ACLU of Ohio Foundation, Inc.
4506 Chester Avenue
Cleveland, Ohio 44103
Email: flevenson@acluohio.org
Telephone: (216) 541-1376

David J. Carey
ACLU of Ohio Foundation, Inc.
1108 City Park Avenue, Suite 203
Columbus, Ohio 43206
Email: dcarey@acluohio.org
Telephone: (380) 215-0997

*Counsel for Amicus Curiae American\
Civil Liberties Union of Ohio*

## CERTIFICATE OF COMPLIANCE AND SERVICE

I hereby certify that the foregoing brief of *Amicus Curiae* complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief is printed in proportionally spaced 14-point Times New Roman font, using Microsoft® Word for Mac 2011 and there are 6,493 words in the brief according to the word count of the word-processing system used to prepare the brief (excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii)). The brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5), and with the type style requirements of Fed. R. App. P. 32(a)(6).

I hereby certify that on November 9, 2026 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by placing a true and correct copy in the United States mail, postage prepaid, to their address of record.

Dated: November 9, 2026

By: /s/ Andrew Crocker
Andrew Crocker

*Counsel for Amicus Curiae*
*Electronic Frontier Foundation*