No. 26-1227

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

LEE SCHMIDT and CRYSTAL ARRINGTON,
Plaintiffs-Appellants,
v.
CITY OF NORFOLK, and MARK TALBOT, in his official capacity as the Norfolk Chief of Police,
Defendants-Appellees.

On Appeal from the United States District Court
for the Eastern District of Virginia
No. 2:24-cv-00621-MSD-LRL
The Honorable Mark S. Davis, U.S. District Court Judge

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF PLAINTIFFS-APPELLANTS AND URGING REVERSAL

Megan Iorio
Kabbas Azhar
Abigail Kunkler
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140
iorio@epic.org

Attorneys for Amicus Curiae

April 20, 2026

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: Schmidt v. City of Norfolk

Pursuant to FRAP 26.1 and Local Rule 26.1,

Electronic Privacy Information Center
(name of party/amicus)

who is amicus, 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/ Megan Iorio Date: April 20, 2026

Counsel for: Electronic Privacy Information Center

Print to PDF for Filing Reset Form

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

Michael Stavola, *Kansas Police Chief Used Flock License Plate Cameras 164 Times to Track Ex-Girlfriend.*, Wichita Eagle (Aug. 17, 2024) 24

Nicole Einbinder, *'Flock Flocked Up': How a License Plate Camera Misread Unraveled One Man's* Life, Business Insider (Mar. 9, 2026) 21, 22

Oona Milliken & Isabella Aldrete, *Vegas Police are Big Users of License Plate Readers. Public Has Little Input Because It's a Gift*, Nevada Independent (Feb. 22, 2026) 14

Rashida Richardson et al., *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. Rev. 192 (2019) 19

Sarah Brayne, *Big Data Surveillance: The Case of Policing*, 83 Am. Socio. Rev. 977 (2017) 18, 20

U.S. Dep't of Justice, Off. Att'y Gen., *The Attorney General's Report on Criminal History Background Check* (June 2006) 11

Vehicle Manager, Motorola Solutions 12

Virginia Dep't of Gen. Serv., *Approved Automated License Plate Recognition Systems* 12

Virginia State Crime Comm'n, *Law Enforcement Use of Automatic License Plate Recognition (ALPR) Update* (Jan. 2026) 4

Youngsub Lee et al., *The Effectiveness of Big Data-Driven Predictive Policing: Systematic Review*, 7 Just. Evaluation J. 127 (2024) 18

INTEREST OF THE AMICUS CURIAE[1]

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. EPIC regularly participates as *amicus curiae* in cases concerning emerging privacy issues, the Fourth Amendment, and mass surveillance technologies, including license plate readers. *See, e.g.*, Brief of *Amici Curiae* EPIC et al., *Chatrie v. United States*, 136 F.4th 100 (4th Cir. 2025), *cert. granted*, 2026 WL 120676 (Jan. 16, 2026); Brief of *Amici Curiae* EPIC et al., *Kansas v. Glover*, 140 S. Ct. 1183 (2020); Brief of *Amici Curiae* EPIC et al., *Carpenter v. United States*, 138 S. Ct. 2206 (2018); Brief of *Amici Curiae* EPIC et al., *Riley v. California*, 134 S. Ct. 2473 (2014).

[1] The Plaintiffs-Appellants and Defendants-Appellees consent to the filing of this *amicus curiae* brief. In accordance with Rule 29, the undersigned state that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

SUMMARY OF ARGUMENT

The Court should reverse the judgment of the district court and hold that Norfolk's warrantless operation of its mass surveillance Automated License Plate Reader (ALPR) system is an unreasonable search in violation of the Fourth Amendment. Two reasons compel this conclusion.

First, modern ALPR systems expose the "privacies of life" of everyday people to law enforcement. The Fourth Amendment assures the "degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo v. United States*, 553 U.S. 27, 34 (2001). Part and parcel of that constitutional analysis is looking to the evolving capabilities of a surveillance system and what it enables law enforcement to infer. That is why the Supreme Court in *Carpenter v. United States* looked to how the "Government could, *in combination with other information*, deduce a detailed log of Carpenter's movements," 585 U.S. 296, 312 (emphasis added), and that is why this Court's analysis in *Leaders of a Beautiful Struggle v. Baltimore Police Department* looked to "not only the raw data, but what that data can reveal," 2 F4th 330, 344 (4th Cir. 2021), when it assessed the constitutionality of Baltimore's Aerial Investigation Research (AIR) program.

This Court need only follow its own established rule here to find that modern ALPR systems are unconstitutional. Modern ALPR systems not only amass vast troves of sensitive location information but also knit it together with

other information—commercial and otherwise—that allows law enforcement to infer identity and monitor the habits and routines of everyday people. AI-enabled ALPR systems further allow law enforcement to instantly surface insights from these troves of data and permit continual monitoring for suspicious patterns. These capabilities far outstrip what law enforcement could do with manual review of the data, and evaluating modern ALPR systems as only a collection of a few scattered data points misses the forest for the trees.

Second, AI-enabled ALPR systems perpetuate discriminatory and potentially unconstitutional predictive policing practices. Built off unvetted, outdated, and inherently biased data that overrepresents poor and minority populations, modern ALPRs make enforcement recommendations and even automatically generate suspicion about individuals. Any decisions are made within a proprietary black box and under the guise of objectivity, limiting anyone's ability to understand or challenge them. In this way, ALPRs apply enforcement unequally and obstruct constitutional rights guaranteed by the Fourth, Fifth, and Sixth Amendments. Absent strict safeguards, ALPRs revive the arbitrary powers of the reviled general warrant and undercut democracy. A warrant is the proper first obstacle to place in the way of this too-permeating police surveillance.

ARGUMENT

On any given day, networked systems of Automated License Plate Reader ("ALPR") cameras capture the movements of hundreds of thousands of people going about their daily lives.[2] Each camera, placed at a busy intersection or "high-crime" area, JA9, takes a photo whenever a person passes by in their vehicle. This image records where the person is at a particular time, in which direction the person is headed, and in what vehicle the person is traveling. Once a photo is captured, the ALPR system automatically compares the image and extracted license plate number against hot lists of vehicles that are of interest to law enforcement agencies. These lists may include stolen vehicles, vehicles associated with persons of interest, or vehicles otherwise considered suspicious. If a vehicle matches one on a hot list, law enforcement officers—including those using Flock—are typically notified in real time. The image and associated information

[2] As of 2020, every police department serving over one million residents and about 90% of sheriffs' offices with 500 or more sworn deputies were already using ALPRs. *See* Kristin Finklea, Cong. Rsch. Serv., R48160, *Law Enforcement and Technology: Use of Automated License Plate Readers* (2024). In 2025, the Virginia State Crime Commission sent out a survey to all 361 Virginia law enforcement agencies to determine ALPR usage. Of the 251 agencies that responded, 63% reported using ALPRs. Of those using ALPRs, 86% reported using Flock Safety as their ALPR vendor. Virginia State Crime Comm'n, *Law Enforcement Use of Automatic License Plate Recognition (ALPR) Update*, 4-7 (Jan. 2026), https://vscc.virginia.gov/2026/VSCC%20ALPR%20Report%20January%202026%20FINAL%20REVISED%20Jan%2021%202026.pdf.

are also stored in a database for a default period (up to 21 days in Virginia's case),[3] or far longer if such data is deemed relevant to an ongoing investigation or legal action. *See* Va. Code § 2.2-5517. With the help of the ALPR system, an officer can connect these photos to potentially hundreds of images that reflect where a person was going in their vehicle at other times.

An AI-enabled ALPR system like Flock has other features convenient to law enforcement agencies: it can stream live video and capture clips, JA146; it can point out if other vehicles were traveling with someone officers are interested in, JA141; and it can look at a vehicle's past travel history and offer probabilities for where the vehicle might go next, *id*. Still more features are being introduced or are in development. Officers can now instantly match a suspected vehicle with a range of other data including the owner's address, where they might work or go to school, to whom they are related, and with whom they spend time. Joseph Cox, *License Plate Reader Company Flock is Building a Massive People Lookup Tool, Leak Shows*, 404 Media (May 14, 2025).[4] All of this happens, day in and day out, without a single warrant ever being issued. This is the world we live in. It is not the world that the Fourth Amendment allows.

---

[3] At the time of the events relevant to this case, Virginia law allowed ALPR image data to be stored by default for up to 30 days.

[4] https://www.404media.co/license-plate-reader-company-flock-is-building-a-massive-people-lookup-tool-leak-shows/.

The Court should reverse the judgment of the district court and hold that Norfolk's warrantless operation of its mass surveillance ALPR system is an unreasonable search in violation of the Fourth Amendment. The Supreme Court has recognized two critical guideposts for resolving which expectations of privacy are entitled to protection under the Fourth Amendment. First, the Fourth Amendment secures "'the privacies of life" against 'arbitrary power.'" *Carpenter v. U.S.*, 585 U.S. 296, 305 (2018) (citing *Boyd v. United States*, 116 U.S. 616, 630 (1886)). Second, it places "'obstacles in the way of a too permeating police surveillance.'" *Id.* (citing *United States v. Di Re*, 332 U.S. 581, 595 (1948)). Both call for this Court to hold that the warrantless collection of personal data via ALPR systems violates the Fourth Amendment.

Amicus emphasizes two points in support of this conclusion. First, courts must look at the entirety of modern ALPR systems' capacity to reveal the "privacies of life" when assessing their constitutionality. This evaluation must account for both the panoply of data that undergirds ALPR systems and their sophisticated analytical capabilities, current and emerging. Second, warrants are the proper first obstacle to place in the way of the too permeating police surveillance posed by ALPR systems that extend historic patterns of discrimination, obscure decision-making, and threaten to subvert constitutional rights against arbitrary power.

I. Modern ALPR systems reveal the "privacies of life."

In determining whether the use of a particular surveillance tool violates a reasonable expectation of privacy, the Supreme Court has relied on a holistic analysis that accounts for the evolving nature of such technologies. To that end, a court subjecting a surveillance system to Fourth Amendment scrutiny must consider the full range of its capabilities, including the inferences the system allows or may later enable. Modern ALPR systems are sharply different from earlier ALPR systems in how they operate and what they can reveal. They store massive troves of location data, unlike traditional security cameras, and will soon link to vast quantities of commercial data that make it easy to infer identity. AI-enabled ALPR systems take this a step further, surfacing insights without traditional queries and revealing life patterns and habits. At bottom, these systems enable the exercise of "arbitrary power" and "too permeating police presence" that the Fourth Amendment protects against. *Carpenter*, 585 U.S. at 305.

A. Modern ALPR systems must be evaluated according to their evolving capabilities and the inferences they enable.

The Supreme Court's Fourth Amendment jurisprudence looks to a technology's evolving capabilities. In *Kyllo*, the Court rejected a "mechanical interpretation" of the Fourth Amendment that would leave people at the mercy of advancing technology when it ruled that thermal imaging of a home constituted a search. *Kyllo*, 533 U.S. at 35–36 . Thus, it held that its rule "must take account of

more sophisticated systems" already in use or in development. *Id.* at 36. Seventeen years later, *Carpenter* followed. There, the Court took note of the rapidly increasing accuracy of CSLI even as the factual record "reflect[ed] the state of the technology at the start of the decade[.]" *Carpenter*, 585 U.S. at 313. As *Carpenter* reflects, accounting for this sophistication must include an assessment of the information that a given technology allows to be inferred. Even though the Government maintained that location records "'did not on their own suffice to place [Carpenter] at the crime scene,'" the Court looked to how those location records "could, in combination with other information, deduce a detailed log of Carpenter's movements[.]" *Id.* at 312. Looking at the location data alone would otherwise allow inferences made from the search to escape appropriate scrutiny. *Id*. (citing *Kyllo*, 533 U.S. at 36).

When assessing an aerial drone surveillance program that enabled tracking of individuals across the City of Baltimore, this Court held that "*Carpenter* applie[d] squarely," *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 341 (4th Cir. 2021), and that the aggregation and processing of such drone imagery constituted a search under the Fourth Amendment. Despite gaps in coverage, police could deduce identities by "cross-referenc[ing] against publicly available information and, even more valuably, their own data systems." *Id.* at 344. The program "transcend[ed] mere augmentation of ordinary police capabilities,"

and "[w]ith analysis, it c[ould] reveal where individuals come and go over an extended period of time." *Id.* at 345–46. And because "the AIR [Aerial Investigative Research] program enable[d] police to deduce from the whole of individuals' movements," the Court held that "accessing its data [was] a search, and its warrantless operation violate[d] the Fourth Amendment." *Id.* at 346.

Several courts—not "wish[ing] to speculate about what the future may hold for [ALPR] capabilities," JA3 (citing *United States v. Martin*, 753 F. Supp.3d 454, 476 (E.D. Va. 2024))—have rejected Fourth Amendment challenges to the warrantless uses of such surveillance tools. Unfortunately, the future of these systems is no longer a matter of speculation. Current ALPR systems are not the "conventional surveillance techniques and tools" that *Carpenter* carved out. JA32. Like Baltimore's AIR system, Flock and other ALPR systems piece together disparate sources of information at massive scale. In concluding that "scattered ALPR data points" were not a search because they "simply…contribute[d] one or more pieces to a larger investigative jigsaw puzzle," JA49, the district court failed to heed the lesson of *Leaders of a Beautiful Struggle*.

Flock does not just photograph license plates. Nor is it just a camera network. Its system is undergirded by continuously updating hotlists, commercial datasets, other law enforcement databases, and more. It incorporates artificial intelligence (AI) to instantly surface insights based on millions of datapoints.

Focusing on the mere collection of images of license plates alone ignores the broader architecture of ALPR systems, which "enable[] police to deduce from the whole of individual's movements[.]" *Leaders of a Beautiful Struggle*, 2 F.4th at 346.

B. Modern ALPR systems reveal tremendous amounts of information.

To be sure, the location information captured by ALPR systems is, by itself, enough to reveal the "privacies of life." *Carpenter*, 585 U.S. at 311. Location information provides an intimate window into a person's life, "revealing not only his particular movements, but through them his familiar, political, professional, religious, and sexual associations." *Id*. Most people "start and end most days at home," meaning that even a few points of location data can reveal habits that uniquely identify people. *Leaders of a Beautiful Struggle*, 2 F.4th at 343. These habits enable deductions about "'what a person does repeatedly, what he does not do, and what he does ensemble[.]'" *Id.* at 342 (citing *United States v. Maynard*, 615 F.3d 554, 562-563 (D.C. Cir. 2010)). While the district court below discounted the Flock location data because it differed from GPS/CSLI data, JA41–42, "the source of the underlying location data is entirely irrelevant[.]" *Leaders of a Beautiful Struggle*, 2.F4th at 343-44 (rejecting district court's decision to discount study showing ability to infer identity from location data because study was based on CSLI and the AIR program was not). What matters is whether you can deduce a

person's identity from said data. In any case, ALPR location data allows just that. *See* Jing Gao, Lijun Sun & Ming Cai, *Quantifying Privacy Vulnerability of Individual Mobility Traces: A Case Study of License Plate Recognition Data*, 104 Transp. Rsch. Part C: Emerging Technologies 78 (2019) (five location data points over half a day are enough to uniquely identify 90% of people). Norfolk's ALPR cameras collected over 41 million photographs with associated location data in just a month. JA136. That is more than enough to constitute an unreasonable search.

But Flock and other modern ALPR surveillance products go far beyond collection of location information. The standard hot lists that Flock runs incorporate a bevy of data; the FBI's National Crime Information Center hotlist alone draws information from 13 different federal data sources,[5] and with dubious accuracy.[6] Flock also allows officers to create and share custom hot lists with no

[5] Data sources include: Vehicle, License Plate, Wanted Person, Protection Order, Extreme Risk Protection Order, Missing Person, Gang, Threat Screening Center, Supervised Release, National Sex Offender Registry, Immigration Violator, Protective Interest, and Violent Person. FBI CJIS Division, *License plate reader data extract in NCIC* (June 4, 2024), https://le.fbi.gov/cjis-division/cjis-link/license-plate-reader-data-extract-in-ncic.

[6] In 2006, the Attorney General released a report on FBI's criminal background check system and reported that fifty percent of the criminal arrest records in the Interstate Identification Index, which is incorporated into NCIC data, were missing final disposition information such as whether the person was acquitted or even charged. U.S. Dep't of Justice, Off. Att'y Gen., *The Attorney General's Report on Criminal History Background Check*, 3 (June 2006), https://bjs.ojp.gov/sites/g/files/xyckuh236/files/media/document/ag_bgchecks_report.pdf.

clear guardrails on criteria for inclusion.[7] Thus, each time an ALPR camera takes a photo of any passing vehicle, that image is *immediately* cross-referenced against reams of data to identify vehicles of interest. Further, modern ALPR systems vastly expand surveillance networks via private-public partnerships. Far beyond the investigative technique of "accessing [] citizen provided doorbell camera footage," JA49, modern ALPR systems provide centralized, real-time, around-the-clock access to private feeds. Jason Koebler, *Home Depot and Lowe's Share Data from Hundreds of AI Cameras with Cops*, 404 Media (Aug. 6, 2025).[8] For example, Norfolk law enforcement have 24/7 access to the entire state-wide Home Depot Flock network. JA216. This far exceeds the analysis that would be possible with manual law enforcement review.

Nor do modern ALPR systems stop there: they also incorporate massive databases of existing license plate captures. Motorola Solutions, for example, boasts of access to "billions of detections beyond your own" via its Vehicle Manager[9] and is an approved ALPR vendor under Virginia law. Virginia Dep't of

---

[7] When asked how law enforcement officials were able to make a hot list for a missing person if making such a list required a documented criminal predicate, Mark Talbot, Chief of Norfolk Police, Mark Talbot responded, "there are certainly ways." JA1113-1114.

[8] https://www.404media.co/home-depot-and-lowes-share-data-from-hundreds-of-ai-cameras-with-cops/.

[9] Vehicle Manager, Motorola Solutions (last visited Apr. 16, 2026), https://www.motorolasolutions.com/en_xl/video-security-access-control/license-

Gen. Serv., *Approved Automated License Plate Recognition Systems* (last visited Apr. 13, 2026).[10] These databases are "retrospective" and give police access to "otherwise unknowable" information. *Carpenter*, 585 U.S. at 312. And they stand to grow: "Flock Nova" integrates various commercial data broker and other open-source intelligence sources that, as one Flock employee put it, helps "jump from plate to person . . . link to other people that are related to that person [] marriage or through gang affiliation[.]" Cox, *supra*. Flock Nova knits together data from credit bureaus such as Experian and Transunion, public information such as property and occupancy data, and open-source social media intelligence scraped together by data brokers. *Id.* Flock Nova, as Flock puts it, is not just an ALPR system that captures photos: "it consolidates, actions, and visualizes connections in data" for law enforcement. Flock Safety, *Correcting the Record: Flock Nova will not Supply Dark Web Data* (May 30, 2025).[11] Select agencies had early access to the product as of February 2025. *See* Flock Safety, *Flock Nova - Early Access Application* (last visited Apr. 16, 2026) (noting early access to Flock Nova beginning in February

---

plate-recognition-camera-systems/vigilant-vehiclemanager-lpr-analytics-software.html.

[10] https://dgs.virginia.gov/content/dam/site-assets/dps/Documents/specifications/VA-230420%20Breakout%20of%20Products%20-%20DGS.pdf.

[11] https://www.flocksafety.com/blog/correcting-the-record-flock-nova-will-not-supply-dark-web-data.

2025);[12] *see also* Flock Nova™, Flock Safety (last visited Apr. 17, 2026) (Mt. Juliet PD set up Flock Nova within 30 days);[13] Oona Milliken & Isabella Aldrete, *Vegas Police are Big Users of License Plate Readers. Public Has Little Input Because It's a Gift*, Nevada Independent (Feb. 22, 2026) (reporting that Horowitz Family Foundation donated millions to the Las Vegas Metropolitan Police Department Foundation in October 2025 to purchase Flock Nova subscriptions while evading public scrutiny).[14]

AI-enabled ALPR systems are set to further exploit their accumulated troves of location data. Flock's "FreeForm" AI tool allows officers to search such data with open-ended search terms across millions of data points. *See* Flock FreeForm™, Flock Safety (last visited Apr. 16, 2026).[15] Flock's patent for its query tool explicitly outlines its potential ability to identify "different classes of people (male, female, race, etc.)." System and Method for Object Based Query of Video Content Captured by a Dynamic Surveillance Network, U.S. Patent No. 11,416,545 B1 col. 19 l. 16-17 (filed Oct. 4, 2020) (issued Aug. 16, 2022). And it is trivial to run a facial recognition algorithm on an existing database of photos such as

[12] https://docs.google.com/forms/d/e/1FAIpQLSeBUthV7qH11nBEGWr-2DkBN8Po6m4Y7d019W53d-6qC4Xo4A/viewform.
[13] https://www.flocksafety.com/products/flock-nova.
[14] https://thenevadaindependent.com/article/vegas-police-are-big-users-of-license-plate-readers-public-has-little-input-because-its-a-gift.
[15] https://www.flocksafety.com/products/flock-freeform.

Flock's. "Investigations Manager" and "Multi-State Insights" products analyze surveillance data to flag patterns that suggest criminal behavior. Jay Stanley, *Surveillance Company Flock Now Using AI to Report Us to Police if it Thinks Our Movement Patterns Are "Suspicious,"* ACLU (Jul. 23, 2025).[16] Features such as "Convoy Analysis" and "Real-Time Routing," which identify suspicious accompanying vehicles and project probabilistic routes, JA142, do precisely what this Court has identified as requiring a warrant: enable "deduc[tions] from the whole of an individuals' movements." *Leaders of a Beautiful Struggle,* 2 F.4th at 346.

The abuse of such systems is already underway. In late 2025, investigative journalists unveiled a Customs and Border Protection (CBP) program that flagged vehicles with suspicious driving patterns using its nationwide network of ALPR cameras. Byron Tau & Garance Burke, *Border Patrol is Monitoring US Drivers and Detaining Those with 'Suspicious' Travel Patterns*, AP News (Nov. 20, 2025).[17] CBP officers then flagged drivers for local law enforcement to stop on a pretextual basis, citing to traffic code violations when the basis for the stop was entirely different. *Id.* CBP's Conveyance Monitoring and Predictive Recognition

[16] https://www.aclu.org/news/national-security/surveillance-company-flock-now-using-ai-to-report-us-to-police-if-it-thinks-our-movement-patterns-are-suspicious.
[17] https://apnews.com/article/immigration-border-patrol-surveillance-drivers-ice-trump-9f5d05469ce8c629d6fecf32d32098cd.

System program runs exactly like Flock does; it "collects license plate images and matches the processed images against established hot lists to assist . . . in identifying travel patterns indicative of illegal border related activities." *Id.* Indeed, Flock and Vigilant were two of the three commercial vendors that CBP obtained license plate data from to help run this program. *Id.*

The same mass surveillance programs are poised to be turned on everyday people by local law enforcement all across America. They are far from the "conventional surveillance techniques and tools" that *Carpenter* carved out, 585 U.S. at 315, and far from simply a "more resource-efficient surveillance method," *United States. v. Vankesteren,* 553 F.3d 286, 291 (4th Cir. 2009). Modern ALPR systems reveal "the privacies of life," *Carpenter*, 585 U.S. at 311, and "enable[] police to deduce from the whole of individual's movements." *Leaders of a Beautiful Struggle*, 2 F.4th at 346. They constitute precisely the sort of "arbitrary power" and "too permeating police surveillance" that the Fourth Amendment was designed to forestall. *Carpenter*, 585 U.S. at 305. As such, this Court should find that the warrantless use of modern ALPR systems like Flock constitutes an unreasonable search.

II. AI-enabled ALPR systems perpetuate unconstitutional predictive policing and reinstate general warrant powers incompatible with democracy.

ALPRs are a form of predictive policing, systems that incorporate often unvetted, outdated, and biased data to make enforcement decisions on behalf of police, at times with AI. These systems hide biased policing under a guise of objectivity and dilute the Fourth Amendment by removing individualized suspicion and shrouding decision-making. In effect, ALPR predictive policing revives the general warrant and facilitates arbitrary power. Networked and AI-enabled ALPR systems are compatible with neither the Fourth Amendment nor a healthy democracy—at least absent significant constraints.

A. AI-enabled ALPR systems facilitate discriminatory and potentially unconstitutional predictive policing practices.

ALPR predictive policing entrenches discriminatory policing and diminishes Fourth Amendment rights. Built off of data that overrepresents poor and minority communities, and deployed in areas populated by those communities, such policing necessarily entrenches patterns of discrimination and renders some more susceptible to search and seizure based on their identity or residence alone. Fourth Amendment protections are further diluted when an ALPR system uses AI to *generate* suspicion about individuals. The decisions made by an ALPR system are cloaked in objectivity and hidden in a proprietary black box, making it nearly

impossible for someone to fully vindicate their rights under the Fourth and Fifth Amendments.

1. Modern ALPRs are predictive policing systems.

"Predictive policing" refers to computer systems that combine and analyze data using AI techniques to predict when or where a crime will happen or who will be involved. Elizabeth Joh*, Policing by Numbers: Big Data and the Fourth Amendment*, 89 Wash. L. Rev. 35, 42–48 (2016). These systems make judgments using vast and diverse data at a scale, depth, and speed that no law enforcement agency could manage with traditional policing methods, surfacing connections that were previously unknowable. *See generally* Sarah Brayne, *Big Data Surveillance: The Case of Policing*, 83 Am. Socio. Rev. 977, 977 (2017). Despite wide adoption, predictive policing systems have "at best, questionable effectiveness[.]" *See United States. v. Curry*, 965 F.3d 313, 344 (4th Cir. 2020) (Thacker, J. & Keenan, J., concurring); *see also* Youngsub Lee et al., *The Effectiveness of Big Data-Driven Predictive Policing: Systematic Review*, 7 Just. Evaluation J. 127, 127 (2024).

AI-enabled ALPRs are part of larger predictive policing systems. First, like other predictive policing tools, *see* David Robinson & Logan Koepke, *Stuck in a Pattern: Early Evidence on "Predictive Policing" and Civil Rights*, Upturn at 2–3

(Aug. 2016),[18] Norfolk's ALPRs are clustered in "high-crime" areas, JA9, necessarily increasing scrutiny of certain groups and casting residents as inherently suspicious. *See Curry*, 965 F.3d at 330–31; *id*. at 331-334 (Gregory, C.J., concurring). Second, through a Real Time Crime Center like Norfolk's, JA228–232, or within an AI-enabled ALPR system like Flock's, data captured by the ALPR is combined with other information to unearth likely travel routes, identify associations, and report suspicious drivers. Tau & Burke, *supra.* Like other predictive policing, there is little evidence that ALPRs work to reduce or prevent crime. Jason Koebler, *Let's Talk About the Flock Study that Says It Solves Crime*, 404 Media (Mar. 20, 2024).[19]

2. Predictive policing entrenches patterns of discrimination, shrouds decision-making, and threatens constitutional rights.

Bias is a fact of data. This is particularly true for predictive policing, which is built atop historic police enforcement patterns riddled with systemic discrimination. *Curry*, 965 F.3d at 344–45 (Thacker, J., & Keenan, J., concurring). Coupling these distorted datasets with unverified information from data brokers, web scraping, and public records, ALPR predictive policing is bound to extend the judgments and biases inherent to the data. *See* Rashida Richardson et al., *Dirty*

[18] https://www.upturn.org/static/reports/2016/stuck-in-a-pattern/files/Upturn_-_Stuck_In_a_Pattern_v.1.01.pdf.
[19] https://www.404media.co/researcher-who-oversaw-flock-surveillance-study-now-has-concerns-about-it/.

Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice, 94 N.Y.U. L. Rev. 192, 16–26 (2019). At one point Flock even planned to include illegally gained data leaked through data breaches, Cox, *supra*, though the company backtracked on its plan following public outcry.

The risks of ALPR predictive policing are not borne equally by the public. While ALPR systems universally lower the threshold for inclusion in a police database, the likelihood of being put into the system is not randomly distributed. Rather, the system is populated by the movements of particular groups (most often poor people and people of color). Brayne, *supra*, at 979, 996–1000. This is true in Norfolk, where cameras were placed by Flock in clusters based on crime and service call rates. JA9. The same groups overrepresented in ALPR databases are also overrepresented in the datasets ALPRs connect with to make policing decisions. Brayne*, supra*, at 996–1000. This vicious cycle of distorted data collection heavily skews which populations are policed and leads to cascading inequalities as individuals avoid other necessary social systems, such as healthcare, in an attempt to avoid even further inclusion. *Id*. The data collection underpinning ALPRs thus "shape[s] the behavior of the police and the public" and is imminently relevant to an "informed constitutional determination." *Curry*, 965 F.3d at 336 (Wynn, J., concurring).

ALPR predictive policing outsources police discretion and diminishes the constitutional guarantee of equal protection from unreasonable stops, searches, and arrests. To pull someone over ordinarily requires an officer to form a reasonable suspicion about that person. Modern ALPRs significantly weaken this constraint, manufacturing suspicion automatically and independently based on information that may never be specifically articulated beyond the tautological statement that "the person was suspicious because they drove suspiciously." *See id*. at 335. Because the system operates under a patina of objectivity, an officer is unlikely to question the recommendation. *See* Eric Bogart et al., *Humans Rely More on Algorithms than Social Influence as a Task Becomes More Difficult*, 11 Sci. Rep. (Apr. 13, 2021); *see also* Nicole Einbinder, *'Flock Flocked Up': How a License Plate Camera Misread Unraveled One Man's Life*, Business Insider (Mar. 9, 2026).[20] Again, this suspicionless policing will apply unevenly, making some more susceptible to search and seizure based on who they are or where they live—an approach "emphatically rejected" by this Court. *See Curry*, 965 F.3d at 331. This model cannot be reconciled with the salutary limitations on traditional policing; the targeted investigation of individuals is not akin to the perpetual, suspicionless policing of entire populations. *See* Joh, *supra*, at 61.

[20] https://www.businessinsider.com/flock-safety-alpr-cameras-misreads-2026-3.

Modern ALPRs also threaten to erode rights to due process and confrontation. ALPR predictive policing happens within a proprietary black box system. While general data sources have been identified—either by Flock or external reporting, *see* Cox, *supra*—many other important factors are obscured from view. The precise sources and categories of information contained and cross-referenced by the Flock system, Flock's methods for processing data, the factors on which the ALPR system bases its recommendations, the weight afforded to those factors, and the system's error rates all remain unknown. Yet these facts are essential for individuals to understand the evidence against them or to adequately vindicate their rights after being wrongfully arrested, held at gunpoint, or even mauled by police dogs. *See* Einbinder, *supra*.

B. The bulwark that the Fourth Amendment provides against the arbitrary exercise of power is subverted by modern ALPR systems.

While privacy is a central concern of the Fourth Amendment, it is not the only one. Rather, the Framers chose privacy as the mechanism by which the Fourth Amendment would deter arbitrary power, defeat oppression, and preserve the political and personal expression necessary for the democracy they envisioned. *See Carpenter*, 585 U.S. at 305; *see also* Matthew Tokson, *Artificial Intelligence and the Anti-Authoritarian Fourth Amendment*, 27 J. Const. L. 1068, 1090–93 (2025). Pervasive and unaccountable AI-enabled ALPR systems run contrary to this, instead resembling the reviled general warrant and enabling the very arbitrary

power the Founders rejected. *Id*. At a minimum, the answer to such a system should be: "get a warrant." *Riley v. California*, 573 U.S. 373, 401 (2014).

The Fourth Amendment was created in response to general warrants that allowed British authorities to arbitrarily rummage for evidence of criminal doings at any time. *See id*., at 27–28. AI-driven policing tools like ALPRs functionally revive the general warrant, eroding key democratic protections and turning the Fourth Amendment on its head. First, such systems diminish structural checks on state authority. Tokson, *supra*, at 1083–85. Despite the breadth and depth of the information, always-on ALPR policing is incredibly cheap. *Joh*, *supra*, at 48. As costs dwindle and storage capacity increases, ALPRs have become staggeringly ubiquitous and internetworked. *See* Section I, *infra*. Police may evade Fourth Amendment scrutiny by relying on systems like Flock that automatically incorporate and analyze vast quantities of data across jurisdictions. These systems are often cut off from public oversight by assertions that transparency would reveal trade secrets or confidential business information. *See supra* Section II.A.3. Self-regulation cannot close this structural loophole when individuals (including police officers) tend to follow algorithmic recommendations with little pushback. *See* Section II.A.2.

AI-enabled ALPRs likewise facilitate abuses of power akin to the general warrant. *See* Tokson, *supra*, at 1087–89. Like the general warrant, ALPR policing

is applied broadly to entire populations, enabling the state to both generate suspicion and marshal evidence post hoc. Moreover, there is a well-documented pattern of abuse of Flock tools. Law enforcement personnel have used them to stalk ex-girlfriends, Michael Stavola, *Kansas Police Chief Used Flock License Plate Cameras 164 Times to Track Ex-Girlfriend.*, Wichita Eagle (Aug. 17, 2024),[21] track protestors, Dave Maass & Rindala Alajaji, *How Cops Are Using Flock Safety's ALPR Network to Surveil Protestors and Activists*, EFF (Nov. 20, 2025),[22] and provide ICE a backdoor to systems it is otherwise barred from accessing, Jason Koebler & Joseph Cox, *ICE Taps into Nationwide AI-Enabled Camera Network, Data Shows*, 404 Media (May 27, 2025).[23] All of this happens within proprietary black box systems that are largely invisible to those targeted. The result is police surveillance marked by corruption, diminished oversight, and chilled dissent. *See generally* Tokson, *supra*.

A warrant is the proper first obstacle to this "too permeating police surveillance." *Carpenter*, 585 U.S. at 305. Internal law enforcement policies and protocols are not enough to restrain a system that sweeps in a great deal of information from disparate sources and treats every person as a potential suspect.

---

[21] https://www.kansas.com/news/politics-government/article291059560.html.
[22] https://www.eff.org/deeplinks/2025/11/how-cops-are-using-flock-safetys-alpr-network-surveil-protesters-and-activists.
[23] https://www.404media.co/ice-taps-into-nationwide-ai-enabled-camera-network-data-shows/?ref=daily-stories-newsletter.

See Riley, 573 U.S. at 395, 397. Indeed, such protocols have already failed. *See* Koebler & Cox, *supra*. Enforcing a warrant requirement on AI-enabled ALPRs will help to restore the accountability and protection of privacy necessary for a thriving democracy.

CONCLUSION

For the foregoing reasons, *amicus* respectfully urges this Court to reverse the district court's grant of summary judgment in favor of Defendants.

Date: April 20, 2026

/s/ Megan Iorio
Megan Iorio
Kabbas Azhar
Abigail Kunkler
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

Attorneys for Amicus Curiae
Electronic Privacy Information Center

CERTIFICATE OF COMPLIANCE

I am the attorney or self-represented party.

1. This brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(5) because this brief contains 5,320 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 typefont using Microsoft Word in 14-point font in Times New Roman font.

Signature: *<u>/s/ Megan Iorio</u>* **Date**: April 20, 2026

CERTIFICATE OF SERVICE

I certify that on April 20, 2026, this brief was e-filed through the CM-ECF System of the U.S. Court of Appeals for the Fourth Circuit. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

Date: April 20, 2026

/s/ Megan Iorio

Megan Iorio
Kabbas Azhar
Abigail Kunkler
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

Attorneys for Amicus Curiae
Electronic Privacy Information Center