No. 22-4489

In the United States Court of Appeals for the Fourth Circuit

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

OKELLO T. CHATRIE,

Defendant-Appellant.

On Appeal from the United States District Court for the Eastern District of Virginia at Richmond No. 3:19-cr-00130-MHL-1; Hon. M. Hannah Lauck

BRIEF OF PROJECT FOR PRIVACY & SURVEILLANCE ACCOUNTABILITY, INC., AS AMICUS CURIAE SUPPORTING DEFENDANT-APPELLANT AND PETITION FOR REHEARING EN BANC

Gene C. Schaerr Erik S. Jaffe Aaron C. Ward SCHAERR | JAFFE LLP 1717 K Street NW, Suite 900 Washington, DC 20006 Telephone: (202) 787-1060 gschaerr@schaerr-jaffe.com

Counsel for Amicus Curiae

AUGUST 29, 2024

TABLE OF CONTENTS

TABLE	F AUTHORITIES	ii
	UCTION, INTEREST, AND SOURCE OF IICUS CURIAE	
ARGUN	ENT	3
I.	his Case Presents a Question of Exception	al Importance3
	. The use of geofence warrants is explodi	ng3
	B. The panel's decision and the Eleve decision conflict with the Fifth Circuit	
II.	eofenced Data Seizures Constitute a Fourt earch.	
	. <i>Carpenter</i> establishes a totality of the test, and the attributes of the data in factors to be analyzed in future cases, <i>generis</i> descriptions of the facts in that	<i>Carpenter</i> are not merely <i>sui</i>
	8. <i>Carpenter</i> clarifies that turnover to a merely one, non-dispositive, circumst the reasonableness of an expectation of	ance affecting
	2. Seizure of even short-term slices of comp phone location records is incom Founding-era levels of privacy	patible with
III.	eofence Warrants Are Unconstitutional re Not Based on Probable Cause for the Jajority of Individuals Surveilled Under Su	Overwhelming
CONCL	SION	
CERTII	CATE OF COMPLIANCE	

TABLE OF AUTHORITIES

Cases	Page(s)
Carpenter v. United States, 585 U.S. 296 (2018) 1, 2, 4, 7,	, 8, 9, 11, 12
Carroll v. United States, 267 U.S. 132 (1925)	8
<i>Fisher v. U. of Tex. at Austin,</i> 644 F.3d 301 (5th Cir. 2011)	3
Katz v. United States, 389 U.S. 347 (1967)	7
<i>Kyllo v. United States,</i> 533 U.S. 27 (2001)	4, 8
Leaders of a Beautiful Struggle v. Baltimore Police Dep't, 2 F.4th 330 (4th Cir. 2021)	10, 12
Matter of Search Warrant Appl. for Geofence Location Data Stored at Google Concerning an Arson Investigation, 497 F. Supp. 3d 345 (N.D. Ill. 2020)	13
Riley v. California, 573 U.S. 373 (2014)	11
Smith v. Maryland, 442 U.S. 735 (1979)	6
United States v. Chatrie, 107 F.4th 319 (4th Cir. 2024)	7, 9, 10
United States v. Davis, 109 F.4th 1320 (11th Cir. 2024)	2, 5
United States v. Hargrove, 625 F.3d 170 (4th Cir. 2010)	8
United States v. Miller, 425 U.S. 435 (1976)	11

United States v. Ojedokun, 16 F.4th 1091 (4th Cir. 2021)6
United States v. Smith, 110 F.4th 817 (5th Cir. 2024)
Rules
Fed. R. App. P. 29
Fed. R. App. P. 351, 3
Other Authorities
Haley Amster & Brett Diehl, Against Geofences, 74 Stan. L. Rev. 385 (2022)
Lukas Haas et al., <i>PIGEON: Predicting Image Geolocations, in</i> 2024 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) (2024)

INTRODUCTION, INTEREST, AND SOURCE OF AUTHORITY OF AMICUS CURIAE¹

This case presents an exceptionally important Fourth Amendment question: Can the government demand, without a warrant, a multi-hour slice of a comprehensive database of numerous individuals' movements in an effort to track all persons within a specified geographic area and time? The principles underlying the Supreme Court's Fourth Amendment caselaw strongly suggest this increasingly widespread practice violates the Constitution because it is incompatible with "that degree of privacy against government that existed when the Fourth Amendment was adopted." *Carpenter v. United States*, 585 U.S. 296, 305 (2018) (citation omitted). Both the magnitude of the issue and a multicircuit split warrant *en banc* review. Fed. R. App. P. 35(a)-(b).

In the underlying case, a detective attempting to solve a bank robbery applied for a "geofence warrant" requiring Google to identify all individuals passing within 150 meters of the bank during a one-hour

¹ No counsel for a party authored this brief in whole or in part, and no party, party's counsel, or person other than *amicus*, its members, or its counsel made a monetary contribution intended to fund the brief's preparation or submission. A motion for leave to file this brief is filed concurrently pursuant to Rule 29(b)(3).

period. The district court upheld the warrant on the good-faith exception. But on appeal, a panel of this Court affirmed on alternative grounds, holding that no warrant was even required, reasoning that the limits on location tracking from *Carpenter* applied only to longer-term tracking. Shortly thereafter, in a similar case, the Eleventh Circuit agreed. But in a subsequent case, the Fifth Circuit correctly held that not only is there an expectation of privacy in location data, but broad geofence warrants are inherently unconstitutional. *Compare United States v. Davis*, 109 F.4th 1320, 1330 (11th Cir. 2024) *with United States v. Smith*, 110 F.4th 817, 835-38 (5th Cir. 2024).

Because of the serious privacy issues geofence warrants raise, they are of particular concern to *Amicus Curiae* Project for Privacy & Surveillance Accountability, Inc. (PPSA), a nonprofit, nonpartisan organization dedicated to protecting privacy rights. *Amicus* PPSA files this brief, pursuant to Fed. R. App. P. 29(b), to urge this Court to reverse the panel decision, hold that Americans have a reasonable expectation of privacy in even short-term portions of long-term tracking databases, and thus ensure that Fourth Amendment rights are not left "at the mercy of advancing technology." *Carpenter*, 585 U.S. at 305 (citation omitted).

ARGUMENT

This case presents both a significant constitutional question with far-reaching implications and an emerging circuit split, warranting rehearing *en banc*. On such rehearing, the panel decision should be reversed because it misinterprets *Carpenter* as applying only to *long-term intervals* of long-term location records held by third parties. The framework set forth in *Carpenter* is not so limited.

I. This Case Presents a Question of Exceptional Importance.

A case "presents a question of exceptional importance if it involves" an issue that is itself important and consequential *or* "an issue on which the panel decision conflicts with the authoritative decisions of other United States Courts of Appeals that have addressed the issue." Fed. R. App. P. 35(b)(1)(B). Here, both alternatives are satisfied.

A. The use of geofence warrants is exploding.

The warrants here present a significant Fourth Amendment issue and "may determine the [geofence] policies of" law enforcement agencies throughout the "Circuit, or beyond, for many years." *Fisher v. U. of Tex. at Austin*, 644 F.3d 301, 307 (5th Cir. 2011) (Jones, C.J., dissenting from denial of rehearing *en banc*). Far from a minor or occasional concern, such warrants "have become increasingly common," Haley Amster & Brett Diehl, *Against Geofences*, 74 Stan. L. Rev. 385, 388 (2022). While the true number of requests is not known given their issuance to multiple companies, the burden posed by them has become so severe that Google changed its location tracking system to protect itself and its customers. *See Smith*, 110 F.4th at 822 n.3.

Beyond the increasing use of such warrants, this Court has a constitutional duty to ensure it does not leave the public's Fourth Amendment rights "at the mercy of advancing technology." *Carpenter*, 585 U.S. at 305 (citation omitted). Rulings made about current technology should be forward-looking regarding the rule's impact on privacy, and "the rule the Court adopts 'must take account of more sophisticated systems that are already in use or in development." *Id.* at 313 (quoting *Kyllo v. United States*, 533 U.S. 27, 36 (2001)).

Here, systems already in development could enable even more intrusive forms of geofenced data searches and seizures. For instance, instead of requesting the location history of all individuals within a geofence for further scrutiny, it may soon be possible to request all photos that seemingly were taken within the geofence. Even photos that do not ordinarily contain geolocation data could be scanned for other locational clues and turned over to law enforcement. Researchers have demonstrated artificial intelligence that can estimate—with surprisingly high accuracy—locations from photographs. Lukas Haas et al., *PIGEON: Predicting Image Geolocations, in* 2024 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR) 12893 (2024).²

The reasoning of the panel's decision that no warrant is required to request or seize limited-time geofence data could easily justify demands for still more limited-time slices of geofenced information such as all photos or videos in Google's or Apple's cloud that match particular locations and times. The danger to constitutionally protected privacy, both under present and future technology, makes the panel decision ripe for *en banc* review.

B. The panel's decision and the Eleventh Circuit's decision conflict with the Fifth Circuit.

An emerging split on this issue also warrants *en banc* review. The panel decision held a warrant is not even required for certain geofence data seizures. A few weeks later, the Eleventh Circuit agreed. *Davis*, 109 F.4th at 1330. But then the Fifth Circuit split from those courts and held

² Available at https://tinyurl.com/5azmd2fa.

that geofence warrants and search requests are unconstitutional in nearly all cases. *Smith*, 110 F.4th at 835-38.

Furthermore, the consequences of this split are exacerbated by the possibility of "spillover" between conflicting circuits: A warrant issued in one circuit could lead to an arrest and trial of a defendant in another circuit. *See, e.g., United States v. Ojedokun,* 16 F.4th 1091, 1107 (4th Cir. 2021) ("conspiracies operate in a sweeping geographic sense"). The existing split and its significant cross-circuit implications are yet further strong grounds for *en banc* review.

II. Geofenced Data Seizures Constitute a Fourth Amendment Search.

On the merits, this Court should reverse the panel decision. A Fourth Amendment search or seizure occurs when information or items are obtained or seized, the person has a subjective expectation of privacy in the information or items searched or seized,³ and the expectation would have been recognized as reasonable at the time of the Founding or is necessary to preserve Founding-era levels of privacy. *See Carpenter*,

³ A subjective expectation of privacy merely requires "seek[ing] to preserve something as private." *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (cleaned up). This is easily satisfied here.

585 U.S. at 304-05; Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Carpenter, moreover, explained that the reasonableness of an expectation of privacy should be evaluated using the totality of the circumstances, and disclosure to a third party is simply one among multiple circumstances affecting reasonableness. Nor is Carpenter restricted to seizures of longer-term "slices" or "windows" of movement history; that decision expressly declined to approve seizures of short-term windows of information, 585 U.S. at 310 n.3, and there are ample other factors supporting application of the Fourth Amendment's requirements here. For example, the seized data here closely matches that in *Carpenter*, people reasonably expect to be free from government identifying their location at any time or place absent a warrant, and warrantless search and seizure of such location data is incompatible with Founding-era expectations of privacy.

A. Carpenter establishes a totality of the circumstances test, and the attributes of the data in Carpenter are factors to be analyzed in future cases, not merely sui generis descriptions of the facts in that case.

While *Carpenter* lies "at the intersection of two lines of cases," *United States v. Chatrie*, 107 F.4th 319, 328 (4th Cir. 2024) (citation omitted), both lines ultimately address the same question: Does a reasonable expectation of privacy exist? *Carpenter* explains that an expectation of privacy is reasonable when it would have been recognized as reasonable at the Founding or is necessary to preserve a Founding-era degree of privacy. *See, e.g., Carpenter,* 585 U.S. at 305 ("As technology has enhanced the Government's capacity" to surveil, "this Court has sought to 'assure ... preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." (quoting *Kyllo*, 533 U.S. at 34)).⁴

To achieve that end, *Carpenter* evaluates reasonableness using a totality-of-the-circumstances formula, with history and certain "guideposts" to be considered. *Id.* at 304-05. Just as with other totality-of-the-circumstances tests—such as *Miranda* analysis—circumstances in individual cases are factor-like, even if they do not provide a traditional balancing test. *See, e.g., United States v. Hargrove,* 625 F.3d 170, 178-79 (4th Cir. 2010) (comparing to specific facts from past cases).

The panel thus erred by reducing the relevant circumstances in *Carpenter* to mere supporting observations for a more limited rule

⁴ See also Carpenter, 585 U.S. at 304-05 (quoting Carroll v. United States, 267 U.S. 132, 149 (1925) (footnote omitted))); *id.* at 320.

restricting Fourth Amendment protections to long-term tracking data, rather than factor-like circumstances to apply prospectively to any type of personal data the government seeks to access, long-term, short-term, or otherwise.⁵ Indeed, the *Carpenter* court explicitly declined the "parties['] suggest[ions]" that tracking "becomes a search only if it extends beyond a limited period" such as "a 24-hour cutoff." Carpenter, 585 U.S. at 310 n.3. And it is unlikely that a 24-hour period would be qualitatively different than the 2-hour period here in terms of its ability "in isolation" to reveal private information such as who a person might have visited, what meetings they might have gone to, or any other private information that could easily be revealed by a two-hour window into a person's movements. Chatrie, 107 F.4th at 335. It is also noteworthy that the Carpenter court, despite addressing Justice Kennedy's dissent at length, did not challenge his characterization of the decision as a "multifactor analysis—considering intimacy, comprehensiveness, expense, retrospectivity, and voluntariness[.]" Carpenter, 585 U.S. at 340 (Kennedy, J., dissenting).

⁵ See Chatrie, 107 F.4th at 333 (quoting Carpenter, 585 U.S. at 310-11).

Leaders of a Beautiful Struggle v. Baltimore Police Department, 2 F.4th 330 (4th Cir. 2021), is not to the contrary. Beautiful Struggle merely ruled out warrantless long-term tracking, rather than approving short-term tracking, and it acknowledged concerns raised by the data in *Carpenter* that are also present in shorter-term tracking, such as a "retrospective quality" which "enables the government to 'travel back in time to retrace a person's whereabouts," *id.* at 341 (citations omitted). And if the panel were somehow correct that *Beautiful Struggle* limited *Carpenter* to long-term tracking, this Court should correct circuit law and clarify that *Carpenter* also applies to retrospectively accessible shortterm slices of long-term surveillance.

B. *Carpenter* clarifies that turnover to a third party is merely one, non-dispositive, circumstance affecting the reasonableness of an expectation of privacy.

As to whether third-party access to data vitiates any reasonable expectation of privacy, the panel is technically correct that *Carpenter* itself "did not reduce the [third-party] doctrine to one factor in a totalityof-the-circumstances balancing inquiry." *Chatrie*, 107 F.4th at 337. Rather, *Carpenter* clarified that the third-party line of cases *always* viewed disclosure to a third party as merely one factor in that inquiry. 585 U.S. at 314 ("*Smith* and *Miller*, after all, did not rely solely on the act of sharing. Instead, they considered 'the nature of the particular documents sought' to determine whether 'there is a legitimate "expectation of privacy" concerning their contents."" (quoting *United States v. Miller*, 425 U.S. 435, 442 (1976))).

This is true even if information is knowingly or voluntarily given to a third party. *Id.* at 314 ("The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another. But the fact of 'diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely." (quoting *Riley v. California*, 573 U.S. 373, 392 (2014))). Indeed, *Carpenter* discussed the issue of involuntary disclosure only as an alternative argument, *after* concluding there was a reasonable expectation of privacy in the data at issue despite being stored by a thirdparty. *See id.* at 315 ("Neither does the second rationale underlying the third-party doctrine—voluntary exposure—hold up when it comes to CSLI.").

In short, under *Carpenter*, the mere fact that individuals allow some third parties access to data for particular purposes hardly suggests abandonment of a reasonable expectation of privacy as to access by others—especially the government. Letting a plumber into your house to fix a sink does not mean you have no expectation of privacy when the police come knocking.

C. Seizure of even short-term slices of comprehensive cell phone location records is incompatible with Foundingera levels of privacy.

Applying *Carpenter*'s totality of the circumstances test shows there is clearly an expectation of privacy in the data here, which is nearly identical to that in *Carpenter*. Such data allows easy and inexpensive access to a "deep repository of historical location information at practically no expense." *Carpenter*, 585 U.S. at 311. It "achieves nearperfect surveillance," "runs against everyone," and allows the government to "travel back in time to retrace a person's whereabouts." *Id.* at 312.

The only differences here are nominal knowledge, nominal supposed consent, and the use of a shorter slice of an extraordinarily long-term tracking program. But it is difficult to imagine, either at the Founding Era or even "prior to the digital age," *Beautiful Struggle*, 2 F.4th at 341 (cleaned up), any ordinary citizen feeling comfortable

12

giving a government official the ability to glimpse back at a near-perfect record of years' worth of the individual's movements—even if the window in some cases is only a few hours, and even if it was nominally voluntarily disclosed to a corporation. This Court should thus hold there is a reasonable expectation of privacy in such data.

III. Geofence Warrants Are Unconstitutional Because They Are Not Based on Probable Cause for the Overwhelming Majority of Individuals Surveilled Under Such Warrants.

For the reasons detailed in *United States v. Smith* and in the briefing below, geofence warrants inherently lack the particularity required by the Fourth Amendment. *See Smith*, 110 F.4th at 836-38. While there are arguably exceptions where "almost all location data retrieved will be for individuals who" satisfy probable cause, that is not the case here. *Matter of Search Warrant Appl. for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 353 (N.D. Ill. 2020).

CONCLUSION

Geofence warrants combine previously unimaginable and precise retrospective surveillance with something akin to a general warrant. This Court should enforce the Fourth Amendment against them and similar advances in technology by holding that there is a reasonable expectation of privacy in cell-phone location data, even for short-term snippets taken from a long-term compilation.

August 29, 2024

Respectfully submitted,

/s/ Gene C. Schaerr

Gene C. Schaerr Erik S. Jaffe Aaron C. Ward SCHAERR | JAFFE LLP 1717 K Street NW, Suite 900 Washington, DC 20006 Telephone: (202) 787-1060 gschaerr@schaerr-jaffe.com

Counsel for Amicus Curiae

CERTIFICATE OF COMPLIANCE

The foregoing Brief of Project for Privacy & Surveillance Accountability, Inc., as *Amicus Curiae* Supporting Defendant-Appellant and Petition for Rehearing *En Banc* complies with the type-volume limit of Fed. R. App. P. 29(b)(4), because, excluding the parts of the document exempted by Fed. R. App. P. 32(f), this document contains 2,555 words.

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

> <u>/s/ Gene C. Schaerr</u> Gene C. Schaerr

Dated: August 29, 2024

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. 22-4489 Caption: United States of America v. Okello T. Chatrie

Pursuant to FRAP 26.1 and Local Rule 26.1,

Project for Privacy & Surveillance Accountability, Inc. (name of party/amicus)

who is <u>______</u>, makes the following disclosure: (appellant/appellee/petitioner/respondent/amicus/intervenor)

- 1. Is party/amicus a publicly held corporation or other publicly held entity? \Box YES \checkmark NO
- 2. Does party/amicus have any parent corporations? ☐ YES ✓NO If yes, identify all parent corporations, including all generations of parent corporations:

- 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/ Gene C. Schaerr

Date: 08/29/24

Counsel for: Amicus Curiae

USCA4 Appeal: 22-4489 Doc: 77-3 Filed: 08

Filed: 08/29/2024 Pg: 1 of 1

00 4400

Total Pages: (22 of 22)

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT APPEARANCE OF COUNSEL FORM

BAR ADMISSION & ECF REGISTRATION: If you have not been admitted to practice before the Fourth Circuit, you must complete and return an <u>Application for Admission</u> before filing this form. If you were admitted to practice under a different name than you are now using, you must include your former name when completing this form so that we can locate you on the attorney roll. Electronic filing by counsel is required in all Fourth Circuit cases. If you have not registered as a Fourth Circuit ECF Filer, please complete the required steps at <u>Register for eFiling</u>.

THE CLERK WILL ENTER MY APPEARANCE IN APPEAL NO. <u>22-4489</u>				
Retained Court-appointed(CJA) CJA associate Court-assigned(non-CJA) Federal Defender				
Pro Bono Government				
COUNSEL FOR: Project for Privacy & Surveillance Accountability, Inc.				
	_as the			
(party name)				
appellant(s) appellee(s) petitioner(s) respondent(s) amicus curiae intervenor(s) n	novant(s)			

/s/ Gene C. Schaerr

(signature)

Please compare your information below with your information on PACER. Any updates or changes must be made through PACER's <u>Manage My Account</u>.

Gene C. Schaerr Name (printed or typed)

Schaerr | Jaffe LLP Firm Name (if applicable)

1717 K Street NW, Suite 900

Washington, DC 20006

Address

(202) 787-1060 Voice Phone

(202) 776-0136 Fax Number

gschaerr@schaerr-jaffe.com E-mail address (print or type)

CERTIFICATE OF SERVICE (required for parties served outside CM/ECF): I certify that this document was served on by personal delivery; mail; third-party commercial carrier; or email (with									
served on	by	personal delivery;	mail;	third-party d	commercial	carrier; or	email (with	
written consent) on the	followin	g persons at the addr	esses or email	ail addresses	shown:		_		

Signature

Date