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
Richmond Division (The Honorable M. Hannah Lauck)

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF VIRGINIA, AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT–APPELLANT'S PETITION FOR REHEARING *EN BANC*

Jake Karr
TECHNOLOGY LAW AND POLICY CLINIC
NEW YORK UNIVERSITY SCHOOL OF LAW
245 Sullivan Street, 5th Floor
New York, NY 10012
(212) 998-6042
jake.karr@nyu.edu

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

Additional Counsel for Amici Curiae *Listed on Following Page*

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

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
(415) 343-0758
jgranick@aclu.org

Matthew W. Callahan
Eden B. Heilman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF VIRGINIA
P.O. Box 26464
Richmond, VA 23261
(804) 523-2146
mcallahan@acluva.org

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

INTEREST OF *AMICI CURIAE*[1]

The American Civil Liberties Union ("ACLU"), ACLU of Virginia, and Electronic Frontier Foundation have a longstanding commitment to the protection of privacy as guaranteed by the Fourth Amendment, and submitted briefs during panel consideration of this appeal.

SUMMARY OF ARGUMENT

The Court should grant *en banc* review because of the factual and legal deficiencies in the panel majority's opinion identified by Defendant's petition, Judge Wynn's panel dissent, and the Fifth Circuit's opinion in *United States v. Smith*, No. 23-60321, 2024 WL 3738050 (5th Cir. Aug. 9, 2024). *Amici* highlight two reasons why this case warrants rehearing.

First, the panel majority's opinion conflicts with the Supreme Court's decision in *Carpenter v. United States*, 585 U.S. 296 (2018). The panel majority held that the government's geofence request was not a Fourth Amendment search because the location data it revealed covered hours, not days, and because it believed the data had been voluntarily shared by phone users with Google. But the majority disregarded *Carpenter*'s animating principle—that courts must "assure . . .

[1] Counsel for *amici* certify that no person 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. Fed. R. App. P. 29(a)(4)(E). This brief is accompanied by a motion for leave to file. Fed. R. App. P. 29(b)(2).

preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted," *id.* at 305 (citation omitted)—and it misinterpreted the Court's discussion of voluntariness.

Second, this case presents novel constitutional questions of exceptional importance, but the panel majority failed to account for the sweeping consequences of its ruling. The case involves a powerful and fundamentally new capability: here, police instantaneously summoned a list of people located within a 17.5-acre area during a one-hour period—including inside closed spaces not open to public view. JA1351. Geofence searches sweep up innocent people's location history, implicating First Amendment and reproductive rights and contributing to the over-policing of marginalized communities. Such digital dragnets are just one type of "reverse search," increasingly common tools that enable law enforcement access to massive amounts of personal and invasive information, including what we search for, read, and watch online. The *en banc* Court should rehear this case and issue a ruling that coheres with *Carpenter*, establishes proper Fourth Amendment guardrails for geofence searches, and provides guidance for future courts assessing all kinds of reverse searches.

ARGUMENT

I. The panel majority opinion contravenes *Carpenter*.

The panel majority's opinion ignored the animating principle of *Carpenter* and gave decisive import to a single factor—voluntariness—that all nine Justices in *Carpenter* recognized cannot carry such weight.

A. In *Carpenter*, the Court explained that in cases involving government exploitation of digital-age technologies, courts must "assure . . . preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." 585 U.S. at 305 (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)). The *Carpenter* Court applied that principle by recognizing that "[i]n the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection." *Id.* at 312. But cell phone tracking, which is "remarkably easy, cheap, and efficient compared to traditional investigative tools," allows police to "travel back in time to retrace a person's whereabouts" in ways previously impossible, thus unsettling reasonable expectations of privacy and triggering Fourth Amendment safeguards. *Id.* at 311–12.

That principle was hardly new. In *Kyllo*, the Court held that police use of a thermal imaging device to learn information about the interior of the home was a Fourth Amendment search, because learning equivalent information prior to the digital age would have been impossible without entering the home. 533 U.S. at 34.

Similar reasoning drove the Court's holding in *Riley v. California*, 573 U.S. 373 (2014), and the opinions of the five concurring justices in *United States v. Jones*, 565 U.S. 400 (2012). *See Riley*, 573 U.S. at 393–94 (warrant required to search cell phone seized incident to arrest because privacy interest in phone is incomparable to privacy interest in pre-digital items individuals might carry on their person); *Jones*, 565 U.S. at 429–30 (Alito, J., concurring in judgment) (long-term GPS tracking of car is a search because similar intrusion would have been virtually impossible prior to GPS technology); *id.* at 415–16 (Sotomayor, J., concurring).

This Court has acknowledged this principle, too. In *Leaders of a Beautiful Struggle v. Baltimore Police Department*, 2 F.4th 330 (4th Cir. 2021) (en banc), this Court held that Baltimore's surveillance program constituted a search, contrasting police's ability to "tail suspects" with mass aerial surveillance that "is more like attaching an ankle monitor to every person in the city." *Id.* at 341 (cleaned up). Other courts have ruled similarly. *See, e.g.*, *State v. McKelvey*, 544 P.3d 632, 645 (Alaska 2024) (refusing "to mechanically extend the open view doctrine to airborne surveillance"). And they have done so in cases involving even short-term real-time location tracking of phones, explaining that although "[p]olice have always had the capacity to visually track a suspect from some starting location," modern tools like cell site simulators or cell phone pinging requests mean that police have a fundamentally new power to "remotely activate the latent tracking function of a

device that the person is almost certainly carrying in his or her pocket or purse: a cellphone." *Jones v. United States*, 168 A.3d 703, 711–13 (D.C. 2017). This provides police with a radically new capability to precisely locate a person who was "not under visual police surveillance," and so constitutes a search. *Commonwealth v. Reed*, 647 S.W.3d 237, 249 (Ky. 2022); *accord State v. Muhammad*, 451 P.3d 1060, 1071–74 (Wash. 2019) (en banc).

While the panel majority tangentially acknowledged this binding principle, *see* Op. 25 (observing that *Carpenter* found a search because "no comparable record of a person's movements was available to law enforcement in a pre-digital age"), nowhere did it apply it to the facts at hand. As Judge Wynn explained, "[a] geofence intrusion certainly would have been impossible to replicate in the pre-internet age." Op. 68 (Wynn, J., dissenting). Never before has the government been able, "[w]ith just the click of a button" and "at practically no expense," *Carpenter*, 585 U.S. at 311, to assemble a record of who was in a neighborhood at a particular time, where exactly they were, and who they were near, *see Smith*, 2024 WL 3738050, at *11. The "depth, breadth, and comprehensive reach," *Carpenter*, 585 U.S. at 320, of this capability is staggering, destabilizing the traditional balance of power between the people and the government. But the panel majority's opinion failed to address, much less credit, this reality.

B. The panel majority further contravened *Carpenter* in giving decisive weight to its conclusion that "Chatrie voluntarily exposed his location information to Google." Op. 20. *Contra Smith*, 2024 WL 3738050, at *13–14 (contesting "the 'voluntary' nature of Google's opt-in process"). Although *Carpenter* did discuss voluntariness as one factor in the reasonable expectation of privacy analysis, the opinions of all nine Justices make clear that it cannot be an outcome-determinative one.

As Judge Wynn explained, *Carpenter* treated voluntariness as just one among several factors informing the Fourth Amendment calculus. *See* Op. 68–69 (Wynn, J., dissenting) (discussing *Carpenter*, 585 U.S. at 313–16). And while some of the dissenting Justices in *Carpenter* disagreed that cell site location information should be protected, every one of them agreed that at least some sensitive information voluntarily shared with a third party retains Fourth Amendment protection, citing emails held by a service provider as an example. 585 U.S. at 332 (Kennedy, J., dissenting); *id.* at 388 (Gorsuch, J., dissenting); *id.* at 319 (majority opinion). Indeed, as Judge Wynn noted, many kinds of highly sensitive data, from health information to digital journal entries, are voluntarily shared with companies so that they can provide a requested service. Op. 72 (Wynn, J., dissenting). That sharing cannot, by itself, foreclose Fourth Amendment protection. Otherwise, the government could "secure your DNA from 23andMe without a warrant." *Carpenter*, 585 U.S. at 388

(Gorsuch, J., dissenting). That "unlikely" interpretation, *id.*, "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks," *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring). Without correction by the *en banc* Court, the panel's holding imperils all manner of highly sensitive digital-age data in which residents of this Circuit have—and should retain—an expectation of privacy.

II. This case presents important and novel constitutional questions.

The panel's decision failed to grapple with both the unique dangers that geofence searches pose to the rights of all Americans and the consequences of its ruling for all kinds of "reverse searches"—unprecedented tools that law enforcement increasingly use to acquire personal information beyond the location data at issue in this case.

A. Geofence searches ensnare innocent individuals based on their "mere propinquity" to the site of an alleged crime, *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979), implicating their First Amendment and reproductive rights and contributing to the over-policing of marginalized communities. Geofence searches may inhibit citizens "from exercising their associational and expressive freedoms, . . . knowing that the Government may be watching them." Op. 102 (Wynn, J., dissenting) (cleaned up). They could sweep up anyone present at a public demonstration,

chilling peaceful protest.[2] They could ensnare individuals at places of worship, as in this case, chilling free exercise. JA1351 (geofence encompassed the Journey Christian Church). And they could be used by law enforcement in states that have attempted to criminalize traveling out of state to obtain an abortion, to target medical clinics in states where such care is legal, in an attempt to identify residents of the abortion-ban state who have traveled there to obtain care.[3] That means someone visiting a clinic for a legal abortion—or for a routine gynecological exam, breast cancer screening, or STI test—could become the subject of a criminal investigation simply because they visited a reproductive health facility to obtain legal care. According to the panel's decision, law enforcement should be free to conduct these searches "with no judicial oversight or accountability" and "surveil anyone exercising their First Amendment (or other) rights at the government's whim." Op. 102 (Wynn, J., dissenting).

Geofence searches also exacerbate over-policing through indiscriminate surveillance of people in and around targeted areas, which are often communities

[2] *See, e.g.*, Russell Brandom, *How Police Laid Down a Geofence Dragnet for Kenosha Protesters*, Verge (Aug. 30, 2021), https://perma.cc/WLP4-UJFM.

[3] *See* Alfred Ng, *'A Uniquely Dangerous Tool': How Google's Data Can Help States Track Abortions*, Politico (July 18, 2022), https://perma.cc/5G36-KX4C.

with reduced political power.[4] Their use threatens to strip people who live and work in marginalized neighborhoods of the ability to keep their lives private from the government. *See Leaders of a Beautiful Struggle*, 2 F.4th at 348 ("Too often today, liberty from governmental intrusion can be taken for granted in some neighborhoods, while others experience the Fourth Amendment as a system of surveillance, social control, and violence, not as a constitutional boundary that protects them from unreasonable searches and seizures." (cleaned up)); *see also id.* (Gregory, C.J., concurring) (rejecting the premise that increased "[p]olicing ameliorates violence, and restraining police authority exacerbates it").

B. Law enforcement is increasingly using novel "reverse search" techniques like geofence searches to reveal personal and invasive information beyond location data. Commercial entities like Google collect in bulk information about Internet users as part of their businesses, and over the last few decades, law enforcement's ability to cheaply and easily access this highly sensitive data has accelerated. Law enforcement takes advantage of these massive information repositories not only to conduct "targeted searches" against known suspects, but also to discover *unknown* people using reverse searches, when "officials have *no idea* who they are looking

[4] *See* Jeremy Harris, *Layton Police Use Controversial "Geo-Fence" Warrants to Investigate Property Crimes*, KUTV (May 17, 2022), https://perma.cc/E2M3-V9F8.

for, or whether the search will even turn up a result." *Smith*, 2024 WL 3738050, at *14. These reverse searches allow law enforcement to query private information—including cell site location records, Wi-Fi connection records, and Internet search or browser history—to identify groups of people based on where we go, what we search for online, and even which articles and videos we read and watch.[5] The rapid expansion of these surveillance technologies makes it critical that this Court clarify that reverse searches, whether of location or other sensitive data, are not exempted from Fourth Amendment regulation.

Reverse location searches like geofence searches are becoming more common. "Tower dumps"—in which cellular service providers give law enforcement access to information about what devices have connected to a specified cell tower during a period of time—have been in use for years.[6] Police are starting to use Wi-Fi data in a similar way. A large majority of Americans now own smartphones that they connect to Wi-Fi networks in their homes, offices, and in public spaces,[7] and these networks can be used to track users' location and movements through physical space. In *Pennsylvania v. Dunkins*, for example, law

[5] Eric Rasmussen, *Google 'Keyword Warrant' in Minnesota Now Part of National Privacy Debate*, KSTP (June 27, 2024), https://perma.cc/Y5QT-Y2BS.

[6] Fed. Bureau of Investigation, *Cellular Analysis & Geolocation: Field Resource Guide* 1, 4 (2019), https://perma.cc/ATA3-C3MH.

[7] *Mobile Fact Sheet*, Pew Res. Ctr. (June 12, 2019), https://perma.cc/2CW4-W8AP.

enforcement's reverse search of Wi-Fi connection records on a college campus provided a lead on a burglary suspect, but also revealed the identities of two women who were spending the night in a men's dormitory. 263 A.3d 247, 260 (Pa. 2021) (Wecht, J., concurring and dissenting).

Of special concern are searches that target people based on what they have searched for, read, or watched.[8] Internet searches have become a natural and indispensable way for people to acquire information, and search engines routinely retain user search histories in order to generate user-specific results.[9] When Google users are logged into their accounts, the company stores their search histories alongside their identifying information, as well as all browsing histories: websites they visited, videos played, songs streamed, social media posts viewed and liked.[10] This information can paint a detailed profile of the user's "medical diagnoses, religious beliefs, financial stability, sexual desires, relationship status, family secrets, political leanings, and more."[11] Law enforcement already routinely obtains "reverse-keyword" warrants requiring Google to provide information about users

[8] *See Access & Control Activity in Your Account*, Google Account Help, https://perma.cc/4N4C-7AVZ.

[9] Sundar Pichai, *Keeping Your Private Information Private*, Google: Keyword Blog (June 24, 2020), https://perma.cc/BUK3-UTE6.

[10] Google Account Help, *supra* note 8.

[11] Nathan Freed Wessler, *How Private is Your Online Search History?*, ACLU (Nov. 12, 2013), https://perma.cc/CK64-77V5.

who have searched for specific phrases potentially related to a crime.[12] These warrants present acute threats to expressive freedoms, particularly the right to receive information.

These "[n]ew technologies that collect ever-more-intimate data are becoming integral to daily life in ways we could not have imagined even a short time ago." Op. 103 (Wynn, J., dissenting). The Court should safeguard the public against "a too permeating police surveillance," *Carpenter*, 585 U.S. at 305 (citation omitted), by ensuring the Fourth Amendment protects this data from unfettered reverse searches of all kinds.

CONCLUSION

For the reasons above, and as explained in the petition for rehearing, the Court should grant *en banc* review.

Dated: August 29, 2024

Respectfully submitted,

/s/ *Nathan Freed Wessler*

Jake Karr
TECHNOLOGY LAW AND POLICY CLINIC
NEW YORK UNIVERSITY SCHOOL OF LAW
245 Sullivan Street, 5th Floor
New York, NY 10012
(212) 998-6042
jake.karr@nyu.edu

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

[12] *See* Rasmussen, *supra* note 5.

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

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
(415) 343-0758
jgranick@aclu.org

Matthew W. Callahan
Eden B. Heilman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF VIRGINIA
P.O. Box 26464
Richmond, VA 23261
(804) 523-2146
mcallahan@acluva.org

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

I certify that this brief complies with the type-volume limitation of Fed. R. App. P. 29(b)(4) because, according to the word-processing system used to prepare the brief, it contains 2,580 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f).

I further certify that 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 it has been prepared in a proportionally spaced typeface, Times New Roman, in 14-point font.

Dated: August 29, 2024

Respectfully submitted,

/s/ *Nathan Freed Wessler*
Nathan Freed Wessler

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I certify that I electronically filed the foregoing on August 29, 2024 with the Clerk of the U.S. Court of Appeals for the Fourth Circuit via the Court's CM/ECF system.

I further certify that counsel for all parties will be electronically served via the Court's CM/ECF system.

Dated: August 29, 2024

Respectfully submitted,

/s/ *Nathan Freed Wessler*
Nathan Freed Wessler

Counsel for Amici Curiae