No. 25-112

IN THE

Supreme Court of the United States

OKELLO CHATRIE,
Petitioner,

v.

UNITED STATES OF AMERICA,
Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Fourth Circuit

BRIEF OF THE CENTER FOR DEMOCRACY AND TECHNOLOGY, THE SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT, BRENNAN CENTER FOR JUSTICE, AND DEFENDING RIGHTS & DISSENT AS AMICI CURIAE IN SUPPORT OF PETITIONER

SAMIR JAIN
JAKE LAPERRUQUE
GREG NOJEIM
TOM BOWMAN
CENTER FOR DEMOCRACY AND TECHNOLOGY
1401 K Street, NW, Suite 200
Washington, DC 20005
jlaperruque@cdt.org
(202) 637-9800

Counsel for Center of Democracy and Technology

KATELYN N. RINGROSE
Counsel of Record
J. JONATHAN HAWK
ALEXANDER SOUTHWELL
SAGAR RAVI
TYLER HENRY
MCDERMOTT WILL & SCHULTE LLP
500 North Capitol St. NW
Washington, DC 20001
kringrose@mwe.com
(202) 756-8176

Counsel for Amicus Curiae

February 27, 2026

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D.C. 20002

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

CONSTITUTIONAL PROVISIONS

OTHER AUTHORITIES

STATEMENT OF IDENTITY AND INTEREST

Pursuant to Supreme Court Rule 37, the Center for Democracy and Technology ("CDT"), the Surveillance Technology Oversight Project ("S.T.O.P."), The Brennan Center for Justice at NYU School of Law, and Defending Rights & Dissent respectfully submit this brief as amici curiae in support of the Petitioner's Brief filed by the National Association of Criminal Defense Lawyers ("NACDL") on behalf of Okello Chatrie ("Petitioner").[1] CDT is a non-profit, non-partisan, public interest organization that, for over 30 years, has worked to promote the constitutional and democratic values of privacy, equality, free expression, and individual liberty in the digital age. CDT regularly advocates before legislatures, regulatory agencies, and the courts for policies that protect against invasive and unwarranted government surveillance.

S.T.O.P. is a New York-based civil rights and privacy organization that litigates and advocates against invasive surveillance technologies. S.T.O.P. has participated as counsel or amicus in numerous cases concerning Fourth Amendment protections in the digital age, including challenges to geofence warrants, keyword search warrants, and other forms of digital dragnet surveillance that threaten individual privacy and civil liberties. Since 2020, S.T.O.P. has led a coalition of civil rights

---

[1] Pursuant to Rule 37.6, amici curiae affirm no party or counsel for a party in the pending case authored this brief in whole or in part or made a monetary contribution intended to fund the preparation or submission of the proposed brief. No person or entity other than the amici or their counsel made a monetary contribution to fund the preparation or submission of the proposed brief.

organizations that successfully pressed Google to release transparency data on the volume and growth of geofence warrant requests, which Google began publishing in 2021.

The Brennan Center for Justice at NYU School of Law[2] is a nonpartisan public interest law institute that seeks to improve systems of democracy and justice. The Center has conducted extensive research and writing on domestic surveillance and related law enforcement policies, including the dragnet collection of Americans' communications and personal data and the concomitant effects on First and Fourth Amendment freedoms. It has filed numerous amicus briefs on behalf of itself and others in cases involving electronic surveillance and privacy issues. *See, e.g., Tuggle v. United States*, 142 S. Ct. 1107 (2022); *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *United States v. Hay*, 95 F.4th 1304 (10th Cir. 2024); *United States v. Houston*, 813 F.3d 282 (6th Cir. 2016).

Defending Rights & Dissent is a national civil liberties organization working to strengthen our participatory democracy by protecting the right to political expression.

CDT, S.T.O.P., Brennan Center for Justice, and Defending Rights & Dissent submit this amicus brief in support of Defendant's request that this Court deem the execution of this geofence warrant unconstitutional under the Fourth Amendment due to its overbreadth and lack of particularity. A ruling that fails to properly shield the public from improper use of modern surveillance technologies like geofence

---

[2] This brief does not purport to convey the position, if any, of the New York University School of Law.

warrants could lead to unfettered government access to highly personal information about hundreds of thousands if not millions of users' visits and routes, including their travel to private spaces such as homes, hospitals, and places of worship that are unrelated to the underlying investigation. Such a ruling permitting the use of geofence warrants could also open the door to the use of other novel reverse warrants that pose broad risks to individuals' privacy.

INTRODUCTION AND SUMMARY OF ARGUMENT

In this case, law enforcement issued a geofence warrant to Google, Inc. ("Google") directing the company to search its vast "Location History" database[3] and produce responsive location information for every device that was present within a broad area of approximately 17.5 acres.

In reviewing the propriety of this geofence warrant, the Court takes on a critical question: whether new technologies—and the now commonplace data use practices that have become integral to life in the digital age—will invert the Fourth Amendment. Under such an inversion, the government could search, seize, and stockpile highly sensitive

---

[3] At the time the geofence warrant was sought in this case, Location History was automatically logged, as frequently as every two minutes, even when users were not actively using Google Apps. Specifically, the subscriber's Location History consisted of information derived from various sensors involving the subscriber's device—including cell-site location information ("CSLI"), global positioning system ("GPS") signals, Wi-Fi networks, and Bluetooth—from which an estimated location could be derived. In December 2023, Google announced that it was introducing updates to shift the storage of Location History data from a company database to on-device storage. Marlo McGriff, *Updates to Location History and New Controls Coming Soon to Maps*, The Keyword (Dec. 12, 2023), https://blog.google/products-and-platforms/products/maps/updates-to-location-history-and-new-controls-coming-soon-to-maps/. This means that Google no longer has access to user Location History data. Despite this change at Google, geofence warrants will likely continue to be sought and remain a critical privacy issue given the wide and ever-increasing array of other applications and services that harness and rely on such location data.

information to develop suspicion, rather than present individualized suspicion as the basis for surveillance. The warrant before the Court focuses on location data, which can be highly revealing of individuals' most intimate activities and their religious, political, romantic, and other private associations. By reversing the process required to conduct a search and obtaining potentially sensitive locations about many individuals, rather than targeting a suspected wrongdoer, this geofence warrant threatens to enable surveillance that catalogs Americans' most sensitive associations and activities. More broadly, permitting this warrant could usher in a broad new class of so-called "reverse searches" and digital dragnets where not only our actions and associations, but *our very curiosities and thoughts* are vulnerable to government surveillance without individualized suspicion. These modern-day general warrants are incompatible with the Fourth Amendment, threaten an unprecedented chilling effect, and would unravel the balance between the government and its citizens that sets the foundation for democratic society.

To preserve the "privacies of life" in the digital age, this Court should reverse the judgement of the Fourth Circuit.

I. The Fourth Amendment Protects Individuals from Warrantless Surveillance of Their Movements

A. People Have a Reasonable Expectation of Privacy in Their Movements From Sense-Enhancing Surveillance

The Court has recognized that "individuals have a reasonable expectation of privacy in the whole of their physical movements," and that "[a] person

does not surrender all Fourth Amendment protection by venturing into the public sphere." *Carpenter v. U.S.*, 585 U.S. 296, 310 (2018) (citing *U.S. v. Jones*, 565 U.S. 400, 430 (ALITO, J., concurring); *Id.* at 415 (SOTOMAYOR, J., concurring)). As the Court stated in *Carpenter*, "what one seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." 585 U.S. at 310 (citing *Katz v. U.S.*, 389 U.S. 347, 351-52 (1967)).

The Court's analyses of whether a person has a reasonable expectation of privacy in their physical movements in a public place that warrants Fourth Amendment protection have focused on what information government personnel have historically been capable of perceiving *without* "sense-enhancing technology." *Carpenter*, 585 U.S. at 305. In *U.S. v. Knotts*, for example, the Court found there was no reasonable expectation of privacy in someone's location where "[t]he governmental surveillance conducted by means of the beeper in this case amounted principally to the following of an automobile on public streets and highways." 460 U.S. 276, 281 (1983). Similarly, in *California v. Ciraolo*, the Court recognized that, "[t]he Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares." 476 U.S. 207, 213 (1986); *see also Jones*, 565 U.S. at 412 (2012) ("mere visual observation does not constitute a search").

But the Court has reached opposite conclusions in Fourth Amendment cases involving the use of sense-enhancing technology to perceive someone's public movements that may have otherwise gone unnoticed. In *Jones*, planting a tracking device on the suspect's car to track his movements in public places

for multiple days was found to constitute a search under the Fourth Amendment. 565 U.S. at 404. Justice Alito observed that "In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken," resulting in "society's expectation . . . 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 for a very long period." 565 U.S. at 429-30 (ALITO, J., concurring). Likewise in *Kyllo*, the government's use of non-public thermal imaging technology, deployed from a public street to detect heat signals emanating from the inside of a private residence that "would previously have been unknowable," violated the Fourth Amendment. 533 U.S. 27, 40 (2001).

The Court's decisions in those cases reflect its recognition that Fourth Amendment protections must respond to, and shield individuals from, unchecked use of technologies that offer unprecedented surveillance power. To find otherwise, would fail to "assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Carpenter*, 585 U.S. at 305 (quoting *Kyllo*, 533 U.S. at 34); *see also Carpenter*, 585 U.S. at 388 (GORSUCH, J. dissenting) ("Can [the Government] secure your DNA from 23andMe without a warrant or probable cause? … [T]hat result strikes most lawyers and judges today—me included—as pretty unlikely."); *Jones*, 565 U.S. at 418 (SOTOMAYOR, J., concurring) ("I for one doubt that people would accept without complaint the warrantless disclosure to the government of a list of

every Web site they had visited in the last week, or month, or year.").

Indeed, as noted in *Carpenter*, "the Court is obligated—as '[s]ubtler and more far-reaching means of invading privacy have become available to the Government'—to ensure that the 'progress of science' does not erode Fourth Amendment protections." 585 U.S. at 320 (quoting *Olmstead v. U.S.*, 277 U.S. 438, 473-74 (1928) (Brandeis, J., dissenting)). Recognizing that "a central aim of the Framers was 'to place obstacles in the way of too permeating a police surveillance,'" the Court's assessment of "which expectations of privacy are entitled to protection … is informed by historical understandings 'of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted,'" and by several "basic guideposts," i.e., "seek[ing] to secure 'the privacies of life' against 'arbitrary power.'" 585 U.S. at 305. Following these principles in *Carpenter*, and distinguishing its cases involving analog surveillance methods, the Court recognized that the government invaded reasonable expectations of privacy where the location data sought enabled the government to "travel back in time to retrace a person's whereabouts, subject only to the retention of policies of the wireless carrier." 585 U.S. at 312.

The location data at issue in this case—relies on GPS, Wi-Fi, Bluetooth, and CSLI data to log a device's location, sometimes with incredible precision—constitutes a sense-enhancing technology that can go back in time to reveal a person's public and private locations in ways unfathomable to investigators using only analog tools. The information is generated based on non-public signals sent from an individual's smartphone, and stored in non-public data

repositories, and can reveal a person's precise whereabouts even though the person may never have been, or never wanted to be, observed at any of those places. *Chatrie*, 590 F. Supp. 3d 901, 907-09 (2022). Protecting such location data aligns with the basic protections of the Fourth Amendment to secure the "privacies of life" against "arbitrary power," and place obstacles in the way of excessive police surveillance. *Carpenter*, 585 U.S. at 305.

B. This Expectation of Privacy Extends Across Different Digital Services and Settings

As this Court has noted, when considering new innovations in airplanes and radios, it must tread carefully to ensure not to "embarrass the future." *Northwest Airlines, Inc. v. Minnesota*, 322 U.S. 292, 300 (1944). If this Court were to hold that users who utilize applications and services that rely on location information have waived Fourth Amendment protections based on a narrow conception of "voluntariness"—such as some technical capacity to limit data collection—it would fundamentally destabilize the public's trust in the panoply of digital services fully integrated into modern life, and create an untenable standard. Such a ruling would make courts into a Sisyphus with the technologies of modern daily life as its boulder. This would invite relentless litigation to address ever-shifting boundaries of what data is "strictly necessary" for a particular service to function, which tools have become "indispensable" to modern society, and what systems settings and Terms of Service are "voluntarily" embraced. That inquiry would be a moving target that would inevitably fail to keep pace with innovations in personal electronic devices, cloud computing services, artificial

intelligence, and ubiquitous computing. In an environment of such uncertainty, the law would effectively force a choice between digital isolation and the surrender of constitutional rights, the precise result this Court sought to avoid in *Carpenter* and should prioritize avoiding here. *See* Brief of The Rutherford Institute as Amicus Curiae in Support of Petitioner, *Wells v. Texas*, No. 25-484 (U.S. Nov. 19, 2025), https://www.rutherford.org/files_images/general/2-5-26_Wells_Amicus_Brief.pdf.

In the years following this Court's decision in *Carpenter,* technological advancements have prioritized the collection of increasingly precise location signals for an ever-growing range of applications and services. These data points facilitate not just modern conveniences; they enable essential components of modern life in a digital world: hailing ride-shares, finding a meeting point for friends at a large event, recovering lost devices, estimating travel times and keeping apprised of traffic, maintaining automated travel journals, connecting with nearby individuals on dating apps, traversing a walking route through an unfamiliar neighborhood, keeping track of children and family members, and more. While these services might appear more "voluntary" than the CSLI addressed in *Carpenter*, the practical necessity of data collection and retention as an assumed component of modern life remains unchanged for the end user. For the average person, disassociating with the multitude of commonly used applications and services that rely on logging precise location data requires disassociating from modern society itself.

In a connected world where devices constantly generate, transmit, and store sensor data, failing to provide Fourth Amendment protection based on each

user's theoretical ability to disable that flow except at the precise moments they are using a service reliant on the data is not a viable option. Just as a user must power down their device to prevent a cell tower from logging CSLI, preventing location-data-dependent services requires either powering down a device, manually pausing *all* services and applications that rely on location data, or retroactively deleting *all* data collected across *all* relevant applications and services. The resulting loss of functionality is not a realistic option for most users. To the extent that these processes are even achievable, navigating them is confusing, time-intensive, and dauntingly complex to a degree that cannot be reasonably expected as a burden of daily life.

Forcing users to constantly track and respond to how services update their available settings and data collection options as well as their terms and services is not a feasible condition for maintaining Fourth Amendment protections in a digital age. Foisting such a burden on users is all the more tedious given the range of applications that require location services, and the lack of clarity that often accompanies data collection options. Charlie Warzel, *The Loophole That Turns Your Apps into Spies*, N.Y. TIMES (Sept. 24, 2019), https://www.nytimes.com/2019/09/24/opinion/facebook-google-apps-data.html.

The often labyrinthian nature of digital applications' policies and settings makes user control over data even more tenuous. Privacy policies and Terms of Service can be lengthy and difficult to digest in myriad ways: statements on how personal data is treated may be buried within other language unrelated to the company's data practices; *Bringing Dark Patterns to Light: Staff Report,* Bureau of

Consumer Protection, Fed. Trade Comm'n 22-23 (Sept. 2022); *see also* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Privacy Policies*, 4 I/S: J.L. & Pol'y for Info. Soc'y 543, 563 (2009) (explaining privacy policies take average users 244 hours per year per person to read); *see also* Geoffrey A. Fowler, *I Tried to Read All My App Privacy Policies. It Was 1 Million Words.*, The Washington Post (May 31, 2022), https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/; there may be discrepancies between the privacy policy and Terms of Service; companies may describe data practices in terms that do not elucidate how data is collected or treated across different apps and services. Ryan Nakashima, *APNewsBreak: Google Clarifies Location Tracking Policy*, The Associated Press (Aug. 16, 2018, at 20:09 ET), https://apnews.com/article/ef95c6a91eeb4d8e9dda9cad887bf211. Companies' updates to app settings can also make it harder to find specific privacy settings or to understand what each setting accomplishes. *Bringing Dark Patterns to Light,* supra, at 17, 25-26. Whether consent for data collection is obtained through an affirmative opt-in setting, imputed from the users' inaction with respect to an opt-out setting, or otherwise assumed from the users' continued use of an app, can vary widely across services. Even when pursued, companies do not consistently honor opt-out signals. Matt Schwartz, Ambrose Vannier, William Walsh, Alan Zhang & Sebastian Zimmeck, *Many Companies May be Ignoring Opt-Out Requests Under State Privacy Laws*, Consumer Reports (Apr. 1, 2025), https://innovation.consumerreports.org/Mixed-Signals-Many-Companies-May-Be-Ignoring-Opt-Out-Requests-Under-State-Privacy-Laws.pdf.

Stemming from these challenges, researchers have documented consent fatigue, information overload, a sense of futility and lack of control over privacy risks, and a tendency to underestimate the risks of providing information as a result. Wenjun Wang, Qikai Wu, Dongqi Li & Xinluan Tian, *An Exploration of the Influencing Factors of Privacy Fatigue Among Mobile Social Media Users From the Configuration Perspective*, Sci. Rep. (Nature) 15:427 (2025), https://www.nature.com/articles/s41598-024-84646-z. It is no surprise people consider privacy policies and options simply a hoop to jump through, with little they can do to actually control how their data is treated. Fifty-six percent of American adults agree to privacy policies without reading them; sixty-one percent of adults consider privacy policies to be an ineffective way for companies to explain data practices; and sixty-nine percent consider privacy policies to be just something to "get past." Colleen McClain, Michelle Faverio, Monica Anderson & Eugenie Park, *How Americans View Data Privacy* (Oct. 18, 2023), Pew Research Ctr., https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.

Finally, were the Court to withhold Fourth Amendment protections for location data because of some potential to use different applications or settings, it would open a Pandora's Box of legal uncertainty and undermine basic protections for an array of digital tools that have become fully enmeshed in daily life. Alternatives that limit third-party data collection will virtually always be available, but be significantly less useful or significantly more cumbersome, complex, or costly. Do the hundreds of millions of Americans that "voluntarily" choose services such as Gmail and Microsoft Outlook lose

Fourth Amendment protections for their email because they rely on companies' ability to sift out spam and malware, and because they do not have the technical savvy to set up their own self-hosted end-to-end encrypted email server or anonymous remailer service? *Anonymous Remailers*, George Mason University, https://mason.gmu.edu/~afinn/html/tele/components/anonymous_remailers.htm (last visited Feb. 21, 2026). Do privacy rights for online browsing evaporate for anyone who does not understand or cannot afford a Virtual Private Network ("VPN") service, or is unwilling to spend over ten times longer loading a webpage using the Tor browser in order to reliably prevent web tracking? Michael Muchmore, *Tor Browser Review*, PCMag (Aug. 31, 2023), https://www.pcmag.com/reviews/tor-browser ("Tor Browser delivered just under 3Mbps download speed with a ping time of 308ms. On the same computer, Firefox showed 160Mbps with a 10ms ping. On the same connection, PCMag.com loaded in *less than a second in Firefox and 11 seconds in Tor Browser*. Your results will vary, but using the browser to stream 4K video may not work at all."). If the only way to retain a constitutional expectation of privacy is to avoid data collection regardless of the burdens of doing so, the Fourth Amendment will become a luxury of the technically sophisticated and wealthy, rather than a right of the people.

II. The Geofence Warrant in This Case Is Unconstitutional

A. Chatrie Had a Reasonable Expectation of Privacy in Location History Data Held By Google

Consistent with the Court's case law, the Location History data retained by Google in this case

is protected under the Fourth Amendment and accessing that data constitutes a "search" pursuant to the Fourth Amendment. Here, the government sought to search Location History data collected through Google's Location History service, which uploads Location History data whenever a phone is on. This service can thus map out all locations visited for each of its millions of users, including where they went to pray, the location of and time they spent in private residences, and the medical centers where they have received care.

Google has long-encouraged users to subscribe to Location History not only as a simple and straightforward means of simplifying daily life in the digital age (*e.g.*, by offering a means of effectively keeping a private journal containing their favorite restaurants, bars, and other locations), but as a basic component of device functionality. Google Maps, *Your Timeline: Revisiting the World that You've Explored* (July 21, 2025), https://maps.googleblog.com/2015/07/your-timeline-revisiting-world-that.html; *see also* Gerard Sanz, *Remember Where You've Been and What You've Done with Your Timeline on iOS*, The Keyword (Apr. 18, 2017), https://blog.google/products-and-platforms/products/maps/remember-where-youve-been-and-what-youve-done-your-timeline-ios/.

While opting into Location History is simple, the process of deleting prior data or pausing automatic collection of data can be complicated and ultimately limited in impact. Google Maps, *Manage Your Google Maps Timeline* (last visited Feb. 17, 2026), https://support.google.com/maps/answer/6258979?hl=en&co=GENIE.Platform%3DAndroid. The technical aspects of controlling acquisition and retention of location data could be vexing for users and even

software engineers to navigate. *Chatrie*, 590 F. Supp. 3d at 913 n.17 ("one Google employee apparently remarked through an email: 'The current [User Interface as of August 13, 2018] feels like it is designed to make things possible, yet difficult enough that people won't figure ... out' how to turn Location History off."). Even if a user deleted the Google Maps application, locations would still be tracked if the user initially enabled Location History, which is tied to a user's Google account and not a specific app or single device. While Google added features that permitted users to enroll in periodic automatic deletion of location data points (e.g., every three months) and to "pause" collection of Location History, it did so in May 2019, less than three weeks before the date this geofence was issued for. David Monsees & Marlo McGriff, *Introducing Auto-Delete Controls for Your Location History and Activity Data*, The Keyword (May 1, 2019), https://blog.google/innovation-and-ai/technology/safety-security/automatically-delete-data. Furthermore, these processes could be limited in their impact—autodeletion does not take place instantly and pausing does not delete previously collected Location History data.

For the tens of millions of users with Location History enabled, access to data maintained by Google could provide an intimate window into their "visits and routes", even if no one actually saw the user go into those places. The District Court properly recognized that "Location History appears to be the most sweeping, granular, and comprehensive tool when it comes to collecting and storing location data." *Chatrie*, 590 F. Supp. 3d at 907. The retrospective nature of the data collected by geofence "provides an intimate window into a person's life," *Carpenter*, 585 U.S. at 311, revealing their "familial, political,

professional, religious, and sexual associations," *Jones*, 565 U.S. at 415 (SOTOMAYOR, J., concurring), and surveilling their "privacies of life," *Carpenter*, 585 U.S. at 311.

B. The Three-Step Methodology Does Not Cure the Particularity Faults of the Geofence Warrant

By transforming mere presence into a basis for suspicion, geofence warrants bypass the constitutional requirement for particularized probable cause, treating every individual within the digital dragnet as a potential target regardless of their actual conduct. *See Ybarra v. Illinois*, 444 U.S. 85 (1979) ("a person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause"). While the three-step investigatory processing applied in this and many other geofence applications[4]—transitioning from requesting anonymized data to the tracking of "devices of interest" and, then finally, to subscriber unmasking—is framed as narrowing data collection, this method does not cure constitutional defects such as lack of individualized suspicion or particularity. In fact, they

---

[4] There is no designated statutory process for geofence warrants and it can vary across cases. In most instances, however, including this case, geofence warrants involve a three-step process: First, the company provides the government with location information on all devices within the geofence. Second, the company provides location information *outside* the geofence for a subset of devices chosen by the government, meaning the location information of those devices for a period of time before and after the set duration of the geofence and beyond its geographic bounds. Third, the company provides deanonymizing account information for a subset of those devices chosen by the government. *Chatrie*, 590 F. Supp. 3d at 914-16.

in some ways serve to actually *expand* the scope of surveillance.

Once law enforcement officers identify devices of interest within the initial geofence, they seek information to track those devices' movements in the second step of the geofence warrant process. This takes their surveillance *beyond* the designated geographical and temporal boundaries of the geofence, and effectively extends the reach of the warrant into areas where no probable cause was originally established, capturing what the Court in *Carpenter* warned could provide an "intimate window into a person's life." 585 U.S. at 311. By monitoring "anonymized" movement before and after a specified event, authorities circumvent the initial constraints of the warrant, creating a digital trail that can capture a user's familial, political, and religious associations far from the scene of any alleged crime. *Id.*

Furthermore, the protection offered by "anonymizing" device identifiers prior to the final step of the geofence warrant process is often technically fragile. In the context of persistent, high-precision location data, the unique patterns of a person's daily routine—their movements to and within their homes, workplaces, and more—act as signatures that make re-identification trivial even without a formal unmasking of identities. Combining these location "signatures" with publicly available information—such as social media accounts—makes it easy to discover the identity of "anonymized" persons. *Chatrie*, 590 F. Supp. 3d at 924.

Therefore, while multi-phase procedures appear to introduce some measures with privacy-protective goals and seemingly provide a framework for judicial oversight, they do not rectify the

fundamental constitutional infirmity of the initial seizure or the privacy invasions inherent in the final data disclosures. Nor do they satisfy the particularized probable cause requirement required by the Fourth Amendment. Similarly, they do not cure the harms of the distinct chilling effect this dragnet would have on highly sensitive activities, including First Amendment protected activities and associations. After all, the three-step procedure offers no consolation for a person who decides not to attend a religious service or a protest for fear their location data might be incidentally searched even in the absence of wrongdoing. A person should not surrender their First and Fourth Amendment protections for venturing into the public sphere, only to be caught in a geofence even though they engaged in no suspicious, let alone unlawful, activity.

Moreover, the three-step process offers no guarantee that even the final list of "unmasked" individuals—which are solely selected by the government, without any particularized showing or court involvement—consists solely of persons with respect to whom there is probable cause specific to them. *See* Meg O'Connor, *Avondale Man Sues After Google Data Leads to Wrongful Arrest for Murder*, Phoenix New Times (Jan. 16, 2020), https://www.phoenixnewtimes.com/news/google-geofence-location-data-avondale-wrongful-arrest-molina-gaeta-11426374/. It may often include innocent bystanders whose only "wrongdoing" was their physical proximity to a crime scene at the wrong time. *Chatrie*, 590 F. Supp. 3d at 930-31.

C. The Geofence Warrant Was Not Supported By Particularized Probable Cause

The geofence warrant at issue serves as a blaring alarm of how this surveillance technique can use limiting parameters and narrowing steps to give the illusion of particularity, while in reality grossly violating it. Here, the government "lacked any semblance of such particularized probable cause." *Chatrie*, 590 F. Supp. 3d at 927.

The geofence at issue was immense in size. With a 150-meter radius, it spanned a broad area of approximately 17.5 acres, larger than three football fields and far beyond the building where the crime being investigated occurred. *Id.* at 918. Disturbingly, the geofence directly encompassed a church; multiple courts have already cited *Chatrie* to highlight the risks of a geofence pulling in sensitive locations. *See*, *e.g.*, *Price v. Superior Ct.*, 93 Cal. App. 5th 13, 46 (2023); *State v. Contreras-Sanchez*, 5 N.W.3d 151, 170 (Minn. Ct. App. 2024), review granted (May 29, 2024). If deployed in a densely-populated urban area, such a geofence warrant could capture data on many thousands of unknowing individuals. *See* Michael Kolomatsky, *How Big Is an Acre, Anyway?*, N.Y. Times (July 26, 2018), https://nyti.ms/345CjS7 (explaining that 17.5 acres would be around three and a half New York City blocks); *see also Population FactFinder*, NYC Department of City Planning, https://popfactfinder.planning.nyc.gov/#14.08/40.77709/-73.95597 (last visited Feb. 25, 2026) (showing that three blocks on New York's Upper East Side contained a population of 5,070 in 2020 for Census Tract 136.02). Approving such a warrant would open the door to precisely the type of stockpiling of sensitive associations, activities, and free exercise of speech and faith that the Court should be most concerned with.

Technical factors extend the scope of this geofence's surveillance even further. Despite technologies offering significant potential precision,[5] geofences can include "false positives," listing someone as being within the geofence when they were actually outside it. And in this case the confidence interval for devices was dozens—and in one case *hundreds*—of meters in size, meaning "the Geofence Warrant could have captured the location of someone who was *hundreds of feet outside the geofence*." *Chatrie*, 590 F. Supp. 3d at 922 (emphasis added). This balloons the geographic scope of the surveillance, and potentially pulls in guests staying at a hotel, patrons at a restaurant, numerous private residences, a senior living facility, and a pair of busy streets. *Id.* at 922-23.

Rather than narrow the impact of the geofence's surveillance, the subsequent "steps" actually expand it further. As explained above, in "Step 2" of the three-step process, the government demanded and Google provided location *outside* the geofence, broadening the

---

[5] The estimated location of devices stored in Location History accounts, which was searched and obtained for the geofence warrant, was based on multiple potential inputs, including cell-site location information ("CSLI"), global positioning system ("GPS") signals, Wi-Fi networks, and Bluetooth devices. For specific instances the degree of granularity of location information generated can vary based on which of these inputs were available and how they contributed to generating location data. Sometimes the location of a device can be refined to a several meter radius, allowing someone reviewing the data to distinguish which side of the street a user was on or what building they entered; some cases it could even reveal the floor or specific area of a building, such as a store in a shopping mall or a certain office within a hospital. But other times, as occurred with this geofence warrant, there is a larger radius of where precisely a phone might be located.

surveillance to track users' location information for a period of time before and after the set duration of the geofence, and *without any limit to its geographic bounds*. In this case, the government initially sought such information on *all* individuals within the geofence, reflecting a desire to fish for more data at the outset, rather than narrow its privacy impact. While Google pushed back against this demand absent any narrowing, it nonetheless provided the government with this broader Step 2 location information on *nearly half* of the individuals who were within the geofence. This demand was made and fulfilled without any additional judicial authorization, without any justification for why certain devices were targeted for additional surveillance, without any indication if less invasive alternatives were available, and without any efforts to seek a less invasive remedy, such as asking Google or the court to review and refine the data based on certain parameters such as what direction a device entered or exited the geofence from. Then for Step 3 of the process, the government demanded and obtained deanonymizing information not for a specific person for whom probable cause of wrongdoing existed, but rather for a third of all the devices reviewed through its Step 2 surveillance.

The warrant at issue in this case was overbroad and lacked particularity. Approving it would be improper, and would set a dangerous precedent, whereby the government could use the "narrowing steps" of a geofence warrant to cloak overbroad surveillance with a veneer of particularity, while in reality using such data for sweeping dragnets and cataloging of Americans' most sensitive activities and associations.

III. Authorizing This Geofence Warrant Would Enable Pervasive Dragnet Surveillance and Chill Critical Associations and Activities

If the Court were to uphold the validity of the legal process in *Chatrie*, it would set a dangerous precedent threatening to normalize suspicionless fishing expeditions across the digital landscape. Validating the premise that law enforcement may sift through and seize the sensitive data of a group of innocent bystanders to identify a single suspect effectively removes the traditional barriers against general searches. In the physical world, the consequences of such power would be immediately rejected; we would not allow a law enforcement officer to compel every person who walked past a particular street corner, entered a house of worship, or attended a political rally to provide their identity. Yet, geofence and other reverse-search warrants risk institutionalizing exactly this level of intrusion. If the Court permits digital dragnets to bypass Fourth Amendment protections simply because the dragnet is of a digital nature, it would risk creating a society where the fear of being monitored by the state chills the very behaviors—such as intellectual curiosity, free practice of religion, and political dissent—that the Founders designed the Constitution to protect.

A. Geofence Warrants Threaten Pervasive Surveillance of Those Participating in Highly Sensitive Activities

Geofence warrants can significantly endanger the free exercise of those activities that are integral to a free and democratic society, and that the First and Fourth Amendments were established to protect. By identifying people's precise past locations at places such as churches and political rallies, geofence

warrants for Location History or similar collections of location data can easily amount to compelled disclosure of the identities of groups of people associating or attendees at events within the geofenced area. This in turn can have a broader unconstitutional chilling effect on peoples' participation in activities protected by the First Amendment as well as other highly sensitive activities. Geofence warrants have already been used to target sensitive locations including private residences, hospitals, workplaces, and numerous protests. *See, e.g. United States v. Wright*, No. 4:19-CR-149, 2023 WL 5804161 at 9 (S.D. Ga. Sept. 7, 2023); Zack Whittaker, *Minneapolis Police Tapped Google to Identify George Floyd Protesters*, TechCrunch (Feb. 6, 2021, at 8:00 PT), https://techcrunch.com/2021/02/06/minneapolis-protests-geofence-warrant/; Russell Brandom, *How Police Laid Down a Geofence Dragnet for Kenosha Protestors*, The Verge (Aug. 30, 2021), https://www.theverge.com/22644965/kenosha-protests-geofence-warrants-atf-android-data-police-jacob-blake; *Search Warrant for Geofence Location Data Used in Kenosha Riot Arson at Library* (No. 20-M-370) (E.D. Wis. Sept. 3, 2020), https://www.documentcloud.org/documents/21052213-google-geofence-warrant-used-in-kenosha-riot-arson-at-library/; Igor Bonifacic, *FBI Used Google Location Data to Investigate Seattle Arson Following BLM Protest*, Engadget (Feb. 5, 2022, at 12:35 ET), https://www.engadget.com/fbi-google-geofence-warrant-seattle-police-union-arson-173540099.html. In multiple cases—including the one currently before the Court—geofence warrants have targeted a house of worship. *Chatrie*, 590 F. Supp. 3d at 918; Complaint at 4, *Calvary Chapel San Jose v. Santa Clara Cnty*, 5:23-CV-04277 (N.D. Cal. Aug. 22, 2023). Allowing the

government to wield such surveillance powers would fail to recognize that a "central aim of the Framers was to place obstacles in the way of a too permeating police surveillance." *Carpenter*, 585 U.S. at 305.

The Court has "long understood as implicit in the right to engage in activities protected by the First Amendment a corresponding right to associate with others." *Americans for Prosperity Foundation v. Bonta*, 594 U.S. 595, 606 (2021) (quoting *Roberts v. United States Jaycees,* 468 U.S. 609, 622 (1984)), that "[e]ffective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association," and "the vital relationship between freedom to associate and privacy in one's associations." *NAACP v. Alabama ex rel. Patterson,* 357 U.S. 449, 460, 462 (1958). Indeed, "inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs." *Id.* at 462. It follows that "compelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as [other] forms of governmental action." *Id.*; *see also Baird v. State Bar of Ariz.,* 401 U.S. 1, 6 (1971) (plurality opinion).

Due protections for the privacy of one's associations, however, are unconstitutionally side-stepped where associations are revealed via an overbroad, insufficiently particularized warrant looking for all visitors to a *place*, rather than looking for evidence tied to a *particular individual*. As the Court in *Carpenter* recognized, location data is more than capable of revealing an individual's sensitive associations: "[a]s with GPS information, the time-stamped data provides an intimate window into a

person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" 585 U.S. at 311. Even under a narrow timeframe and geographic areas, surveillance centered around specific locations can be highly revealing of:

> [T]rips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.

Jones, 565 U.S. at 415 (SOTOMAYOR, J., concurring). The dragnet nature of a geofence amplifies this risk, allowing the government not only to hone in on those most sensitive venues and events, but also to catalog *everyone* at them.

Even the mere threat of such surveillance power being wielded could have severe harms. Were people to believe that such information could be revealed *en masse* pursuant to broad geofence demands, they may simply choose to not exercise their First Amendment rights to free expression and association. They may choose to not attend a religious ceremony or political rally where they could be associated by the government with a group espousing unpopular, albeit lawful, messages. They may avoid going to an event out of concern that, if any others at or near that event act inappropriately, their location data could be obtained and reviewed as part of a broader investigation into those other people—including the possibility that they are incorrectly accused of wrongdoing based merely on their presence at the event—or investigations pursued as a pretense

for fishing and cataloging members of a disfavored group.

B. Overbroad Geofence Warrants Risk Facilitating a Broader Set of "Reverse Warrants" That Create Immense Risks to Privacy

Upholding the overbroad geofence warrant at issue in this case risks shepherding in a litany of overbroad "reverse warrants." Indeed, the proliferation of geofence warrants has already set a dangerous precedent for additional forms of reverse warrants and digital dragnets. The Fourth Amendment requires that a warrant "particularly describe" the place to be searched and the persons or things to be seized; however, the "reverse" logic inherent in these warrants turns this constitutional mandate on its head. U.S. Const. amend. IV. Instead of targeting a specific individual based on pre-existing evidence, these warrants authorize a broad, indiscriminate and suspicionless sweep to discover a suspect amongst innocent masses all subject to surveillance.

"Reverse searches" have already moved beyond geofence warrants to even more speculative demands, such as reverse keyword warrants. These warrants compel search engines to identify every user who searched for particular terms—a "thought police" practice that is fundamentally speculative as it equates digital curiosity or basic information-gathering with criminal intent. The government has already attempted to exploit the speculative nature of reverse keyword search warrants, as evidenced by demands that were denied because they include terms that are generic in nature and could generate millions of results. *In re Ct. Order for Produc. of Recs. to*

Google, LLC, No. 2024CV30942 (Colo. Dist. Ct. Larimer Cnty. Dec. 6, 2024). A permissive ruling for geofence warrants and the features of "reverse searches" more generally could open the door to these highly speculative and aggressive demands. By transforming the mere act of seeking information into a ground for state suspicion, keyword warrants create a significant chilling effect on free expression, research, and even personal thought and curiosity.

A corollary to reverse keyword searches with potentially even more profound dangers are reverse warrants for AI chatbot prompts. Despite the novelty of AI chatbots services, use of reverse warrants for ChatGPT prompts has already been publicly documented. Thomas Brewster, *DHS Ordered OpenAI To Share User Data In First Known Warrant For ChatGPT Prompts*, Forbes (Oct. 20, 2025), https://www.forbes.com/sites/thomasbrewster/2025/10/20/openai-ordered-to-unmask-writer-of-prompts/. While chatbots perform a similar role to search engines in providing responsive information to a query, users' prompts can be far more detailed and revealing, and designed to facilitate an ongoing "dialogue," potentially regarding the user's most intimate thoughts and ideas.

Equally concerning is the emergence of reverse internet protocol ("IP") warrants, which compel platforms to unmask individuals who have visited a specific web page or viewed a particular video. Through this form of reverse warrant, law enforcement can effectively monitor the intellectual and spiritual lives of the public, targeting the fundamental right to associate and access information anonymously. For example, courts have begun permitting this form of surveillance through warrants

requesting the identities of all viewers who have watched specific YouTube videos. Zack Whittaker, *'Reverse' Searches: The Sneaky Ways That Police Tap Tech Companies for Your Private Data*, TechCrunch (Apr. 2, 2024), https://techcrunch.com/2024/04/02/reverse-searches-police-tap-tech-companies-private-data/. These reverse warrants could unmask hundreds or thousands of individuals that watched a particular video.

And like the house of worship pulled into the geofence in *Chatrie*, mere proximity to an investigation or incidentally discovered traits—such as asking ChatGPT to create a joke about the President—can serve as the basis for surveillance under these reverse warrants. Brewster, *DHS Ordered OpenAI To Share User Data*, supra. If such innocuous activities could serve as the basis, or pretext for, surveillance, the dangers would be immense. It could allow the government to, in effect, electronically rifle through the pews of a church by cataloging everyone who viewed a speech on YouTube from a pastor being investigated for tax fraud, or keep digital tabs on a campaign rally by tracking everyone who watched the speech of a politician accused of inciting violence. This proliferation of reverse warrants stands to chill the exercise of First Amendment rights and undermine anonymity—not only anonymity in one's movement and location as is the case of *Chatrie*—but anonymity in one's curiosity and imagination. This Court has long ruled that the right to anonymous speech and association is protected by the First Amendment, noting that "[a]nonymity is a shield from the tyranny of the majority." *McIntyre v. Ohio Elections Commission*, 514 U.S. 334, 357 (1995); *see* Katelyn Ringrose & Divya Ramjee, *Watch Where You*

Walk: Law Enforcement Surveillance and Protester Privacy, 11:349 Calif. L. Rev. Online 349 (2020).

The risks of content-based collection—searches centered on what a person is reading, watching, asking, or thinking—are uniquely dangerous, they threaten individuals' privacy absent any evidence of wrongdoing. The Court must recognize that a procedural "narrowing" of data, such as the three-step process for geofence warrants, is unlikely to protect the public. If the Court permits digital dragnets simply because the dragnet is of a digital nature, it would risk creating a society where the fear of being monitored by the state chills the very behaviors—intellectual curiosity, free practice of religion, and political dissent—that the Founders designed the Constitution to protect.

IV. Conclusion

The geofence warrant in this case fails to satisfy Fourth Amendment particularity and probable cause requirements. By sanctioning a suspicionless digital dragnet, the lower court has authorized a modern-day general warrant that is fundamentally incompatible with the Constitution. To preserve the "privacies of life" in the digital age and prevent the normalization of mass surveillance, this Court should reverse the judgment of the Fourth Circuit.

DATED: February 27, 2026

Respectfully submitted,

SAMIR JAIN
JAKE LAPERRUQUE
GREG NOJEIM
TOM BOWMAN
CENTER FOR DEMOCRACY AND TECHNOLOGY
1401 K Street, NW, Suite 200
Washington, DC 20005
jlaperruque@cdt.org
(202) 637-9800

Counsel for Center of Democracy and Technology

KATELYN N. RINGROSE
Counsel of Record
J. JONATHAN HAWK
ALEXANDER SOUTHWELL
SAGAR RAVI
TYLER HENRY
MCDERMOTT WILL & SCHULTE LLP
500 North Capitol St. NW
Washington, DC 20001
kringrose@mwe.com
(202) 756-8176

Counsel for Amicus Curiae