No. 25-112

IN THE
Supreme Court of the United States

OKELLO T. CHATRIE,

Petitioner,

v.

UNITED STATES,

Respondent.

On Writ of Certiorari to the U.S. Court of Appeals for the Fourth Circuit

BRIEF OF *AMICI CURIAE* LAW & TECHNOLOGY AND FOURTH AMENDMENT SCHOLARS IN SUPPORT OF PETITIONER

ALAN BUTLER
Counsel of Record
MEGAN IORIO
THOMAS MCBRIEN
SARA GEOGHEGAN

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire
Avenue NW
Washington, DC 20036
(202) 483-1140
butler@epic.org

March 2, 2026

TABLE OF CONTENTS

INTEREST OF THE *AMICI CURIAE* 1

SUMMARY OF THE ARGUMENT 4

ARGUMENT 6

I. A geofence order compelling a provider to search the historical location data of its users is a search under *Carpenter*. 8

II. The Fourth Amendment protects users of Google and other internet services, even if they allow apps to collect location data. .. 13

A. Permission screens presented during app setup are a bad way to assess consumer preferences for privacy or the scope of Fourth Amendment protections. 14

B. Most apps and services, including Google, require data permissions to enable functionality..... 20

C. Even where data permissions are theoretically optional, users are nudged to activate them..... 21

D. Users have brought suit to challenge unauthorized collection, use, and disclosure of their data..... 26

III. A warrant based solely on the time and location of a suspected crime cannot support the type of geofence search used in this case. 28

CONCLUSION 33

TABLE OF AUTHORITIES

CASES

Berger v. United States.
388 U.S. 41 (1967) 31, 32

Carpenter v. United States,
585 U.S. 296 (2018) 7, 8, 11, 13

Commonwealth v. McCarthy,
142 N.E.3d 1090 (Mass. 2020) 10

Kyllo v. United States,
533 U.S. 27 (2001) 12

Marron v. United States,
275 U.S. 192 (1927) 31

Naperville Smart Meter Awareness v. City of Naperville,
900 F.3d 521 (7th Cir. 2018) 9

Riley v. California,
573 U.S. 373 (2014) 7, 28

Smith v. Maryland,
442 U.S. 735 (1979) 6

Stanford v. Texas,
379 U.S. 476 (1965) 30, 31

State v. Diaw,
2024-Ohio-2237 (Ohio Ct. App.) 10

United Sates v. Miller,
425 U.S. 435 (1976) 6

United States v. Diggs,
385 F. Supp. 3d 648 (N.D. Ill. 2019) 10

United States v. Gratkowski,
964 F.3d 307 (5th Cir. 2020) 9

United States v. Jones,
565 U.S. 400 (2012) (Alito, J., concurring) 12

United States v. Tolbert,
326 F. Supp. 3d 1211 (D.N.M. 2018) 10

Wyoming v. Houghton,
526 U.S. 295 (1999) 30, 31

Zurcher v. Stanford Daily,
436 U.S. 547 (1978) 30

STATUTES

Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, title III, § 802 32

OTHER AUTHORITIES

Bobby Allyn, *Google Pays Nearly $392 Million to Settle Sweeping Location-Tracking Case*, NPR (Nov. 14, 2022) 27

Cass Sunstein, *Deciding by Default*, 162 U. Pa. L. Rev. 1 (2013) 22

Christine Utz, *et al.*, *(Un)Informed Consent: Studying GDPR Consent Notices in the Field*, 2019 ACM SIGSAC Conf. on Comput. and Commc'n Sec. (Nov. 2019) 22

Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. Chi. L. Rev. 317, 335 (2008) 19

Estelle Laziuk, *iOS 14.5 Opt-in Rate – Daily Updates Since Launch*, Flurry (May 25, 2021)..... 23

Filippo Lancieri, *Narrowing Data Protection's Enforcement Gap*, 74 Maine L. Rev 1 (2022) 17

Isaiah Poritz, *Google Hit With $425 Million Jury Verdict in Privacy Trial*, Bloomberg (Sept. 3, 2025) 27

Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. Leg. Analysis 43 (2021) 21

Jennifer Valentino-DeVries *et al.*, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. Times (Dec. 10, 2018) 18

Joseph Turow *et al., Americans Can't Consent to Companies' Use of Their Data,* Annenberg Sch. for Commc'n, Univ. of Pa. (2023)..... 17

Laura K. Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181 7

Lauren E. Willis, *Why Not Privacy By Default?*, 29 Berkeley L. & Tech. J. 61 (2014) 14

Letter from Sens. Richard Blumenthal & Edward Markey to Joseph Simons, Chairman, Fed. Trade Commission (May 11, 2018) 20

Marc Chase McAllister, *Modernizing the Video Privacy Protection Act*, 25 Geo. Mason L. Rev. 102 (2017) 17

Matthew Tokson, *Automation and the Fourth Amendment*, 96 Iowa L. Rev. 581 (2011) 19

Matthew Tokson, *Government Purchases of Private Data*, 59 Wake Forest L. Rev. 269 (2024) 11, 16, 18, 19, 25

Matthew Tokson, *Inescapable Surveillance*, 106 Cornell L. Rev. 409 (2021) 21

Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018–2021*, 135 Harvard L. Rev. 1790 (2022) 9

Matthew Tokson, *The Carpenter Test as a Transformation of Fourth Amendment Law*, 2023 U. Ill. L. Rev. 507 (2023) 10

Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 Wash. U. L. Rev. 1461 (2019) 16, 25

Norwegian Consumer Council, *Deceived by Design*, Forbrukerradet (June 27, 2018) 22

Press Release, *Attorney General Bonta Announces $93 Million Settlement Regarding Google's Location-Privacy Practices*, Cal. Off. of Att'y Gen. (Sept. 14, 2023) 27

Press Release, *Attorney General Ken Paxton Secures Historic $1.375 Billion Settlement with Google Related to Texans' Data Privacy Rights*, Att'y Gen.of Texas (May 9, 2025) 27

Sara Morrison, *The Winners and Losers of Apple's Anti-Tracking Feature*, Vox (Apr. 29, 2022) 22

Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 Mich. L. Rev. 547 (1999) 29

William J. Cuddihy, *The Fourth Amendment: Origins And Original Meaning* (2009) 7

Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. Rev. 1687 (2020) 17

INTEREST OF THE *AMICI CURIAE* [1]

This brief is submitted on behalf of *amici curiae* scholars whose work focuses on the fields of Law & Technology and the Fourth Amendment. Their contributions here focus on both the legal and the socio-technical context of the collection of location data from Google's Sensorvault. They urge the Court to reverse the Fourth Circuit decision below and find that the execution of the geofence warrant in this case violated the Fourth Amendment because users have not waived their privacy interests in that data and because a warrant based solely on the time and location of a crime being investigated is not sufficiently particularized to protect against arbitrary government intrusion into the private affairs of hundreds of millions of internet users.

Woodrow Hartzog
Andrew R. Randall Professor of Law
Boston University

Thomas Kadri
Associate Professor of Law
University of Georgia School of Law

Jerry Kang
Ralph and Shirley Shapiro Distinguished Professor of Law
University of California, Los Angeles

---

[1]In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

Wayne Logan
Teaching and University Research Professor
Wake Forest University School of Law

Neil Richards
Koch Distinguished Professor in Law
Director, Cordell Institute
WashU Law

Pamela Samuelson
Richard M. Sherman Distinguished Professor of Law
Berkeley Law School

Bruce Schneier,
Fellow and Lecturer, Harvard Kennedy School

Daniel Solove
Bernard Professor of Intellectual Property and Technology Law
Faculty Co-Director, GW Center for Law & Technology
Faculty Director, Privacy & Technology Law Program
George Washington University Law School

Alicia Solow-Niederman
Associate Professor of Law
George Washington University Law School

Katherine J. Strandburg
Alfred Engelberg Professor of Law
Faculty Director, Information Law Institute
New York University

Matthew Tokson
Professor of Law
University of Utah S.J. Quinney College of Law

David Vladeck
A.B. Chettle, Jr., Professor of Law
Georgetown University Law Center

Ari Ezra Waldman
Professor of Law
University of California, Irvine

Shoshana Zuboff
Charles Edward Wilson Professor of Business Administration Emeritus
Harvard Business School
Co-Director, Fellowship on Surveillance Capitalism or Democracy, Carr Center for Human Rights
Harvard Kennedy School

(affiliations listed for identification only)

SUMMARY OF THE ARGUMENT

The principles of *United States v. Carpenter* compel the conclusion that using an order to obtain location data is a Fourth Amendment search. Geofence searches expose large amounts of sensitive data to the government. Cell phone users do not voluntarily relinquish their rights in this data or assume the risk that it will be handed over for government inspection. Indeed, companies give users little choice in whether and how this data is collected. Geofence searches should be subject to the warrant requirement. Further, given the broad discretion that law enforcement exercised to search through large amounts of personal data in this case, the Court should hold that the execution of this geofence warrant was unconstitutional because it was not sufficiently particularized.

Carpenter provides a useful and workable test for determining when a Fourth Amendment search has occurred. Three of *Carpenter*'s factors have proven to be especially influential in lower courts: (1) The revealing nature of the data sought by the government; (2) the amount of data searched; and (3) the voluntariness of the disclosure by the suspect to the third party. Each of these factors militates in this case in favor of finding that geofence searches require a warrant backed by particularized probable cause. The government's theory that data collected by cell phone apps can be subject to search without any warrant is incompatible with meaningful Fourth Amendment protections for digital information in the modern age.

The mobile location data Google collects and stores in its Sensorvault is even more precise, and potentially revealing, than the cell-site location information at

issue in *Carpenter*. And as this brief will explore in detail, users' provision of location data to companies such as Google is hardly voluntary. While users may be able to avoid using any specific app, the vast majority of Americans use cell phone apps every day, and giving these apps access to data necessary to function is, in practice, unavoidable.

Some courts, including lower courts in this case, have erroneously found that cell phone users waive their Fourth Amendment rights when they grant apps permission to access location data. But app permission prompts are too sparse, misleading, and manipulative to measure users' actual consent. Users are largely unaware of how apps collect and store their data, and permission screens do little to inform them. Even if users were fully informed, the app setup process is burdensome and confusing for users who lack technological expertise. In addition, automated processing of users' data by private companies is very different from collection and use by law enforcement to track their activities. Users do not consent to a police search when they permit an app to access their location data, and the Fourth Amendment applies to geofence searches.

The warrant the officers obtained in this case was not sufficiently particularized to satisfy the Fourth Amendment standard. The only probably cause offered was the location and time of the crime being investigated, and there was no limit on the officer's discretion to obtain identifying information and broader location data about any device within the geofence. Such a sweeping authorization to rummage through sensitive location records is incompatible with the Fourth Amendment.

ARGUMENT

In 2026, most personal data about Americans is generated, collected, or mediated through our mobile devices. These devices (e.g. smartphones, watches, tablets, etc.) rely on third-party service providers to function. Cell phone providers enable our access to telephone and data networks. E-mail and messaging providers enable us to communicate with friends, family, and colleagues. App providers enable us to take on a wide range of tasks including navigating the streets, reading the news, checking the weather, shopping for groceries, and joining meetings or classes.

It is impossible for individuals to carry out many day-to-day tasks without allowing data to be generated, collected, processed, and transferred by their cell phones. But this reality creates a tension with earlier interpretations of the Fourth Amendment issued in *Smith v. Maryland*, 442 U.S. 735 (1979), and *United Sates v. Miller*, 425 U.S. 435 (1976), long before the internet as we know it existed. The tension is that the "third-party doctrine" established under those cases is incompatible with the protection of privacy in the digital age. A rote application of the doctrine to this modern context would find that most Americans have no protection from arbitrary government intrusion into the vast majority of their sensitive files and records, which are collected, processed, and transferred to trusted service providers every day in order to carry out routine tasks.

The Court in *Riley v. California* made clear that a rote application of rules established in the pre-digital era is not appropriate where those rules would eviscerate the rights the Fourth Amendment was established

to protect. *See Riley v. California*, 573 U.S. 373, 385, 400–01, 403 (2014); *see also* William J. Cuddihy, *The Fourth Amendment: Origins And Original Meaning*, 602–1791, at lix–lxviii (2009) (collecting sources objecting to general warrants on privacy grounds); Laura K. Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181, 1316–18 (2016) (describing English and American legal commentary that highlights the privacy interests at stake in exposing a person's papers). It is necessary therefore, as the Court recognized in *Carpenter v. United States*, 585 U.S. 296 (2018), to re-evaluate the scope of protection given to data held by third-party providers in the digital era and to recognize that the warrantless collection of such data is unconstitutional.

In evaluating Fourth Amendment protections for our digital records, many lower courts—including those in this case—have focused on the terms of use and privacy permissions a user grants to their service providers. But that analysis frequently misunderstands the nature of the user-provider relationship and how those terms and permissions are presented and managed in practice. It is wrong to assume in this case, and would be wrong to apply as a rule in future cases, that a user has agreed to give up all constitutional privacy protections when they agree to terms or permissions that allow a provider to collect and store their data.

In the first section of this brief, we explain why the values underlying *Carpenter* indicate that geofence searches are Fourth Amendment searches that require a warrant.

In the second section, we expand on why users' acceptance of third-party data collection on their devices

should not be construed by the Court as a waiver of constitutional rights or as a reasonable assumption of risk that their data will be disclosed to law enforcement.

In the third section of this brief, we argue that the application of the Fourth Amendment standard to the geofence search in this case requires more than a simple probable cause warrant based on the location and time of a crime.

I. A geofence order compelling a provider to search the historical location data of its users is a search under *Carpenter*.

The Court should hold that geofence searches are Fourth Amendment searches under *Carpenter*. This conclusion flows naturally from the Court's framework in *Carpenter* and is in line with insights from lower courts that have applied *Carpenter* in a wide range of circumstances.

In *Carpenter*, the Court discussed several considerations that supported its holding that the Fourth Amendment applied to cell phone location data. The Court discussed the "deeply revealing nature" of location data, *Carpenter*, 585 U.S. at 320, which could expose the intimate details of a person's life, *id.* at 311. The large quantity of data available to the government about a person's past movements increased the potential for violations of a person's privacy. *Id.* at 311–12, 315. The Court next mentioned that the government's capacity to track people wherever they go applies not only to an individual suspect but to everyone with a cell phone, because location information is "logged for all of the 400 million devices in the United States." *Id.* at 312. The Court also noted that data is automatically

transmitted by a cell phone, rather than actively disclosed by the user. *Id.* at 315. Likewise, using a cell phone is a largely inescapable part of modern life, such that users have little practical choice but to use one. *Id.* For these reasons, any disclosure to a third party was essentially involuntary. *Id.* Finally, the Court noted that cell phone tracking was "remarkably easy, cheap, and efficient," capable of accessing vast stores of personal data at little cost to government agents. *Id.* at 311.

This case presents an important opportunity to clarify the precise application of *Carpenter* both in the geofence search context and more broadly in light of how lower courts have applied *Carpenter* in other location data cases. Since 2018, hundreds of courts have applied *Carpenter* to address a wide variety of surveillance technologies. *See* Matthew Tokson, *The Aftermath of Carpenter: An Empirical Study of Fourth Amendment Law, 2018–2021*, 135 Harvard L. Rev. 1790, 1794 (2022). Over time, three of the considerations discussed at length in *Carpenter* have emerged as key factors in courts' decisions. *Id.* at 1831–33.

These three factors are: (1) The revealing nature of the data sought by the government; (2) the amount of data searched; and (3) the voluntariness of the disclosure by the suspect to the third party. *See id.* These factors have guided the outcomes in a large proportion of the cases applying *Carpenter*. *Id.* at 1820–24. Together, these cases have formed an emerging test that can determine whether a person has a reasonable expectation of privacy in their digital data. *See, e.g.*, *United States v. Gratkowski*, 964 F.3d 307, 311–13 (5th Cir. 2020); *Naperville Smart Meter Awareness v. City of Naperville*, 900 F.3d 521, 527 (7th Cir. 2018);

United States v. Diggs, 385 F. Supp. 3d 648, 652 (N.D. Ill. 2019); *United States v. Tolbert*, 326 F. Supp. 3d 1211, 1225 (D.N.M. 2018); *Commonwealth v. McCarthy*, 142 N.E.3d 1090 (Mass. 2020); *State v. Diaw*, 2024-Ohio-2237 (Ohio Ct. App.) (expressly adopting the three factors as a test). This emerging test offers more concrete guidance than the pre-*Carpenter* reasonable expectation of privacy cases.

Lower courts' successful and largely consonant applications of *Carpenter* show that it is the proper framework to apply to determine whether modern investigative techniques are Fourth Amendment searches. Unlike *Katz* alone, the *Carpenter* approach focuses the analysis and produces relatively clear answers, offering more predictability than its predecessor. Although judges may disagree over how to assess one or another of the factors, or about how to weigh the various factors against each other, the spectrum of potential disagreement over *Carpenter*'s factors is narrow compared to the wide range of disagreement possible under *Katz*. *See* Matthew Tokson, *The Carpenter Test as a Transformation of Fourth Amendment Law*, 2023 U. Ill. L. Rev. 507, 528 (2023). Relatedly, the *Carpenter* test imposes concrete limits on what is a Fourth Amendment search. If the government searches unrevealing data, in small amounts, and the data was voluntarily disclosed, then it is clear that no Fourth Amendment search has occurred. *Id.* If the government searches highly revealing data, and large amounts of it, and the data was not voluntarily disclosed, then it is clear that a Fourth Amendment search has occurred. *Id.*

Applying the relevant *Carpenter* considerations to geofence searches, the Court should find that they are

searches subject to the Fourth Amendment that require a particularized warrant.

First, location data, such as the historical mobile location data at issue in this case, is uniquely sensitive and revealing. As the Court concluded in *Carpenter*, location data can provide "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 (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)). Location data collected by cell phone apps is usually far more precise than the data at issue in *Carpenter*, because it relies primarily on a combination of GPS data, Wi-Fi data, and other data, rather than just cell tower signals. *See* Matthew Tokson, *Government Purchases of Private Data*, 59 Wake Forest L. Rev. 269, 310–11 (2024). As a result, the potential for mobile location data to reveal intimate details of a user's life is even greater than that of cell tower data. This consideration weighs strongly in favor of deeming geofence searches to be searches under the Fourth Amendment.

Second, geofence searches have a "retrospective quality," similar to the tower data search in *Carpenter*, that enables access to a substantial quantity of information that would be "otherwise unknowable." *Carpenter*, 585 U.S. at 312. Not only can this data be stored indefinitely, but it provides a total account of all devices within the geofence area (and beyond) that have Google's Location History enabled. When Google received the geofence order in this case, it was storing Location History data about "numerous tens of millions of Google users" who had selected that feature forever, unless the user intervened. J. App. JA-45; Pet.

App. 281a–284a. The data the government obtained from Google is narrower than the data collected in *Carpenter* in the temporal sense (i.e., less than seven days), but it is significantly broader and even more "unknowable" absent the geofence mechanism because it concerns *all devices* within the area around the geofence at the time indicated. While it is, in theory, possible to imagine a "tiny constable" with "incredible fortitude and patience" following a single individual around for many days, *United States v. Jones*, 565 U.S. 400, 420 n.3 (2012) (Alito, J., concurring), it is not even theoretically possible for an officer to travel back in time and to identify every device that was within the 300m circle identified in the warrant between the hours of 4:20 to 5:20pm on May 20, 2019. This geofence search could have identified devices located not only in the bank but also in the nearby restaurant, storage unit, apartment building, church, senior living facility, hotel, and other properties. Pet. App. 302a. Even a tiny and incredible constable could not know all the devices in those myriad buildings, even if he had been standing there at the time armed with the thermal imaging device as in *Kyllo v. United States*, 533 U.S. 27 (2001).

The government's proposed approach, wherein an individual geofence search does not implicate the Fourth Amendment because, in part, it requests seven or more days of location data, would permit essentially all geofence searches to proceed without a warrant because an individual geofence search tends to expose hours, not days, of location data. *See* Resp'ts Br. Opposing Cert. at 10. Yet, without a warrant requirement, nothing prevents government officers from stitching together multiple geofence searches to cumulatively amass vast amounts of geolocation data.

Government agents could reach indefinitely into the past, using multiple geofence searches to uncover who attended church services one morning, a protest later that afternoon, and an LGBTQ bar in the evening. This is equally invasive, and substantially broader, than retrospective searches of an individual's cell tower data. And law enforcement officers, like the one in this case, already recognize that a warrant is necessary for geofence searches: the only uses of geofence searches in cases of which *amici* are aware involve geofence warrants. Declaring that geofence searches do not implicate the Fourth Amendment at all would undercut existing standards and would, in practice, permit the government to track any person's movements years into the past, so long as they did not request more than seven days' worth of location data in total in any single instance. *See Carpenter*, 585 U.S. at 310 n.3.

Finally, Google and other companies' collection of location data is not the type of voluntary disclosure that eliminates privacy interests. As will be explained in Section II, the collection of data by an online service provider is rarely a voluntary act of the user in any meaningful sense and should not be construed as a waiver of their constitutional privacy rights.

II. The Fourth Amendment protects users of Google and other internet services, even if they allow apps to collect location data.

Cell phone users do not waive their Fourth Amendment rights against police location tracking by clicking "yes" or "accept" on bare-bones permission screens. Cell phone app permissions are largely meaningless for indicating voluntariness in the Fourth Amendment context. Most users are not aware of how apps collect

and store their data; they do not read privacy policies and would not understand them if they did; and the automated processing of their information by private companies in no way resembles the personalized human observation involved in police surveillance. Accordingly, users do not voluntarily assume the risk that their personalized data will be available to law enforcement when they click "yes" or "accept" on app permission screens.

A. Permission screens presented during app setup are a bad way to assess consumer preferences for privacy or the scope of Fourth Amendment protections.

Permission screens forced on users during app setup are a notoriously bad way to measure actual consumer preferences and should not be given significant weight in a Fourth Amendment analysis. The process of obtaining user permission via prompts during app setup is generally known as a "forced choice" regime, where users are forced to either grant or deny permission for something before they can use an app. *See* Lauren E. Willis, *Why Not Privacy By Default?*, 29 Berkeley L. & Tech. J. 61, 84 (2014). Forced choice regimes, and especially forced choices during app setup with very limited disclosures, are bad at capturing actual consumer preferences. *See id.* at 80. This is especially true when users don't understand the impact of their choices. *See id.* Given the minimal and often misleading disclosures accompanying permission screens, current app procedures ensure that most people will be profoundly uncertain about what giving permission means when they are confronted with a prompt.

Even if the Court were to consider forced choice permission screens a valid means of assessing people's preferences, clicking "yes" on such a screen should not be deemed sufficient to waive users' constitutional rights. The information in these prompts is typically incomplete or misleading. The standard permission screen for Google Location History, for example, reads:

> "Saves where you go with your devices."

Pet. App. 279a. This confusing fragment is then followed by two sentences that downplay the ways the data may be used:

> "This data may be saved and used in any Google service where you were signed in to give you more personalized experiences. You can see your data, delete it and change your settings at account.google.com."

Pet. App. 281a, 332a. This seems to imply that Google might save a user's Google Maps destinations to provide more personalized experiences, such as recommending frequent destinations. In theory, the user could change their settings later by navigating to the settings page, but they will not likely write down or remember how to find the settings, and they are given no reasons why they might want to change these settings later since they are only told how the data enables a benevolent-sounding "personalized experience." This is the only disclosure the user sees before being offered the highlighted default selection of "Turn on" Location History. *Id.* at 281a.

Google's permission window hides a great deal of relevant information behind a small, unlabeled caret ("^") that most users will not click on, or within a long

and legalistic privacy policy that they are unlikely to read or understand. *See, e.g.*, Pet. App. 66a–68a; Tokson, *Government Purchases*, *supra*, at 304; Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 Wash. U. L. Rev. 1461, 1478–86 (2019). On the primary permission screen referenced in this case, Google did not inform users that it would automatically collect their location data every two minutes at a level so precise it includes which floor of a building they were on, Pet. App. 271a–272a, that it would collect their location data even when they were asleep or when they deleted the app to which they gave permission, *see id.* at 231a, 273a, that Google may disclose location data to third parties for marketing purposes, *see id.* at 271a–272a, or that their location data might be turned over to the police in the absence of probable cause that they committed a crime, among many other omissions. Indeed, internal emails from another Google employee expressed concern at the company's failure to even hint at disclosure to parties beyond Google, writing that they would "want to know which of these options . . . enter me into the wrongful-arrest lottery" of unregulated geofence disclosures. Tr. of Hr'g on Mot. to Suppress at 33, *United States v. Chatrie*, 590 F. Supp. 3d 901 (E.D. Va. 2022) (Dkt. No. 202) [hereinafter Day 2 Transcript].

Further, even if permission screens fully disclosed to users how their location data would be used, other factors prevent users from making informed decisions about data disclosures during the app setup process. Privacy policies are dense, long disclosures that "run for thousands of words and are generally not designed to optimize consumer understanding." Filippo Lancieri, *Narrowing Data Protection's Enforcement Gap*, 74

Maine L. Rev. 1, 29 (2022).[2] Research shows that users cannot comprehend the entities that may potentially access their data in the future. "[O]verwhelmingly, and to an extent not known before, Americans neither understand commercial surveillance practices and policies nor do they feel capable of doing anything about rampant data extraction." Joseph Turow *et al., Americans Can't Consent to Companies' Use of Their Data,* Annenberg Sch. for Commc'n, Univ. of Pa. 17 (2023).[3]

Users are also confronted with numerous permission screens during the initial setup of their cell phones and apps; they are frequently rushed, distracted, and especially prone to just clicking "Accept" and hoping for the best. *See e.g.*, Marc Chase McAllister, *Modernizing the Video Privacy Protection Act*, 25 Geo. Mason L. Rev. 102, 110 (2017). A single app can ask users for many permissions in rapid succession during setup, with the average app asking five times. *See* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. Rev. 1687, 1735–36 (2020). The app setup process is likely to be confusing for users who lack technological expertise. Even experts get confused by these systems: a Google software engineer who thought they had turned off location tracking later discovered it was still turned on. As the engineer wrote in an internal email, "I thought I had location tracking turned off on my phone. However the location toggle in the quick settings was on. So our messaging around this is enough to confuse a privacy focused Google

---

[2] https://digitalcommons.maine-law.maine.edu/mlr/vol74/iss1/3/.

[3] https://www.asc.upenn.edu/sites/default/files/2023-02/Americans_Can%27t_Consent.pdf.

[software engineer]. That's not good." Day 2 Transcript, *supra*, at 35.

Even if users manage to navigate the settings, they are not likely to have sufficient technical understanding of the many data processing systems to understand to the implications of their choice. These systems include location tracking, data storage, third-party data transfer agreements, digital ad networks, targeting algorithms, ad servers, data auctions, and cross-device tracking. *See, e.g.*, Tokson, *Government Purchases*, *supra*, at 304. The upshot is that most users have little to no idea about the data collection practices and risks they are exposed to when they respond to an app permission request. As an advertising industry executive acknowledged about app permissions, "[m]ost people don't know what's going on." Jennifer Valentino-DeVries *et al.*, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. Times (Dec. 10, 2018).

Finally, even imagining that a user did hours of intensive research on every app permission question they faced, read every lengthy and jargon-filled privacy policy, understood the practical implications of all of their choices at the level of an experienced lawyer and technologist, and made an active and affirmative choice regarding a particular company's collection of their data, they still might not understand the Fourth Amendment implications of their choices.

People consider sharing data with companies' automated systems as very different from sharing data with law enforcement officers. Individuals consenting to the former should not be assumed to be accepting the risk of the latter. Consumer data collected to enable the functionality of an app, like the data at issue in

this case, tends to be stored in large blocks of data that are at least putatively deidentified and processed by automated servers. *See* Tokson, *Government Purchases*, *supra*, at 306. Consumers generally perceive the capture of such data as substantially less worrisome than that of personal information. Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. Chi. L. Rev. 317, 335 (2008). Likewise, consumers are generally far less worried about the disclosure of their information to automated systems than to other humans. Matthew Tokson, *Automation and the Fourth Amendment*, 96 Iowa L. Rev. 581, 619–29 (2011). Although this data can often be easily re-linked with a person's identity, app company employees and even third-party data brokers are unlikely to do so in a way that government officers do, i.e., with specific humans investigating a specific, known user's movements. *Id.* A user who permits software to access their data is not agreeing to turn that data over to government agents; the two things are substantially different.

Accordingly, consumers do not consent to police tracking of their personal data when they give apps permission to access their data. Users are largely ignorant of how mobile apps gather and store their data; they do not read privacy policies and could not feasibly do so even if they wanted to; and consumers view the commercial, automated processing of their information by private companies as nothing like the personalized, human tracking involved in police surveillance. Cell phone users are not waiving their Fourth Amendment rights: they are clicking yes on bare-bones permission screens with little understanding of what is going on other than a vague sense that they need to say yes in order to use their apps and their phones.

B. Most apps and services, including Google, require data permissions to enable functionality.

People's intuitive sense that their apps and phones may not function well if they deny permissions during setup is often accurate. Many apps may not work as well, or work at all, if users deny them access to data. For example, in Google Maps, failing to give permission for Location History causes the app to forget previously searched addresses. Users who find themselves retyping a familiar address while on the road might feel compelled to give Google access to a bit more data in order to avoid crashing their cars while navigating. And app settings typically do not give granular control over how much data is collected and how it can be used. Frequently, permission to collect some data necessary for functionality is made inextricable from broader permissions that give the company the right to analyze or use the data for other purposes. The reduction of functionality for users who declined permission for broader location tracking was a primary complaint of a May 11, 2018, letter about Google that Sens. Richard Blumenthal and Edward Markey sent to the chairman of the Federal Trade Commission. *See* Letter from Sens. Richard Blumenthal & Edward Markey to Joseph Simons, Chairman, Fed. Trade Commission (May 11, 2018).

Even beyond the Google context, any mapping app (like Apple Maps) or ridesharing app (like Uber) requires users to disclose their location while the app is in use in order to function. Weather apps, dating apps, popular social media apps, and many other apps often premise certain functions on access to location data, contacts, and other phone data. Many of these services

are beneficial to society, an important part of modern life, or both. Navigation apps reduce traffic and help users avoid getting lost; dating apps lead to millions of marriages and relationships; ride-sharing app use is correlated with a significant reduction in drunk driving deaths. *See* Matthew Tokson, *Inescapable Surveillance*, 106 Cornell L. Rev. 409, 433–37 (2021). Penalizing users for giving the permissions necessary to make these apps work creates harmful incentives and is incompatible with meaningful Fourth Amendment protection in the digital age. *Id.* at 436–37. People should not have to choose between using beneficial modern technologies and preserving their constitutional rights. *Id.*

C. Even where data permissions are theoretically optional, users are nudged to activate them.

Companies manipulate users into turning on location collection by employing dark patterns, which misrepresent that location data collection is necessary for app functionality and use design features that pressure users toward making choices more beneficial to the company at the expense of the user. *See* Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. Leg. Analysis 43, 44 (2021). These dark patterns undermine the voluntariness of user choices to grant app permissions. Manipulated users should not be punished by losing constitutional protections to their sensitive data.

Companies coerce consent through dark patterns such as pre-selecting privacy-invasive defaults, obscuring opt-out options, and providing the illusion of control. The default settings exert a powerful effect on consumers, and they select them with remarkable

frequency. *See* Cass Sunstein, *Deciding by Default*, 162 U. Pa. L. Rev. 1, 3–5 (2013). One study showed that when the default tracking option was switched from "off" to "on," the rate of users accepting tracking increased from 0.16% to 83.55%. Christine Utz, *et al.*, *(Un)Informed Consent: Studying GDPR Consent Notices in the Field*, 2019 ACM SIGSAC Conf. on Comput. and Commc'n Sec. (Nov. 2019), at 973, 982.[4] And Google goes further by making design choices that "obscure some of these settings so that the user cannot know that the more privacy intrusive option was preselected." Norwegian Consumer Council, *Deceived by Design*, Forbrukerradet (June 27, 2018).[5] Google's use of coercive design features that prevent meaningful choice should not be interpreted as a user waiving their Fourth Amendment rights.

Users generally choose to protect their privacy when presented with a meaningful choice to limit online tracking. Take the roll-out of Apple's App Tracking Transparency initiative (ATT). ATT prevented advertisers from accessing a user's unique identification numbers unless the user opted into such tracking. Sara Morrison, *The Winners and Losers of Apple's Anti-Tracking Feature*, Vox (Apr. 29, 2022).[6] Only 5% of U.S. Apple users consented to such cross-app tracking in the weeks following the rollout of ATT. Estelle Laziuk, *iOS 14.5 Opt-in Rate – Daily Updates*

---

[4] https://dl.acm.org/doi/epdf/10.1145/3319535.3354212.

[5] https://storage02.forbrukerradet.no/media/2018/06/2018-06-27-deceived-by-design-final.pdf

[6] https://www.vox.com/recode/23045136/apple-app-tracking-transparency-privacy-ads.

Since Launch, Flurry (May 25, 2021).[7] ATT's meaningful option to protect privacy starkly differs from Google's "consent" flow where a user was nudged towards agreeing to terms and warned that the app would malfunction if a user does not consent.

Chatrie's experience with Google's dark patterns is illuminating. At the time Chatrie purchased his phone, any user who attempted to use (or accidentally activated) a new Google app that collected location data was asked or told to give permission via a barebones permission screen. On this screen, Google highlighted the "Turn on" button in blue, making it both easily visible and emphasizing it as the default choice. By contrast, the "No thanks" button was not highlighted and was written in a light gray text that was less visible. Day 2 Transcript, *supra*, 54–55. The effect was to nudge users, particularly those hurrying through cell phone or app setup and faced with a barrage of confusing permission screens, to select the default choice. In other words, rather than an opt-in system, Google used something closer to an opt-out approach, where consumers had to reject the default choice—"Turn on"—and select the unhighlighted, seemingly disfavored option. And the explanatory text surrounding this choice was minimal and confusing, with Google's location tracking practices barely explained. *See infra* Part I.A.

Companies also pressure users to turn location services on by misrepresenting the consequences of not doing so. In this case, Chatrie did not "voluntarily"

---

[7] https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update/.

expose his location information to Google. A few days after Chatrie purchased his phone, he activated a built-in app called Google Assistant, probably by accidentally pressing the home button on the phone for a few seconds. *See* Day 2 Transcript, *supra*, at 74. According to uncontradicted expert witness testimony, Chatrie viewed a page entitled "Meet your Google Assistant" that directed users to "Give your new Assistant permission to help you." Pet. App. at 120a. That page then told users to give their permission for three different things at once, one of which was Location History. *Id.* Users were then told, falsely, that "The Assistant depends on these settings in order to work correctly. Turn on these settings for [your account]." *Id.* Unbeknownst to users and contrary to the statements on the permission screen, the Assistant software can function without collecting location data.

This process was essentially the opposite of a cell phone user who voluntarily opted in to having their location tracked. Rather, Google directed the user to give permission for location tracking during the setup of an app, and told them, falsely, that a core program built into their phone will not work unless they give this permission. A typical cell phone user, told that their new phone will not work properly unless they give various permissions and then admonished by their phone to turn on those permissions, will turn on the permissions. The fact that Google's description of the permissions and the need for them was not accurate only makes its coercive qualities more obvious.

Chatrie was like the many cell phone users who generally grant permissions blindly even in far less coercive contexts because they are not told of the consequences of doing so and because they want their

phones to work. *See, e.g.*, Tokson, *Government Purchases*, *supra*, at 302; Richards & Hartzog, *Pathologies*, *supra*, at 1478–79.

Some of the lower court opinions in this case reasoned that Chatrie did meaningfully consent to location tracking by accepting tracking on the forced permission screens. This conclusion was based in part on misleading statistics about the percentage of Google users who have Location History enabled. The courts were presented with statistics showing that only one-third of Google users granted location permissions. In the Fourth Circuit's panel opinion, Judge Richardson wrote that the fact "[t]hat two-thirds of active Google users have not enabled Location History is strong evidence" that the decision was voluntary. Pet. App. 169a. But, as Judge Berner wrote in a concurring opinion to the Fourth Circuit's *en banc* decision, a closer look at Google employees' testimony at trial shows that, in reality, a far larger proportion of users asked to enable Location History did so, underlining the coercive nature of this mechanism. *See* Pet. App. 120a–121a. The two-thirds of "active Google users" not tracked via Location History included everyone with a Google account via any app or service, which would include Gmail and other Google apps that do not ask users to sign up for Location History, not to mention desktop-accessible services through which many people have Google accounts, like YouTube. *See id.* Many of these users would never have seen a Location History permission screen in the first place. *Id.* Further, as Google confirmed, the denominator of "active Google users" also *included users who live in countries where Location History is banned altogether*. Day 2 Transcript, *supra*, at 151, 154.

In other words, it is not remotely the case that two-thirds of Google users actively chose not to activate Location History; many were never shown the prompt at all. While Google has never disclosed the proportion of American users who approve location promotion requests when prompted by a Google app, it is likely to be very high.

D. Users have brought suit to challenge unauthorized collection, use, and disclosure of their data.

The premise of third-party doctrine decisions in the pre-digital era, that individuals forego legal rights to protect their information once it is conveyed to a business, no longer holds in the digital age. Indeed, users have vigorously and successfully asserted their legal rights to control the collection and disclosure of their location data, in particular, in recent years. It is clear that users retain legal rights to their data, including privacy rights against improper disclosure, even when they grant an app permission or agree to terms of service. The terms and permission language used is certainly relevant to disputes between a user and the company that has collected their data, but these terms do not—and cannot—destroy every legal right the user has, nor should they be read to eviscerate a user's Fourth Amendment rights. Indeed, many privacy cases brought by users (including Google users) show that these individuals have not given up legally protected interests in their location data when they agree to terms and conditions to use apps and services on their phones.

Users and Attorneys General have successfully sued Google and other companies when they improperly collected or disclosed their location data. *See* Press

Release, *Attorney General Bonta Announces $93 Million Settlement Regarding Google's Location-Privacy Practices*, Cal. Off. of Att'y Gen. (Sept. 14, 2023).[8] A group of 40 Attorneys General also sued Google when the company improperly collected the location data of millions of users, Google paid $392 million to settle the allegations. Bobby Allyn, *Google Pays Nearly $392 Million to Settle Sweeping Location-Tracking Case*, NPR (Nov. 14, 2022).[9] Texas secured a $1.375 billion settlement after its Attorney General sued Google for improper location data practices. Press Release, *Attorney General Ken Paxton Secures Historic $1.375 Billion Settlement with Google Related to Texans' Data Privacy Rights*, Att'y Gen. of Texas (May 9, 2025).[10] And a federal jury in California recently awarded $425.7 million in damages after the jury found in favor of plaintiffs' common law claims of invasion of privacy and intrusion upon seclusion. Isaiah Poritz, *Google Hit With $425 Million Jury Verdict in Privacy Trial*, Bloomberg (Sept. 3, 2025).[11]

Hundreds of millions of users have asserted their collective legal rights, and states have stepped in to protect their residents, when Google and other companies improperly collect or disclose location data. These

---

[8] https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-93-million-settlement-regarding-google%E2%80%99s.

[9] https://www.npr.org/2022/11/14/1136521305/google-settlement-location-tracking-data-privacy.

[10] https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-historic-1375-billion-settlement-google-related-texans-data.

[11] https://news.bloomberglaw.com/litigation/google-violated-privacy-of-nearly-100-million-users-jury-finds.

cases show that just because a user has allowed an app to access their location data, or has provided the terms of service, that does not mean they lose all rights to control and limit access to that data. Consequently, users do not relinquish their Fourth Amendment right against unreasonable searches and seizures when they take such actions.

III. A warrant based solely on the time and location of a suspected crime cannot support the type of geofence search used in this case.

The Government's actions in this case—compelling Google to search through and disclose location records concerning Chatrie and other users—constituted a Fourth Amendment search for the reasons articulated in Chatrie's brief and further supported by the first two sections of this brief. In most cases involving a search, the answer to the question of what the Fourth Amendment requires is simple: "get a warrant." *Riley v. California*, 573 U.S. 373, 403 (2014). However, in this case the question is more complicated because of how the geofence search was executed and how the warrant was drafted. The broad scope of the searches conducted in this case and the lack of particularity and probable cause in the warrant as to Chatrie are fatal defects that render the search unconstitutional.

The Court has held that "a search conducted pursuant to a warrant that fails to conform to the particularity requirement of the Fourth Amendment is unconstitutional." *Id.* At 559. This particularity requirement is rooted in the common-law tradition in which "delegation of discretionary authority to ordinary, 'petty,' or 'subordinate' officers was anathema to framing-era lawyers." Thomas Y. Davies, *Recovering the*

Original Fourth Amendment, 98 Mich. L. Rev. 547, 578 (1999). And this tradition was codified in the Fourth Amendment through its two clauses, the first "outlawing promiscuous search and seizure" and the second "clarif[ying] precisely what will be required for a particularized warrant to be valid." Donohue, *supra*, at 1193 (emphasis in original).

Applying the particularity rule to searches of large volumes of digital evidence can be challenging, especially regarding a database holding millions of individuals' precise location records. But the Court should find that execution of the geofence warrant in this case was unconstitutional where the warrant failed to describe target devices with particularity and gave unlimited discretion to officers executing the warrant to obtain precise location data about any device that happened to be in the vicinity of the crime they were investigating within a one-hour period.

The warrant in this case identified Google's "computer servers" as the place to be searched and requested the court to order Google to identify and provide data first about all devices "inside the geographical area described" during a specific time frame. That data included "a numerical identifier for the account, the type of account, time stamped location coordinates and the data source that this information came from if available." Not. of Attach. to Resp. in Opp. of Mot. to Suppress at 4, *United States v. Chatrie*, 590 F. Supp. 3d 901 (E.D. Va. 2022) (Dkt. No. 54-1). The warrant empowered law enforcement officers to obtain additional location data including "contextual data points with points of travel outside of the geographical area" for a period of 30 minutes before and after the initial search term. And, finally, the warrant required Google

to provide "identifying account information/CSI" for specific accounts identified by the officers including "user name and subscriber information to include date of birth . . . email address . . . electronic devices associated with the account . . . [and] telephone number[s] associated with the account." *Id.* All of this data could be obtained by the officers without any further showing of probable cause or particularity as to the accounts they selected from Google's initial search.

While the specific extent of probable cause and particularity must necessarily be decided on a case-by-case basis, the Court has rejected warrants that "authorized the searchers to rummage among and make judgments about books and papers and was the functional equivalent of a general warrant." *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (summarizing *Stanford v. Texas*, 379 U.S. 476 (1965)). That characteristic of unaccountable discretion to invade the affairs of private individuals is present in this case and is readily distinguishable from cases that involved searches of vehicles and other seized "containers." *See Wyoming v. Houghton*, 526 U.S. 295, 300–303 (1999) (discussing the rules for searching packages and containers applied in *United States v. Ross*, 456 U.S. 798 (1982) and other cases).

The harms identified in *Stanford* and echoed in *Zurcher* and other cases centered on the discretion that broad warrants give government officers to invade privacy and obtain private data without probable cause or judicial scrutiny. When the thing to be seized under a warrant is information rather than particular goods, the constitutional requirement of particularity should be applied with "scrupulous exactitude." *Stanford*, 379 U.S. at 485. The warrant at issue in this case

exhibited the opposite: It only specified the area where a broad range of location data, most of it concerning innocent bank patrons, passersby, and churchgoers, and it permitted police to track and identify whomever they chose without further judicial safeguards. This level of discretion conferred by the "indiscriminate sweep of [the warrant's] language is constitutionally intolerable. To hold otherwise would be false to the terms of the Fourth Amendment, false to its meaning, and false to its history." *Id.* at 486; *see also Marron v. United States*, 275 U.S. 192, 196 (1927) (explaining why the particularity requirement ensures that "nothing is left to the discretion of the officer executing the warrant").

The unique sensitivity and large volume of location data contained in Google's Sensorvault, combined with the discretion given to the officer to collect specific identifying information from devices flagged by Google in its geofence search, support the conclusion that the execution of the warrant in this case was unconstitutional. But the Court will likely look beyond these specific facts to consider whether any form of geofence search could be constitutional. The millions of Google users whose location data was stored in Sensorvault are not akin to the passengers in a vehicle being subject to a lawful search in *Houghton*, 526 U.S. at 304–305, and their interests should necessarily weigh against broad and discretionary geofence searches. Indeed, the invasion of the privacy interests of parties unrelated to the crime being investigated was central to the Court's rejection of the New York eavesdropping warrant in *Berger v. United States*. 388 U.S. 41, 59–60 (1967). The extensive scope of the search combined with the discretion given to the officer in the second

and third phases of the search also weigh against the reasonableness and particularity of the warrant here.

It may not be possible to answer every question concerning the validity of geofence warrants in this case, but in analyzing the question the Court can provide signposts for future answers. For example, in *Berger*, the Court identified factors that undermined the reasonableness of a New York eavesdropping statute, 388 U.S. at 58–60, and those factors directly shaped the Wiretap Act that Congress passed the following year in the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, title III, § 802.

* * *

For these reasons, the Court should hold that retrospective geofence tracking is a Fourth Amendment search, and that the execution of the geofence warrant in this case was unconstitutional.

CONCLUSION

For the above reasons, *amici* respectfully ask the Court to vacate the judgment of the Court of Appeals for the Fourth Circuit and remand for further proceedings consistent with the Court's opinion.

Respectfully submitted,

ALAN BUTLER
MEGAN IORIO
THOMAS MCBRIEN
SARA GEOGHEGAN

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire
Avenue NW
Washington, DC 20036
(202) 483-1140
(202) 483-1248 (fax)
butler@epic.org

March 2, 2026