No. 25-112

IN THE
Supreme Court of the United States

OKELLO T. 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 AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF VIRGINIA, ELECTRONIC FRONTIER FOUNDATION, AND CENTER ON PRIVACY & TECHNOLOGY AT GEORGETOWN LAW IN SUPPORT OF PETITIONER

Nathan Freed Wessler
Brett Max Kaufman
Esha Bhandari
Ben Wizner
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004

Jennifer Lynch
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Jennifer Stisa Granick
Counsel of Record
Cecillia D. Wang
Evelyn Danforth-Scott
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
425 California Street, Suite 700
San Francisco, CA 94104
(212) 549-2500
jgranick@aclu.org

Matthew W. Callahan
ACLU OF VIRGINIA FOUNDATION
P.O. Box 26464
Richmond, VA 23621

Counsel for Amici Curiae American Civil Liberties Union, American Civil Liberties Union of Virginia, Electronic Frontier Foundation, and Center on Privacy & Technology at Georgetown Law

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Statutes, Rules and Other Authorities

INTERESTS OF AMICI CURIAE[1]

The American Civil Liberties Union (ACLU) is a nationwide, nonprofit, nonpartisan organization that since 1920 has sought to protect the civil liberties of all Americans. The ACLU of Virginia is the ACLU's Virginia state affiliate. The ACLU and the ACLU of Virginia have participated as counsel for parties before the Court or amici in many of the Court's cases concerning the right to privacy under the Fourth Amendment. *See, e.g.*, *Carpenter v. United States*, 585 U.S. 296 (2018) (counsel); *Riley v. California*, 573 U.S. 373 (2014) (amici); *United States v. Jones*, 565 U.S. 400 (2012) (amici).

The Electronic Frontier Foundation (EFF) is a member-supported, nonprofit civil liberties organization that works to protect innovation, free expression, and civil liberties in the digital world. EFF actively encourages government and the courts to support privacy and safeguard individual autonomy as emerging technologies proliferate. EFF has served as amicus in many Fourth Amendment cases before this Court, including *Carpenter*, 585 U.S. at 313 (citing EFF's amicus brief); *City of Los Angeles v. Patel*, 576 U.S. 409 (2015), *Riley v. California*, 573 U.S. 373 (2014), *Maryland v. King*, 569 U.S. 435

---

[1] Pursuant to Supreme Court Rule 37.6, counsel for amici certify that no party's counsel authored this brief in whole or in part; no party or party's counsel contributed money that was intended to fund the preparation or submission of the brief; and no person other than amici, their members, or their counsel contributed money intended to fund the preparation or submission of the brief.

(2013), *United States v. Jones*, 565 U.S. 400 (2012), and *City of Ontario v. Quon*, 560 U.S. 746 (2010).

The Center on Privacy & Technology (Privacy Center) at Georgetown Law is a think tank focused on privacy and surveillance law and policy. The Privacy Center has an interest in protecting the privacy of historically marginalized communities, who often are disparately impacted by surveillance programs while simultaneously neglected in privacy debates. The Center has done extensive research and advocacy concerning police surveillance technology.

INTRODUCTION AND SUMMARY OF ARGUMENT

In *Carpenter*, this Court held that it is a Fourth Amendment search when the government demands that a corporation query business records containing a known individual's data for information reflecting their past movements. 585 U.S. 296, 312 (2018). In this case, the government asserts a far more radical and unprecedented authority to conduct "geofence" searches—requests to corporations to search through users' private accounts and the records stored there, without identifying in advance any known individual criminal suspect or even a particular electronic device implicated in a crime. Fulfillment of these requests "gives police access to a category of information otherwise unknowable." *Id.* They thus upset the balance of power between the government and the people by radically undermining "that degree of privacy against government that existed when the Fourth Amendment was adopted." *Id.* at 305 (quoting *Kyllo v. United States*, 553 U.S. 27, 34 (2001)).

Geofence searches allow the government to learn the movements, location, and identity of untold

numbers of people. As such, as in *Carpenter*, they violate users' expectations of privacy in their sensitive location data and thus constitute a Fourth Amendment search. Pet.App.49a-59a (Wynn, J., concurring). The fact that many geofence searches cover hours' worth of location data, not days, does not insulate them from Fourth Amendment limits or meaningfully distinguish them from the search in *Carpenter*. The notion that a shorter time frame does not reveal intimate matters is false. In this case, the defense expert was able to identify several people based on several hours of their location history, including by tracking them to their homes. A snapshot of location data can place a person in a protected and sensitive place—a home, place of worship, or doctor's office. With even a few location points, the government can identify people and record their associations.

Moreover, geofence searches are materially more invasive than the search in *Carpenter* in critical respects. They allow investigators to track and identify anyone who was present in a designated area during any given timeframe in the past without the probable cause or particularity required to search even *one* person's private data. In doing so, they expose numerous individuals' private locations and movements to law enforcement's eye. The warrants purporting to authorize these dragnet searches are general warrants, which the Fourth Amendment forbids. Holding otherwise would open the door to the very kind of investigative tactics that the Founders specifically sought to prevent.

Consider the awesome power geofence searches place in the hands of the government: The warrant here compelled Google to search the accounts of hundreds of millions of users to see if anyone was

within a radius police drew around a crime scene (amounting to several football fields in size and encompassing numerous homes, businesses, and a church). Next, the warrant allowed the government—at its own discretion and without a magistrate's review or approval—to identify 19 individuals to further scrutinize, compelling Google to disclose additional location information for each one of those people. And finally, again without court oversight, police compelled Google to identify three people, including Petitioner, who were then subjected to further investigation.

This is not traditional police work, but rather the leveraging of new and powerful technology to claim a novel and formidable power to invade privacy. By their very nature, geofence searches cast indiscriminate dragnets that turn innocent bystanders into suspects, causing intrusions on a scale far greater than those held unconstitutional in the physical world. *See Ybarra v. Illinois*, 444 U.S. 85 (1979).

Amici urge the Court not only to hold that the search in this case violated the Fourth Amendment, but to make clear that *all* geofence warrants that purport to authorize such searches are unconstitutional general warrants. But if the Court disagrees, there are safeguards it should impose to try to limit the impact of these searches on bystanders. *Cf. Berger v. New York*, 388 U.S. 41, 58-60 (1967) (providing guidance for constitutionally required minimization measures to limit impact of wiretap surveillance on bystanders).

At a minimum, the facts of this case cannot support a blanket ruling that all future geofence

searches escape Fourth Amendment protection. The record reflects how law enforcement conducted geofence searches of Google's location data in 2019 and does not account for updated technology, changed company policies, or how other companies manage their repositories of location data. Crucially, Google no longer maintains its users' location data in a form that is amenable to geofence search, and the record is silent on how other companies that may hold other kinds of location data manage that information or even what form that information takes. Future geofence searches could diverge significantly from this one, and therefore, the answer to the question presented in this case must be cabined to the search conducted here and the record before the Court.

ARGUMENT

I. GEOFENCE SEARCHES VIOLATE REASONABLE EXPECTATIONS OF PRIVACY AND THEREFORE ARE SEARCHES FOR THE PURPOSE OF THE FOURTH AMENDMENT.

A. This Court has consistently applied Fourth Amendment protections to technologies with the capacity to erode historical privacy expectations, and it should do the same here.

To ensure that advances in technology do not erode the "degree of privacy against government that existed when the Fourth Amendment was adopted," this Court has repeatedly held that the use of technology to collect information otherwise unknowable through traditional investigatory techniques triggers constitutional protections. *Carpenter*, 585 U.S. at 305 (quoting *Kyllo*, 533 U.S. at

34 (2001)). In *Carpenter*, the Court applied that principle by recognizing that "[i]n the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection." 585 U.S. at 312. Even targeted searches of an individual's historical cell site location information ("CSLI"), the Court explained, are "remarkably easy, cheap, and efficient compared to traditional investigative tools," and allow police to "travel back in time to retrace a person's whereabouts" in ways previously impossible. *Id.* at 311-12. Because police exploitation of CSLI invaded longstanding and reasonable expectations of privacy, it triggered Fourth Amendment protections. *Id.* at 312. As Justice Alito explained in *Jones*, "[i]n the precomputer age, the greatest protections of privacy were neither constitutional nor statutory, but practical." *United States v. Jones*, 565 U.S. 400, 429 (2012) (Alito, J., concurring in judgment). But in the modern era, "technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes," revealing myriad "privacies of life." *Carpenter*, 585 U.S. at 305 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

This Court's approach of looking to historical expectations of privacy to determine current Fourth Amendment safeguards dates back to even before the dawn of the Internet age. In *United States v. Karo*, 468 U.S. 705 (1984), the Court held that using a radio-tracking beeper to monitor an object's location inside a traditionally protected space was a Fourth Amendment search requiring a warrant even if the tracking device was affixed lawfully. Police, this Court held, should not be allowed to surreptitiously employ advanced technological means to obtain information

that they could not have obtained by observation. *Id.* at 715. The Court relied on similar reasoning in *Kyllo v. United States*, 533 U.S. 27 (2001), holding that police use of a thermal imaging device to effectively peer inside someone's home was a Fourth Amendment search, because conducting an equivalent search before the digital age would have required physically entering the home and thus unquestionably would require a warrant under typical circumstances. *Id.* at 34. And in *Riley v. California*, 573 U.S. 373 (2014), as well as the opinions of the five concurring justices in *Jones*, the Court applied this same principle to newly ubiquitous cell phones and to GPS location tracking. *See Riley*, 573 U.S. at 393-94 (warrant required to search cell phone seized incident to arrest because privacy interest in phone is incomparable to privacy interest in pre-digital items individuals might carry on their person); *Jones*, 565 U.S. at 429-30 (Alito, J., concurring in judgment) (long-term GPS tracking of car is a search because similar intrusion would have been virtually impossible prior to GPS technology); *id.* at 415-16 (Sotomayor, J., concurring).

In each of these cases, the government argued that the Fourth Amendment did not protect against searches conducted using these novel technologies—but this Court ensured each time that technology did not outrun Fourth Amendment safeguards. This case presents another such situation. Geofence searches enable police to call up a record of an unknowable number of people who were in a particular area at a particular time, even months or years later. This ability to retrospectively round up anyone who happened to be near a crime scene and subject them to further investigation—including when they were in homes, churches, and other constitutionally sensitive

spaces—represents an unprecedented expansion of law enforcement's ability to locate people in time and space, *Carpenter*, 585 U.S. at 312, and "it is . . . impossible to think of late–18th-century situations that are analogous." *Jones*, 565 U.S. at 420 (Alito, J., concurring in judgment).

The government could never deploy enough police officers or recruit sufficient informants to be present everywhere just in case a crime occurred, and then quickly and accurately identify every individual in the vicinity, including those inside constitutionally protected spaces and thus shielded from public view. To capture any number of people's whereabouts within any desired range of a future crime scene would be physically impossible. Yet this information is something that law enforcement can almost effortlessly learn through a geofence search. Letting that power go unchecked is inconsistent with basic freedoms in a democratic society.

B. The Fourth Amendment applies to a search of many people's location data just like it applied to the search of one person's location information in *Carpenter*.

1. The geofence search at issue here is a Fourth Amendment search for the same reasons as the government's search in *Carpenter*.

The warrant here, just like other geofence warrants, purports to authorize a Fourth Amendment search under *Carpenter*. *See* Pet.App.49a-59a (Wynn, J., concurring) (highlighting four elements critical to the Court's *Carpenter* decision that apply in full to geofence searches: (1) the comprehensiveness of the

location database; (2) the retrospective quality of the location data; (3) the capacity of location data to reveal intimate details about a person; and (4) the fact that searches of location data are, by leaps and bounds, easier, cheaper, and more efficient than any previous investigative technique and therefore subject to abuse).

Just as in *Carpenter*, the retrospective location tracking police can accomplish via a geofence search is "qualitatively different" from traditional police surveillance. 585 U.S. at 309. Searches of stored location data enable "near perfect surveillance, as if [the government] had attached an ankle monitor to the phone's user." *Id.* at 312. Like *Carpenter*'s cell site location information, geofence location data may be collected and retained for years, and is capable of "reconstruct[ing] a person's movements," such that the person "has effectively been tailed every moment of every day." *Id.* This includes "faithfully follow[ing]" users into "private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Id.* at 311. It is "comprehensive," "retrospective," "intimate," and "easy" to access for investigators. *Id.* at 309-12.

Everything that was true of CSLI in *Carpenter* is true of geofence searches. Like CSLI, at the time of the search here Google logged location data continually for hundreds of millions of its users, "not just [for] persons who might happen to come under investigation." *Id.* at 312. This upends traditional expectations of how the government conducts surveillance, because now, "police need not even know in advance whether they want to follow a particular individual, or when." *Id.*

If anything, reverse location searches are more invasive. CSLI searches begin with an identifiable suspect or phone number. Geofence searches do not. In *Carpenter,* the government obtained two court orders demanding 152 days and seven days of cell phone location data belonging to a single person. 585 U.S. at 302, 310 n.3. Here, in order to *generate* a suspect, the government compelled Google to search location data stored across more than 500 million users' accounts Pet.App.6a; Pet'r's Opening Br.5 & n.1. That search targeted an unknown number of people based not on probable cause to believe that any particular Google user was the suspect, but on the popularity of Google-powered digital services and users' mere proximity to a crime.

Indeed, the search Google conducted for the government can reveal more precise location information than CSLI—and is therefore more intrusive—because it relies not only on cell tower connections but also on GPS, Wi-Fi, and Bluetooth. Pet.App.271a. At the same time, though, it can also be inaccurate. Google has said the data is only an estimate of users' locations, with a "confidence interval" of merely 68%. Pet.App.274a. This means that, responding to a geofence warrant, Google would produce the location data of users if their location was 68% likely to have fallen within the geographic area. JA-51.[2] The upshot is a possibility of both false positives and false negatives—people could be implicated for a crime when they were actually outside the geofence area, and the real perpetrator might not be included at all in the data Google provided to police. Pet.App.303a; *see also People v.*

[2] Citations to the JA refer to the Joint Appendix, Volume I.

Meza, 312 Cal. Rptr. 3d 1, 17 (2023) (geofence warrant's "overbreadth is even more pernicious given that individuals . . . would be included in the warrant return despite an estimated 32 percent chance they were actually not within the search parameter at all.")

Investigators here obtained two hours of information, a shorter time period than the days-long tracking at issue in *Carpenter*. But that is not a constitutionally meaningful difference, especially in light of the unprecedented and expectation-disrupting technology that both types of searches exploit and weighed against the ways in which this search was *more* invasive than the search in *Carpenter*. And of course, without Fourth Amendment limitations, investigators would be able to conduct geofence searches covering however many hours or days they would like.

Regardless, *Carpenter* never purported to identify a magical number of days at which CSLI tracking attained some higher degree of constitutional significance. *Cf.* 585 U.S. at 395-96 (Gorsuch, J., dissenting). Rather, the Court explicitly declined to determine "whether there is [any sufficiently] limited period [of time] for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny." *Id.* at 310 n.3; *see also* Oral Arg. at 8:22, *Carpenter v. United States*, 585 U.S. 296 (2018) (No. 16-402) (Roberts, C.J., remarking, "[i]t seems to me the line is between information to which the authorities have access and information to which they don't" rather than between shorter and longer-durations of data). Indeed, the implication of the Court's decision is that, when it comes to the ways in which new technologies threaten to upend reasonable expectations of privacy, it is the nature of the

intrusion on privacy rather than the duration of a particular surveillance demand that matters most.

In any event, shorter-term location tracking is just as capable of revealing sensitive private information as two or more days of tracking. Geofence searches of even limited duration, like the searches in *Carpenter* and *Jones*, may expose people's "indisputably private" information—the visit 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); *see also id.* ("even short-term monitoring" seriously threatens reasonable expectations of privacy"); *Carpenter*, 585 U.S. at 311. In doing so, geofence searches facilitate inferences about people's habits of life.

This Court has long held that precise, short-term searches run afoul of the Fourth Amendment where, as here, they could reveal information inside constitutionally protected spaces. *See Karo*, 468 U.S. at 715 (Fourth Amendment protects against warrantless electronic tracking into a person's home); *Kyllo*, 533 U.S. at 30, 37 (using thermal imaging to peer through walls of a home was a search, even though scan "took only a few minutes" and could not show much detail). Geofence searches open the door to these kinds of invasions as a matter of course. And because geofence searches cast a wide dragnet, they reveal such information for large numbers of people who happened to be in the chosen radius—including, necessarily, non-suspects.

Beyond identifying people in sensitive places and raising inferences about their lives, police can use geofence data to identify sensitive relationships and associations because the data necessarily identifies any individuals traveling or meeting together. As a result, even short-duration geofence warrants can identify the friends, family, and other intimate associates of any individual caught up in the sweep. Like personal writings, information about where a person was at some time in the past can reveal protected expressive and associational activities—it can reflect "a wealth of detail about her familial, political, professional, religious, and sexual associations." *Riley*, 573 U.S. at 396 (quoting *Jones* 565 U.S. at 415 (Sotomayor, J., concurring)). Information about multiple peoples' locations only increases the privacy harm by showing associations between and among individuals. *See Riley*, 573 U.S. at 396.

Even a small number of data points can reveal private whereabouts in non-public and constitutionally sensitive places. "[E]ven just a few points of . . . location history" can reveal a person's "unique and habitual" movements, so much so that "it is almost always possible to identify people by observing even just a few points of their location history." *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 343-44 (4th Cir. 2021) (en banc) (relying on a study in the record that "shows that identity is easy to deduce from just a few random points of an individual's movements," and explaining that "common sense and ample authority over the last decade corroborates this conclusion" (footnote omitted)). As Mr. Chatrie's forensics expert showed at the district court, identification was possible in this

case as well. Using only the "anonymized" location data points Google provided to the government, the expert was able to locate the homes of three individuals who had merely and momentarily passed through the geofence, and then could determine their identities through public records. Pet.App.321a n.39; *see also Karo*, 468 U.S. at 716 (learning that "a particular article—or a person, for that matter—is in an individual's home at a particular time" is an invasion of privacy to which the Fourth Amendment applies).

2. The government searched the private contents of users' accounts, not Google's business records.

An additional reason for the Court to find that a Fourth Amendment search occurred here is that the contents of an individual's account, including their location history, are the individual's private and personal information, not Google's own business records. Google tells its users as much. JA-15 (location history is "a journal of a user's location and travels that is created, edited, and stored by and for the benefit of Google users who have opted into the service."). Therefore this data is the "modern-day equivalent[] of an individual's own 'papers' or 'effects.'" *Carpenter*, 585 U.S. at 319. It is a search to access an unspecified number of these private user accounts maintained by a third-party service provider like Google, just as it would be a search for the police to rummage through an entire floor of hotel rooms or open each sealed letter in a bag of mail. *Id.* at 326 (Kennedy, J., dissenting) ("the only question necessary to decide is whether the Government searched *anything of Carpenter's*" and recognizing

that individuals have a reasonable expectation of privacy in their things, even if entrusted to third parties (emphasis added)); *see id.* at 400 (Gorsuch, J. dissenting). This Court has consistently recognized this principle. *See, e.g.*, *Ex Parte Jackson*, 96 U.S. 727, 733 (1877) (letters held by mail carrier protected); *Stoner v. California*, 376 U.S. 483 (1964) (contents of hotel room protected even if accessible by hotel staff).[3]

The consequences of holding otherwise would be radical. If the government may search, without constitutional restriction, millions of people's location data at once so long as it only looks at *some* of each person's data, it would be free to cast dragnet upon dragnet, and not even to *act upon* suspicion but to endeavor to *generate* it.

---

[3] That the data in this case belongs to this user is a further distinction from *Carpenter* that strengthens the conclusion that a search occurred here. As the *Carpenter* majority opinion and dissents alike acknowledged, whatever the scope of the "third party doctrine" may be for business records, *see generally United States v. Miller*, 425 U.S. 435 (1976), it does not necessarily apply to private information merely held by a third party, which is the case here. *Carpenter*, 585 U.S. at 297 (CSLI records maintained by wireless carriers protected by Fourth Amendment); *id.* at 342 (Thomas, J., dissenting) (property right depends on creation, right to control and right to destroy, not just maintenance of information); *id.* at 405 (Gorsuch, J., dissenting) (a person's cell-site data could qualify as his property under existing law, a promising basis for Fourth Amendment protection).

II. GEOFENCE WARRANTS ARE UNCONSTITUTIONAL GENERAL WARRANTS.

A. Geofence warrants replicate long-reviled general warrants because they make suspects out of bystanders and grant overbroad discretion to law enforcement.

Geofence searches have inherent and inevitable capacity to ensnare innocent bystanders—and so warrants purporting to authorize this tool can never be constitutionally adequate. Indeed, geofence warrants are a contemporary incarnation of the general warrants that the Founders so reviled.

General warrants' central harm was to bystanders whom the government had no cause to search. Most notoriously, "writs of assistance" gave British officers "blanket authority to search where they pleased"—an authority Revolutionary advocate James Otis called "the worst instrument of arbitrary power . . . because [it] placed the liberty of every man in the hands of every petty officer." *Stanford v. Texas*, 379 U.S. 476, 481 (1965) (citation modified). These instruments let officials go house to house, searching for smuggled goods and evidence of seditious libel. *See United States v. Wilson*, 143 F.4th 647, 653 (5th Cir. 2025). In one infamous case, officers searched and seized papers from up to 50 homes. *See Wilkes v. Wood*, 98 Eng. Rep. 489, 490 (1763). The affronts of these searches, "which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity," were an impetus for the Founding of a new country. *Riley*, 573 U.S. at 403; *Stanford*, 379 U.S. at 481-82.

Geofence warrants replicate the kind of open-ended, "search anyone and anywhere" approach to privacy that the Founders flatly rejected. Indeed, they amount to a digital-age version of the kind of general search this Court rejected almost half a century ago in *Ybarra*. There, law enforcement obtained a warrant to search a tavern and its bartender after demonstrating probable cause that the bartender was dealing heroin from the tavern. In executing the warrant, police conducted patdowns of most of the customers present in the bar at the time of the search. 444 U.S. at 88. When the police searched the pockets of one such customer, Ventura Ybarra, they found foil packets of heroin in a cigarette pack. *Id.* at 89. Ybarra was found guilty of heroin possession at trial. *Id.*

On review, this Court held that the search of Ybarra violated the Fourth Amendment. It explained that while the police had probable cause to search the tavern and arrest its bartender, they "knew nothing in particular about Ybarra, except that he was present, along with several other customers, in a public tavern at a time when the police had reason to believe that the bartender would have heroin for sale." *Id.* at 91. The Court emphatically rejected the notion that "a person's mere propinquity to others independently suspected of criminal activity [could], without more, give rise to probable cause to search that person." *Id.* (citation modified).

Like in *Ybarra*, when police seek a geofence warrant, they are investigating a place without any knowledge whatsoever of the people whose private information they are seeking to obtain—let alone any measure of suspicion or probable cause. And while "a warrant to search a place cannot normally be construed to authorize a search of each individual in

that place," *id.* at 92 n.4, that is precisely what geofence warrants purport to allow, super-powered by Google's retrospective database of the private location information of hundreds of millions of people.

It is axiomatic that a warrant cannot authorize officers to search every house in an area of a town for a suspect, or every safety deposit box in a bank for some evidence of a crime. *Cf. Snitko v. United States*, 90 F.4th 1250, 1263-66 (9th Cir. 2024) (search of numerous safety deposit boxes pursuant to a warrant that purported to allow inventory searches violated Fourth Amendment, because individualized probable cause is required for valid criminal investigative search). Flouting that principle, geofence searches inevitably implicate innocent people who happen to be in the wrong place at the wrong time.[4]

---

[4] Below, the government argued that Petitioner could not raise the interests of other Google users because one may not vicariously assert another's Fourth Amendment rights. Br. for the United States 24, *United States v. Chatrie*, No. 22-4489 (4th Cir. Mar. 10, 2023) (citing *Rakas v. Illinois*, 439 U.S. 128, 133-34 (1978)). But Petitioner is asserting his own rights in his Google account, the data stored there, and the privacy of his movements over time. Once someone demonstrates standing to raise a Fourth Amendment claim, probable cause, overbreadth, and particularity of the warrant are all properly at issue. Particularity and probable cause constrain the search to its lawful scope which necessarily reduces impacts on the privacy of innocent third parties. Thus, a search's impact on innocent bystanders is always part of the calculation of whether or not it is lawful. *See Berger v. New York*, 388 U.S. 41 (1967) (surveillance that impacts third parties must be limited).

B. Geofence warrants fail the Fourth Amendment's probable cause, particularity, and judicial review requirements.

The Framers of the Fourth Amendment sought to preclude general warrants through the Amendment's particularity and probable cause requirements. *See Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971) (Fourth Amendment was meant to forestall "general, exploratory rummaging"); *Andresen v. Maryland*, 427 U.S. 463, 480 (1976) (particularity guards against "a general, exploratory rummaging"); *Steagald v. United States*, 451 U.S. 204, 220 (1981) (warrants that "specif[y] only an offense" and leave to police discretion "the decision as to which persons" to pursue are unconstitutional). Critical to enforcing these limitations is the requirement that neutral magistrates review and issue warrants. *Id.* ("The central objectionable feature of [general] warrants was that they provided no judicial check on the determination of the executing officials that the evidence available justified an intrusion into any particular home."). The geofence warrant in this case fails each of these requirements: It is insufficiently particularized because it does not identify any individual person, device, or account as to whom there is probable cause to search, and it leaves police and Google to decide those details for themselves in a three-step process conducted without judicial supervision.

Consider "Step 2" in this case. The government obtained "contextual" data beyond the warrant's geographical and time constraints. *See* Pet.App.289a-90a ("[I]f a user's location fell within the geofence at Step 1, law enforcement can obtain *all* location points

for identified users over an expanded timeframe at Step 2. This means that, at Step 2, no geographic barrier confines the information searched."). This decision was made without probable cause or judicial oversight. Similarly, at Step 3, police obtained identifying subscriber information for "devices of interest," again selected by Google and the government. *Id.* The exploratory discretion that characterized the execution of these searches of Google-stored data improperly ceded the neutral magistrate's oversight role to government officials and Google's compliance officers. Any similar process "fails to curtail or define the agents' discretion in any meaningful way." *In re Search of: Info. Stored at Premises Controlled by Google, as Further Described in Attachment A*, No. 20 M 297, 2020 WL 5491763, at *6 (N.D. Ill. July 8, 2020); *see* Pet.App.126a ("Google, not a magistrate, was the sole entity that could confine the scope of the ultimate search." (Berner, Circuit Judge, concurring)); Pet.App.105a ("Google's three-step process was neither designed nor mandated by a magistrate" but "merely expresses the preferences and policy of Google, a private company". (Wynn, J., concurring)). All of this contravenes the purpose of the Fourth Amendment's warrant requirement, which "interpose[s] a neutral magistrate between the citizen and the law enforcement officer." *Nat'l Treasury Emps. Union v. Von Raab*, 489 U.S. 656, 667 (1989).

Nor are these warrants supported by probable cause. The mere fact that many, or even most, people use devices that record and store their location information with Google is insufficient to show the perpetrator of a crime under investigation used such a device, and in any case cannot justify a search of the accounts of *all* Google's users to scan their location

data for points of interest. Nor could these warrants justify tracking any users estimated to have been in their target locations during specified time periods. *See Ybarra*, 444 U.S. at 91-92.

Far from meeting constitutional requirements, geofence warrants give police unfettered discretion to engage in digital dragnets that the Founders would have abhorred. *See United States v. U.S. Dist. Ct. ("Keith")*, 407 U.S. 297, 327 (1972) (Douglas, J., concurring) ("recurring desire of reigning officials to employ dragnet techniques to intimidate their critics lies at the core of" the Fourth Amendment).

C. Geofence warrants issued in other investigations further demonstrate their broad impact on bystanders.

As in this case, geofence warrants in other investigations have swept up many people unconnected to the investigation, including people in sensitive locations who just happen to be in the area at the time of the crime. The geofence warrant at issue here authorized the search of a 17.5-acre area over the course of 120 minutes, encompassing a church, a hotel, a senior living facility, and anyone who happened to be inside at the time. Pet.App.294a-95a, 302a-03a. Google has said that all geofence warrants, regardless of the size of the geographic area described in the warrant, require searching through hundreds of millions of user accounts. Pet.App.6a. But even if Google's technology allowed it to constrain initial searches to areas specified in geofence warrants, these warrants would still impact scores of people.

Examples abound: In *People v. Meza*, a single warrant purportedly authorized police to identify all devices in six densely populated areas of Los Angeles

County on a Friday morning during commute hours. 312 Cal. Rptr. 3d at 17. One of the geofenced areas covered seven-and-a-half-acres of residences over a 75-minute period in the early morning when many people would be home, "despite the lack of any evidence (or supported inference) that the suspects left their vehicles." *Id.*

In a case in Wisconsin, two geofence warrants sought data for all Google customers within areas in Milwaukee covering roughly 29,387 square meters during a total of nine hours.[5] In response, Google provided the government with device identifiers for nearly 1,500 devices.

In San Francisco, the second densest city in the United States,[6] a single warrant authorized the search of 13 areas, including "thousands of homes, numerous places of worship, multiple schools, many businesses, and highways and other busy roadways" and resulted in the disclosure of more than 2,600 accounts.[7]

---

[5] See Thomas Brewster, *Google Hands Feds 1,500 Phone Locations In Unprecedented 'Geofence' Search*, Forbes (Dec. 11, 2019), https://www.forbes.com/sites/thomasbrewster/2019/12/11/google-gives-feds-1500-leads-to-arsonist-smartphones-in-unprecedented-geofence-search/.

[6] Kale Williams, *S.F. Ranked No. 2 Most Dense City in U.S.*, SFGate (Apr. 3, 2014), https://perma.cc/QBQ7-NRRV.

[7] Richard Salgado, *Skirting Judicial Scrutiny by Mooting and Scooting*, Lawfare (Feb. 26, 2025), https://perma.cc/D7YB-5XBF; Thomas Brewster, *The Wiretap: Google Fought A Court Order For 2,600 User Locations. And Won.*, Forbes (Feb. 18, 2025) https://perma.cc/4UVR-WANJ.

As part of the FBI's investigation into events at the U.S. Capitol on January 6, 2021, Google provided investigators with location data for more than 5,000 devices.[8]

In New Mexico, Google disclosed data from 3,100 devices over a vast area, including devices from about 1,000 people at a funeral.[9]

And a recent ACLU investigation into geofence warrants issued in San Francisco uncovered searches of "[h]undreds of places where people live . . . 84 places where people work . . . 32 bars and restaurants . . . 12 places of worship . . . 7 medical sites of care . . . 7 schools and daycares" and countless "[p]eople in transit, or simply walking down the street."[10] The vast majority of people affected by these geofence warrants will never even receive notice of the search.

By 2021, geofence warrants constituted more than 25% of all warrants received by Google.[11] These warrants have been used for investigations into a wide variety of major and minor crimes, from homicide to

---

[8] Mark Harris, *A Peek Inside the FBI's Unprecedented January 6 Geofence Dragnet*, WIRED (Nov. 28, 2022), https://www.wired.com/story/fbi-google-geofence-warrant-january-6/.

[9] Ryan Laughlin, *4 Investigates: Geofence Fight*, KOB4 (Sep. 4, 2024), https://perma.cc/JL84-K34Q (current and former U.S. Attorneys recognizing the privacy concerns implicated by such a broad search).

[10] Jake Snow, *Cops Blanketed San Francisco In Geofence Warrants. Google Was Right to Protect People's Privacy*, ACLU of N. Cal. (Jan. 7, 2024), https://perma.cc/JS38-LFQW.

[11] Google, *Supplemental Information on Geofence Warrants in the United States*, https://perma.cc/B9J6-B5HL.

retail theft to theft of a wallet.[12] These warrants have also been used to identify people in particularly controversial investigations, including people at the U.S. Capitol on January 6, 2021, and protesters after police killings in Minneapolis and Kenosha in 2020.[13]

Unsurprisingly, the dragnet nature of these warrants leads to innocent people becoming suspects and suffering severe consequences in their lives. In one case in Gainesville, Florida, police sought detailed information about a man in connection with a burglary after seeing his travel history in the first step of a geofence search.[14] However, the man's travel history was generated through an exercise tracking app he used to log months of bike rides, including a regular loop ride that happened to take him past the site of the burglary several times. And in Minnesota, another innocent man's name was disclosed to a local

---

[12] Tony Webster, *How Did the Police Know You Were Near a Crime Scene? Google Told Them*, MPRNews (Feb. 7, 2019), https://perma.cc/WH2N-S6L2; Jeremy Harris, *Layton Police Use Controversial 'Geo-fence' Warrants to Investigate Property Crimes*, 2KUTV (May 16, 2022), https://perma.cc/3R93-PVY6.

[13] Thomas Brewster, *Google Dragnets Harvested Phone Data Across 13 Kenosha Protest Acts of Arson*, Forbes (Aug. 31, 2021), https://www.forbes.com/sites/thomasbrewster/2021/08/31/google-dragnets-on-phone-data-across-13-kenosha-protest-arsons; Zach Whittaker, *Minneapolis Police Tapped Google to Identify George Floyd Protesters*, TechCrunch (Feb. 6, 2021), https://perma.cc/ZLB2-7P9C; *see also supra* note 8.

[14] Jon Schuppe, *Google Tracked his Bike Ride Past a Burglarized Home. That Made Him a Suspect.*, NBC News (Mar. 7, 2020), https://perma.cc/4T3C-37QV.

reporter after police files identified him in a burglary investigation through a geofence search.[15]

Misidentifications like these are more likely to occur (with serious ramifications) in the geofence context because the only link between an individual and the crime is that the individual happened to be in the area around the time the crime occurred. Additionally, there is a margin of error when calculating location from the data. This can force a suspect to have to prove their innocence—that they were in or near the area for an unrelated purpose—rather than police having to prove their guilt. This not only reverses the presumption of innocence but also increases the risk of erroneous arrests (or worse) based on both confirmation bias and implicit bias.[16]

III. COURTS THAT HAVE GRANTED OR UPHELD GEOFENCE WARRANTS HAVE MADE EFFORTS TO ENSURE THEIR IMPACTS ON BYSTANDERS ARE LIMITED.

Geofence searches are Fourth Amendment searches and courts are issuing impermissible general warrants to authorize and compel them. Recognizing their impact on bystanders, some courts that have disagreed have nevertheless attempted to conform these searches to the standards for a valid warrant by imposing limitations beyond the essential probable cause, particularity, and overbreadth requirements.

---

[15] Jennifer Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police*, N.Y. Times (Apr. 13, 2019), https://perma.cc/3HCX-Y3RV.

[16] *See, e.g.,* Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. Pa. L. Rev. 327 (2015).

First, it is black-letter law that warrants must be approved by a neutral, detached magistrate to limit officer discretion. This is "the time-tested means of effectuating Fourth Amendment rights." *Keith*, 407 U.S. at 318; *see also Johnson v. United States*, 333 U.S. 10, 14 (1948) ("When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer."); *Steagald,* 451 U.S. at 212 ("an officer engaged in the often competitive enterprise of ferreting out crime may lack sufficient objectivity" to determine the necessity of the search (citation modified)).

That didn't happen here. "Steps 2 and 3 of this warrant [still] leave the executing officer with *unbridled* discretion and lack any semblance of objective criteria to guide how officers would narrow the lists of users." Pet.App.327a-28a. Those steps "fail to provide the executing officer with clear standards from which he or she could reasonably . . . ascertain and identify . . . the place to be searched [or] the items to be seized." *Id.* (citation modified).

Recognizing this principle, in some geofence cases, magistrate judges have issued warrants that require additional judicial review or a second warrant before investigators can take any additional steps to alter the scope of the search (such as to expand the time frame or geographic area for a subset of individuals at Step 2) or to unmask individuals at Step 3. In one federal case, the court first denied a warrant that allowed officer discretion at the latter steps in the search, but then granted a new warrant that required law enforcement to seek a second court authorization for additional information. *In re Search of Info. That is Stored at the Premises Controlled by Google LLC*, 579 F. Supp. 3d 62, 88-89 (D.D.C. 2021). Requiring

ongoing involvement of the issuing magistrate is a bare-minimum guardrail to address the failures of the three-step process deployed here.

Second, issuing magistrates should also engage in careful narrowing of the scope of geofence warrants in order to minimize the potential impact of these searches on privacy. Minimization is a longstanding practice when even warranted searches pose risks to Fourth Amendment values. For example, in *Berger v. New York*, 388 U.S. 41 (1967), this Court emphasized that surveillance that impacts not only the target but also innocent third parties should be limited, or minimized, to the extent possible. Ultimately, it struck down a wiretapping statute that had authorized two months' interception of telephone conversations and lacked any requirements that would minimize the impacts on third parties, explaining the Fourth Amendment requires limiting wiretapping that "indiscriminately" overhears "all conversations," *id.* at 58-59, including those of individuals "not even suspected of crime," *id.* at 65 (Douglas, J., concurring). *Berger* set forth the Fourth Amendment principle that surveillance that meaningfully impacts third parties must be narrowly tailored and employ procedural safeguards to avoid sweeping in irrelevant and innocent communications. *See id.* at 58-60.

In the context of other technology-derived searches with similar impacts on bystanders, courts have tried to limit a warrant's impacts on innocent individuals by ensuring the warrant's geographic and temporal scope is narrow and by imposing minimization protocols for data not relevant to the

investigation. *See, e.g.*, *In re Use of A Cell-Site Simulator to Identify a Cellular Device in a Narcotics Trafficking Case*, 623 F. Supp. 3d 888, 890 (N.D. Ill. 2022) (warrant for cell site simulator must include "geographical restrictions on the government's use of the simulator . . ., restrictions on the use of resulting data obtained from the simulator, and deletion of the remaining captured data once the suspect's phone number is identified").

Geofence warrants are narrower if magistrates require that the geofence area be relatively small and drawn to exclude sensitive locations. For example, in one case, a district court noted that surveillance footage showed the suspects were generally alone inside a business in an industrial area and that the geofenced area was drawn specifically to avoid "residences or other particularly sensitive locations." *In re Search of Info. That is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d at 85. Therefore, it concluded the warrant did not "have the potential of sweeping up the location data of a substantial number of uninvolved persons." *Id.* at 80, 85. In an Illinois case, a district court issued a geofence warrant because the target locations excluded "[r]esidences and commercial buildings along the streets" leading to and from the sites of crimes, and "the government [] structured the geofence zones to minimize the potential for capturing location data for uninvolved individuals." *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 353, 358 (N.D. Ill. 2020).

Finally, other techniques, such as anonymization, use of pseudonyms, and robust data deletion practices can also minimize the impacts of geofence searches on bystanders. Bystanders should be effectively masked from law enforcement until the point there is probable cause to believe that the specific person's location data is evidence of the crime under investigation. And courts should also ensure that non-responsive data showing the movements of uninvolved people is not used for other purposes. Any information should be destroyed when it is no longer needed. *See, e.g., Commonwealth v. Perry*, 184 N.E.3d 745, 770 (2022) ("The warrant must include protocols for the prompt and permanent disposal of any and all data that does not fit within the object of the search following the conclusion of the prosecution.").

IV. THIS COURT SHOULD NOT USE THIS CASE, WHICH REFLECTS FACTS FROM 2019, TO AUTHORIZE REVERSE LOCATION SEARCHES CONDUCTED TODAY.

All geofence searches share a critical characteristic: They drag a net through a large repository of information in the hopes of identifying previously unknown suspects based on their proximity to a crime. Along the way they are likely to capture innocent bystanders, impacting their privacy and liberty. Geofence searches' breathtaking intrusion into matters that users reasonably expect to be private is reason enough to find this and other geofence searches are searches within the meaning of the Fourth Amendment and are the product of an unconstitutional general warrant.

At a minimum, however, the record in this case cannot support a blanket ruling in favor of geofence searches in future investigations or other factual contexts. The record below reflects how law enforcement and Google conducted geofence searches in 2019. Seven years later, the landscape has changed dramatically. Today, Google is no longer able to conduct such searches.[17] As the United States acknowledges, that change became effective in July 2025; since then, it has not been possible to conduct such geofence searches with Google users' data. BIO.18. The Court should be wary of setting a Fourth Amendment rule based on discontinued technology that renders the search in this case highly unlikely to recur. *See Carpenter*, 585 U.S. at 316 ("[W]hen considering new innovations . . ., the Court must tread carefully in such cases, to ensure that we do not embarrass the future." (citation modified)). This 2019 investigation involving one company is a poor vehicle for guiding lower courts on how to issue warrants for future geofence searches, especially of data held by other companies.

The record supports a holding that geofence searches are unconstitutional, and gives this Court a factual basis for answering the question presented on the facts of this case: whether this geofence search violated the Fourth Amendment. The Court should take care not to make broader pronouncements that depend on the already-obsolete location-history technology in this case. Myriad issues potentially

---

[17] *See* Marlo McGriff, *Updates to Location History and New Controls Coming Soon to Maps*, Google Keyword Blog (Dec. 12, 2023), https://perma.cc/QA3X-LQT2.

relevant to the Fourth Amendment analysis will depend on how a particular technology and a particular search methodology work. The Court should ensure that any ruling here is based on and cabined to the facts reflected in the record in this case and does not purport to bless geofence searches on the basis of facts not presented here.

CONCLUSION

For the foregoing reasons, this Court should reverse.

Respectfully submitted,

Nathan Freed Wessler
Brett Max Kaufman
Esha Bhandari
Ben Wizner
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
18th Floor
New York, NY 10004

Jennifer Lynch
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Jennifer Stisa Granick
Counsel of Record
Cecillia D. Wang
Evelyn Danforth-Scott
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
425 California Street
Suite 700
San Francisco, CA 94104
(212) 549-2500
jgranick@aclu.org

Matthew W. Callahan
ACLU OF VIRGINIA FOUNDATION
P.O. Box 26464
Richmond, VA 23261

Counsel for Amici Curiae American Civil Liberties Union, American Civil Liberties Union of Virginia, Electronic Frontier Foundation, and Center on Privacy & Technology at Georgetown Law

Dated: March 2, 2026