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 United States Court of Appeals for the Fourth Circuit

BRIEF FOR THE RUTHERFORD INSTITUTE AS AMICUS CURIAE IN SUPPORT OF NEITHER PARTY

JOHN W. WHITEHEAD
WILLIAM E. WINTERS
The Rutherford Institute
109 Deerwood Road
Charlottesville, VA 22911

ETHAN H. TOWNSEND
Counsel of Record
MAURA R. CREMIN
McDermott Will & Emery LLP
500 North Capitol Street NW
Washington, DC 20001
(202) 756-8000
ehtownsend@mwe.com

Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Constitution & Statutes

Other Authorities

Interest of Amicus Curiae[1]

The Rutherford Institute is a nonprofit civil liberties organization headquartered in Charlottesville, Virginia. Founded in 1982 by its President, John W. Whitehead, the Institute provides legal assistance at no charge to individuals whose constitutional rights have been threatened or violated and educates the public about constitutional and human rights issues affecting their freedoms. The Rutherford Institute works tirelessly to resist tyranny and threats to freedom by seeking to ensure that the government abides by the rule of law and is held accountable when it infringes on the rights guaranteed by the Constitution and laws of the United States.

Summary of Argument

The Framers wrote the Fourth Amendment to ensure the persons and property of the American people would be secure from unreasonable search and seizure by the federal government. The Framers had sights trained specifically on general warrants. Those warrants did not name the person or thing to be seized, but just gave blanket authority to search for wrongdoing. Without such guardrails, those warrants gave Crown officials in England and the American colonies virtually unrestricted ability to rummage through the property and papers of individuals. Outrage at this abuse was central to the colonists'

---

[1] No counsel for a party authored this brief in whole or in part, and no entity or person, other than Amicus Curiae, its members, and its counsel, made a monetary contribution intended to fund the preparation or submission of this brief. Counsel of record for the parties received notice of Amicus Curiae's intent to file this brief at least 10 days prior to its due date.

decision to declare independence and enshrine their rights in the Constitution.

But what is old is new again. Law enforcement is using surveillance systems that search the data of millions of individuals based on nothing more incriminating than the fact that they own a cell phone—the same pervasive piece of property as a colonist's quill. The geofence warrants at issue here are one such example. This tool requires Google to search the location data of all its users to identify those who were in a particular place at a particular time, regardless of whether there is a shred of evidence linking any user to a crime.

As this Court has recognized, "an individual maintains a legitimate expectation of privacy in the record of his physical movements." *Carpenter* v. *United States*, 585 U.S. 296, 310 (2018). But the Court has left the precise contours of that right undefined. As a result, lower courts confronting geofence warrants adopt divergent and often contradictory analyses. And this has resulted in Americans' private data being subject to search and seizure by the government without any probable cause. This case provides the Court with a valuable opportunity to clarify the scope of Fourth Amendment privacy protections and head off further encroachments into the rights of American citizens.

Argument

I. Geofence warrants are general warrants of the type the Fourth Amendment is meant to protect against

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches

and seizures, shall not be violated," and guarantees that warrants will not be issued except "upon probable cause * * * and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The purpose of this amendment was to ensure that Americans would always be protected from "intrusion and seizure by officers acting under the unbridled authority of a general warrant." *Stanford* v. *Texas*, 379 U.S. 476, 481 (1965).

A. The Fourth Amendment was designed to prevent the issuance of general warrants.

"[T]he Fourth Amendment was most immediately the product of contemporary revulsion against a regime of writs of assistance." *Stanford,* 379 U.S. at 482. Yet "its roots go far deeper." *Ibid*. General warrants have a history stretching back to at least the 16th century. Laura K. Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181, 1208-1209 (2016). These warrants were considered particularly offensive to individual liberty because they "failed to name the individual possessing the things to be searched or seized." Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 Va. L. Rev. 869, 874 (1985).

1. *General warrants were reviled under 18th century English common law.*

General warrants were issued in England during the Tudor and Stuart periods as part of the Crown's efforts to enforce religious orthodoxy and stifle political dissent. Donohue, *The Original Fourth Amendment*, 83 U. Chicago L. Rev. at 1208-1209. Queen Mary I used them to try to re-establish the Catholic Church in England. *Id*. at 1208. Queen

Elizabeth I established a High Commission to target sedition and slander against the Crown. *Id*. at 1208-1209. Among the Commission's tools were general warrants. *Id*. at 1209. James I expanded the Commission's powers, and after discovering the Gunpowder Plot in 1605, he signed two general warrants to find those responsible. *Id*. at 1210.

English legal scholars increasingly began to condemn general warrants. Perhaps the most prominent critic was the jurist Sir Edward Coke. Despite having assisted James I in executing general warrants during the Gunpowder Plot investigations, Coke became convinced that these warrants were inimical to English freedoms and argued that they violated Magna Carta. *Id*. at 1211-1212. No less a titan of English jurisprudence than Sir Matthew Hale stated in his 1736 *Historia Placitorum Coronae* ("History of the Pleas of the Crown") that a "general warrant to search in all suspected places is not good, but only to search in such particular places, where the party assigns before the justice his suspicion and the probable cause thereof, for these warrants are judicial acts, and must be granted upon examination of the fact." Matthew Hale, 2 *Historia Placitorum Coronae* 150 (Nutt and Gosling 1736). William Blackstone cited both Coke and Hale in his analysis of warrants in the *Commentaries*. William Blackstone, 4 *Commentaries on the Laws of England* 287 (Clarendon 1769). Blackstone rejected the validity of general warrants, stating "[a] general warrant to apprehend all persons suspected, without naming or particularly describing any person in special, is illegal and void for its uncertainty; for it is the duty of the magistrate, and ought not be left to the officer, to judge of the ground of suspicion." *Id*. at 288.

This growing consensus among 17th and 18th century legal scholars about the illegality of general warrants shaped English jurisprudence. The first reported decision on general warrants, *Huckle* v. *Money*, was issued in 1763. 19 How. St. Tr. 1404, 95 Eng. Rep. 768 (C.P. 1763). In that case, Huckle, a journeyman printer, was arrested on suspicion of having printed an allegedly libelous publication. *Ibid*. Though Huckle was only detained for six hours and was treated well while in custody, the jury nonetheless awarded him £300 in damages. *Ibid.* The court sustained the verdict on the ground that Huckle was arrested under a general warrant, since the warrant did not specifically order Huckle's arrest. *Ibid.* The Lord Chief Justice condemned the use of general arrest warrants in strong terms:

> To enter a man's house by virtue of a nameless warrant, in order to procure evidence, is worse than the Spanish Inquisition; a law under which no Englishman would wish to live an hour; it was a most daring public attack made upon the liberty of the subject.

Id. at 769.

In the same year, the court decided *Wilkes* v. *Wood*, captioned "The Case of General Warrants." 98 Eng. Rep. 489 (C.P. 1763); Schnapper, *Unreasonable Searches and Seizures of Papers*, at 878. In that case, government officials suspected that Wilkes, a member of Parliament, had authored libelous materials, and searched Wilkes' home, seizing his papers and manuscripts. *Wilkes*, 98 Eng. Rep. 489. The jury awarded Wilkes damages of £1,000. *Ibid.* at 499. The Court again upheld the verdict on the grounds that the warrant failed to identify the suspect. *Ibid*. at 498.

In the landmark 1765 case *Entick* v. *Carrington*, the court made clear that even a warrant that named the individual suspect could be a general warrant if it failed to identify items to be searched and seized. 19 How. St. Tr. 1029, 95 Eng. Rep. 807 (C.P. 1765). Entick, who authored a weekly paper, was accused of seditious libel. *Ibid.* In an opinion which would serve as a "wellspring of the rights now protected by the Fourth Amendment," *Stanford*, 379 U.S. at 484, the court held that the warrant was unlawful because it failed to identify the items that had been targeted for search and seizure. *Entick* v. *Carrington*, 19 How. St. Tr. at 1067. Instead, the officers could rifle through all of Entick's papers unchecked, which amounted to an illegal general warrant. *Ibid.*

2. *Opposition to general warrants was a cornerstone of the Fourth Amendment.*

American colonists had, if anything, an even greater hatred of search and seizure than their English counterparts. The declarations of rights in early colonial charters and constitutions generally incorporated English common law with respect to search and seizure. Schnapper, *Unreasonable Searches and Seizures of Papers* at 913. During the 17th century, when general warrants were permitted in England, they were far more restricted in the colonies. Donohue, *The Original Fourth Amendment* at 1241-1242. The general warrants cases in England received immense publicity in the American colonies and were the subject of considerable commentary. Schnapper, *Unreasonable Searches and Seizures of Papers* at 913; Donohue, *The Original Fourth Amendment* at 1257-1258.

One type of general warrant that was allowed in the colonies was the so-called writ of assistance,

which provided customs agents with the ability to search locations ranging from ships and storehouses to homes to search for goods that did not meet customs regulations. Donohue, *The Original Fourth Amendment* at 1242. The use of writs of assistance led to escalating conflict between the colonies and the Crown administration. An instructive case is that of Edward Randolph, the chief agent of the commissioners of customs in New England. When Randolph reported that the Massachusetts Bay Company was abusing its charter and tolerating illegal trade, the Crown revoked the Company's charter. *Ibid.* During the 1689 colonial uprising, Randolph was imprisoned and returned to England. *Id*. at 1242-1243. Upon his return to the colonies in 1692, Randolph began investigating nearly all the major ports in the colonies, relying heavily on general warrants to identify smuggling, corruption, and poor record keeping. *Id*. at 1243. Because of Randolph's efforts, Parliament passed new legislation to end illicit trade in the colonies, which colonial officials were instructed to enforce using writs of assistance. *Id*. at 1242-1243. The result was mounting tension, as colonists increasingly found their homes and businesses subject to searches, while they had no judicial recourse to object. *Id*. at 1243.

These tensions grew during the French and Indian War and culminated in the pivotal *Paxton's Case*. In 1755, Governor William Shirley began directing his customs agents (one of whom was named Charles Paxton), to use writs of assistance to crack down on illicit trade with French Canada. *Id*. at 1246-1247. By the 1760s, the practice had become widely accepted, with Lord Chatham, the secretary of state for the Southern Department, directing the new

Governor of the Province of Massachusetts Bay to use writs of assistance to stop trade with the French Indies as well. *Id*. at 1248.

When the writs of assistance expired in 1761, the Society for Promoting Trade and Commerce challenged their renewal. *Ibid.* The Society was represented on a pro bono basis by prominent lawyer James Otis. *Id*. at 1249. In one of the great orations of American history, Otis forcefully condemned writs of assistance as "the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law-book." James Otis, *Speech Against the Writs of Assistance* (February 24, 1761). The exercise of the writ, which "places the liberty of every man in the hands of every petty officer," was the kind of power that had "in former periods of history, cost one king of England his head and another his throne." *Ibid.*

Otis's speech received considerable attention and was credited as helping bring the American public to support independence. Donohue, *The Original Fourth Amendment* at 1250. One particularly enthusiastic observer of Otis's speech was a young John Adams, who later recalled that "[e]very man of an crowded Audience appeared to me to go away, as I did, ready to take up Arms against Writs of Assistants." *Id*. at 1249.

Outrage at writs of assistance would only grow with the passage of the 1767 Townshend Revenue Act, which empowered officials "to enter houses or warehouses, to search for and seize goods prohibited to be imported or exported * * * or for which any duties are payable, or ought to have been paid." Donohue, *The Original Fourth Amendment* at 1260.

The terms of this statute were at odds with practice in the colonies, where any writs granted tended to be specific, and American legal treatises treated the general warrants authorized in the Townshend Act as illegitimate. *Id*. at 1260-1261. For example, in his *Letters from a Farmer in Pennsylvania*, John Dickinson described the writ as "an engine of oppression," noting that "the greatest asserters of the rights of Englishmen have always strenuously contended, that such a power was dangerous to freedom." John Dickinson, *Letters from a Farmer in Pennsylvania, Letter IX*, at 93 (The Outlook Company 1903).

By the time the colonists declared independence, there was overwhelming consensus that general warrants were illegitimate. *See* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 Mich. L. Rev. 547, 655 n. 299 (1999). Indeed, opposition to general warrants was so central to the colonists' sense of civil liberties that it was incorporated into the Virginia Declaration of Rights, which significantly influenced the development of, not only later state constitutions, but the United States Constitution. Donohue, *The Original Fourth Amendment* at 1265. The Virginia Declaration of Rights, which was passed in 1776, unequivocally stated that "general warrants * * * are grievous and oppressive and ought not to be granted." Virginia Declaration of Rights § 10.

The Founding Fathers' concern about general warrants carried through to the drafting of the Bill of Rights. The Antifederalists condemned the Constitution for its failure to specify individual rights. Patrick Henry specifically condemned the

absence of protection against general warrants, stating

> I feel myself distressed because the necessity of securing our *personal rights* seems not to have pervaded the minds of men; for many other valuable things are omitted:--for instance, general warrants, by which an officer may search suspected places, without evidence of the commission of a fact, or seize any person without evidence of his crime, ought to be prohibited.

Donohue, *The Original Fourth Amendment*, at 1286. States, including New York, Rhode Island, and North Carolina, likewise insisted on the inclusion of protections against general warrants in the constitution. *Id*. at 1289-1292. The Antifederalists drew on the English general warrants cases, and particularly the case of John Wilkes, to argue for specific protections against general warrants. Schnapper, *Unreasonable Searches and Seizures of Papers*, at 914-915. In the Antifederalist Papers, Brutus pointed to the threat of general warrants as emblematic of the risks inherent in the absence of a Bill of Rights.

> For the security of liberty it has been declared, * * * that all warrants, without oath or affirmation, to search suspected places, or seize any person, his papers or property, are grievous and oppressive.

Brutus, New York Journal (November 1, 1787) (quotation omitted).

The Antifederalists' concerns about enshrining protections for individual liberty, and particularly for ensuring protection against unlimited search and seizure, culminated in the inclusion of the Bill of

Rights in the Constitution. Donohue, *The Original Fourth Amendment*, at *1297-1298. Not just decades of colonial experience, but centuries of British legal reckoning with the abuses of general warrants, led to the protections which the Fourth Amendment provides.

B. Geofence warrants are general warrants.

The Framers' deep aversion to general warrants was central to the adoption of the Fourth Amendment. As discussed, the principal evil of these warrants was the fact that they allowed government officials "blanket authority to search where they pleased" for incriminating information, without being limited to identified individuals, locations, or materials. *Stanford*, 379 U.S. at 481. By their very nature, geofence warrants allow the government to search unidentified individuals and trace their movements without any probable cause tying the subject of the search to a crime. So they are exactly the sort of general warrant the Fourth Amendment is designed to protect against.

Geofence warrants, which are a form of reverse location searching, have been in use since 2016. Matthew L. Brock, "If You Build It, They Will Come": *Reverse Location Searches, Data Collection, and the Fourth Amendment*, 57 U. Rich. L. Rev. 649, 652 (2023). These warrants allow law enforcement to use Location History data stored by third-party companies to identify electronic devices located within a particular geographic location within a particular time. *Ibid*. Google is the most common recipient of geofence warrants, largely because of the treasure trove of data from Android phone users (approximately 131.2 million Americans) as well as non-Android users who visit a Google-based apps or

websites such as Google Maps or Google Photos on their phone. *Geofence Warrants and the Fourth Amendment*, 134 Harv. L. Rev. 2508, 2512 (2021); *see also United States* v. *Chatrie*, 590 F. Supp. 3d 901, 908-1209 (E.D. Va. 2022), *aff'd*, 107 F.4th 319 (4th Cir. 2024), *on reh'g en banc*, 136 F.4th 100 (4th Cir. 2025), *and aff'd*, 136 F.4th 100 (4th Cir. 2025). Google's Sensorvault database contains the Location History data of all Google users that enable Google Location History services on their Google Accounts. A. Reed McLeod, *Geofence Warrants: Geolocating the Fourth Amendment*, 30 Wm. & Mary Bill Rts. J. 531, 534 (2021). As of 2018, that number was estimated at 592 million, or approximately one-third of all Google users. *United States* v. *Smith*, 110 F.4th 817, 823 (5th Cir. 2024), *cert. denied*, 146 S. Ct. 356 (2025); *see also Chatrie*, 590 F. Supp. 3d at 907 ("Google collects detailed location data on 'numerous tens of millions' of its users.").

To protect user privacy, Google has required law enforcement seeking user Location History data to obtain a warrant. The basis for seeking a geofence warrant typically relies on three premises: first, a criminal perpetrator was either seen with a cell phone or was assumed to have had one based on the near universality of cell phone ownership. McLeod, *Geofence Warrants*, at 533. Second, many cell phones either run on Android's operating system or interface with a Google Account. *Ibid.* Third, because of Google's market dominance, many phone users have a Google Account that enables Google location services. *Ibid.*

By 2018, Google developed a three-step process for law enforcement to receive requested data, which was generally followed by government agencies.

Brock, *If You Build It, They Will Come*, at 657. Police seeking judicial approval to search for user data had to identify some geographic search radius and time within which the search should be conducted. *Geofence Warrants and the Fourth Amendment*, at 2514. Once that approval was obtained, Google applied its "three-step anonymization and narrowing protocol." *Id*. at 2515. (alterations incorporated).[2]

In step one of this process, Google would search the entirety of Sensorvault for all devices identified within the parameters of the search. *Ibid.* Google would provide law enforcement with an anonymized list of the accounts, along with coordinates, timestamps, and source information. *Ibid.* This was an intrusive and resource-intensive process. *See Chatrie,* 590 F.Supp.3d at 908 ("to identify users within the relevant timeframe of a geofence, Google has to compare *all* the data in the Sensorvault. "); *see also* Brief of Google LLC as Amicus Curiae in Support of Neither Party, *United States* v. *Chatrie*, No. 3:19-cr-00130-MHL, 2019 WL 8227162, at *12-13 (E.D.Va. Dec. 20, 2019) ("In order to comply with the first step of the geofence protocol, .*.*.* Google must search across all LH journal entries to identify users with potentially responsive LH data, and then run a

[2] Google announced in December 2023 that it was transitioning Local History data to its users' local devices, rather than in the Sensorvault database and Google no longer uses the same three-step process. 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; Lars Daniel, *Google To Stop Giving Location Evidence To Law Enforcement*, Forbes (Oct. 08, 2024),

https://perma.cc/2ULX-2R4U.

computation against every set of coordinates to determine which LH records match the time and space parameters in the warrant.").

In step two, law enforcement would review the anonymized data to identify the devices it is interested in. *Ibid.* Law enforcement could request additional location information for certain devices at this stage to determine whether those devices were relevant to the investigation. *Ibid.* Though Google was not required to respond to this request unless the warrant explicitly includes it, Google often did so. *Ibid.* At this step, law enforcement could "compel Google to provide additional location coordinates *beyond* the time and geographic scope of the original request." *Chatrie*, 590 F. Supp. 3d at 916 (cleaned up). And while Google "typically require[d] law enforcement to narrow the number of users for which it requests Step 2 data," "Google ha[d] no firm policy as to precisely *when* a Step 2 request [was] sufficiently narrow." *Ibid.* Assuming Google did not object to the government's request, at this stage they would provide the government with "de-identified but geographically unrestricted data." *Ibid*.

In step three, law enforcement could "compel Google to provide *account-identifying information*," including names and email addresses for the individuals the government deems relevant to the investigation. *Ibid.* (cleaned up). While Google seems to have preferred the government narrow down its list of users from Step 2, there is no policy enforcing this preference. Brock, *If You Build It, They Will Come*, at 658-659. With the information procured at step three, law enforcement could pursue leads against identified individuals, including by securing warrants for more

intrusive investigative methods. *Smith*, 110 F.4th at 825.

Despite Google's attempts to limit government access to its users' information, this process does not pass constitutional muster. Geofence warrants do not identify the individuals whose device locations are to be searched, which means that everyone within the set geographical boundaries at the identified time is subject to having their movements traced by the government, regardless of whether there is any evidence tying them to a crime. Brock, *If You Build It, They Will Come*, at 652. In considering facts very similar to those at issue in *Chatrie*, the Fifth Circuit held that the process by which geofence warrants are executed necessarily involves searching through the personal information of individuals who are not suspected of any crime.

> When law enforcement submits a geofence warrant to Google, * * * law enforcement cannot obtain its requested location data unless Google searches through the entirety of its Sensorvault—all 592 million individual accounts—for all of their locations at a given point in time * * * Indeed, the quintessential problem with these warrants is that they never include a specific user to be identified, only a temporal and geographic location where any given user may turn up post-search. That is constitutionally insufficient.

Smith, 110 F.4th at 837. Nor did it matter that the government could tie the information sought to a particular time and place—"[w]hile the *results* of a geofence warrant may be narrowly tailored, the *search* itself is not." *Ibid.* This sort of unrestricted rummaging is "emblematic of general warrants and

[is] highly suspect per se." *Id*. at 838. (quotations omitted).

The Fifth Circuit traced this Court's precedent in *Carpenter* and *Jones* with respect to the "privacy interests inherent in location data," the dangers of "the government being able to comprehensively track a person's movement with relative ease due to the ubiquity of cell phone possession," and the limitations of the third-party doctrine. *Smith*, 110 F.4th at 832, 834-835. Based on this analysis, the Fifth Circuit concluded that the geofence warrant constituted a search. *Id*. at 836.

Having established that the examination of Location History data constituted a search, the Fifth Circuit then carefully analyzed geofence warrants as general warrants, recognizing that because these warrants "*never* include a specific user to be identified, only a temporal and geographic location where any given user *may* turn up post-search," they are "constitutionally insufficient." *Id*. at 837.

The Fifth Circuit's approach follows the understanding of general warrants that informed the Founders. Eighteenth century legal thinkers on both sides of the Atlantic rejected general warrants because they allowed law enforcement officers to rummage through the private lives of individuals without linking them to a crime. *See supra* at 3-10. In Blackstone's words, "it is the duty of the magistrate, and ought not be left to the officer, to judge of the ground of suspicion." Blackstone, *Commentaries* at 287. Yet geofence warrants place all assessment of the grounds of suspicion in the hands of law enforcement, since the warrant itself identifies no individual suspect. Indeed, that is the whole point of the warrant—to allow the government to review the

movements of a universe of private citizens to *identify* those who might become suspects. That process cannot be sufficiently particularized to pass constitutional muster.

The overbreadth of geofence warrants is compounded by the fact that law enforcement's rationale for obtaining these warrants has no limiting principal. As discussed *supra* at 11, law enforcement often applies for geofence warrants based on the likelihood that criminals carry cell phones, given their ubiquity in modern life. And this Court has recognized that cell phones have become "almost a feature of human anatomy." *Carpenter*, 585 U.S. at 311. (citation omitted). That argument discards even the pretense of particularity. If a warrant can be obtained to search the movements of everyone in a given area based on the likely fact that someone who was in that area probably has a cell phone, the government effectively has *carte blanche* to demand site-tracking information on anyone at any time. It would be as if an eighteenth-century judge had determined that since virtually everyone had a quill pen, the disseminators of seditious pamphlets likely also had quill pens, and therefore searching individuals based on quill pen ownership was justified. That logic would make a judge of the Star Chamber blush, yet its analogue continues to be employed in the modern day. The ubiquity of cell phones means government searches of unidentified cell-phone users should be treated with greater, not lesser, suspicion, to guard against wanton government intrusion into the private lives of citizens.

The Fifth Circuit's approach is also consistent with the principles this Court has established in other

cases about surveillance technology. In *Carpenter*, this Court recognized that an individual has a "reasonable expectation of privacy in the whole of his physical movements." 585 U.S. at 313. Surveillance devices, from GPS tracking to cell-site location information threaten that right by allowing the government to "generate[] a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *United States* v. *Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J. concurring). In both *Carpenter* and *Jones*, law enforcement surveillance targeted an identified individual who was suspected of a crime. But here, the intrusive power of government surveillance may be applied to any unfortunate person who happens to be in the wrong place at the wrong time carrying a cell phone. Such intrusion based on a general warrant is not only plainly unconstitutional, but a threat to the fundamental right to privacy.

II. This case offers the court an opportunity to clarify warrant requirements in high-tech searches.

A. If geofence warrants are not categorically unconstitutional, the Court should establish clear warrant requirements.

This Court recognized in *Carpenter* that the gathering of cell phone data "implicates privacy concerns" because it is "about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." 585 U.S. at 315. Yet the court's decision in *Carpenter* was "a narrow one," declining to review surveillance tools like real-time

cell-site location information and "tower dumps," or to "address other business records that might incidentally reveal location information." *Ibid*. at 316. As a result, lower courts have been left with limited guidance on the constitutionality of increasingly intrusive forms of surveillance technology. The result has been not only a split among the circuits on the constitutionality of geofence warrants, but a split between some state and federal courts. Compare *Smith*, 110 F.4th at 838 (finding that geofence warrants are "categorically prohibited by the Fourth Amendment.") *with Chatrie*, 136 F.4th 100, 100 (en banc)(per curiam) (affirming the lower court's denial of the motion to suppress a geofence warrant), and *Wells* v. *State*, 714 S.W.3d 614, 626 (Tex. Crim. App.), *reh'g denied*, 721 S.W.3d 260 (Tex. Crim. App. 2025) (finding that the geofence search warrant satisfied the Fourth Amendment's requirements). The resulting patchwork of rules has led to inconsistent protections for citizens' privacy rights depending on where they are located and what law enforcement body happens to be monitoring them.

Even if this Court finds that geofence warrants are not per se unconstitutional, the Court should establish clear requirements for these warrants. As geofence warrants become an increasingly prevalent part of government investigations, such requirements will be necessary to protect citizens' privacy rights. And given the sweeping amount of data that is collected in geofence searches, *see supra* at 10-11, it is vital that lower courts and law enforcement officials have guidance on constitutional requirements.

At a minimum, the Court should establish clear guidelines for meeting the standards of particularized

probable cause necessary to satisfy the Fourth Amendment in geofence warrant cases. This court has held that to support a finding of probable cause, "the belief of guilt must be particularized with respect to the person to be searched or seized." *Maryland* v. *Pringle*, 540 U.S. 366, 371 (2003). "[A] person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." *Ybarra* v. *Illinois*, 444 U.S. 85, 91 (1979).

This means that warrants that broadly sweep in the data of private citizens, even if they likely also include a suspect's data, cannot survive Fourth Amendment scrutiny. Some lower courts have addressed this issue by requiring that warrants be written to narrowly circumscribe the time and place in which data can be searched. *See Matter of Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 357 (N.D. Ill. 2020) (finding that a warrant adequately particularized where it was limited to a 15-30 minute time frame and where target locations were "narrowly crafted to ensure that location data, with a fair probability, will capture evidence of the crime only."); *Matter of Search of Info. that is Stored at Premises Controlled by Google LLC*, 579 F. Supp. 3d 62, 82 (D.D.C. 2021) (geofence warrant was adequately particularized where it was limited to 185 minutes of data spread out over a five-and-a-half month period and was limited in space to the front half of a building and its parking lot, since the "inquiry here is whether the target locations are drawn to capture location data from locations at or closely associated with the crime.") (cleaned up). By

establishing clear particularity requirements for geofence warrants, the Court will at least limit the ability of the state to gather the data of citizens who are not suspected of any crime.

The Court could further strengthen the protection for individual privacy by instantiating Google's three-step process and requiring that law enforcement secure judicial authorization at each step. Rather than grant law enforcement unbridled discretion to demand increasingly revealing user information, a three-step warrant process would ensure judicial oversight as law enforcement's searches become more intrusive. *See California* v. *Dawes*, No. 19002022 (Cal. Super. Ct., Cnty. of S. F., Sept. 30, 2022) (slip op., at 46-49) (finding that Google's "three-step process afforded law enforcement unbridled discretion, and at each step, law enforcement should have returned for additional judicial review and authorization."). Such a rule, though not foreclosing geofence warrants entirely, would at least ensure that individual privacy interests are overseen by a neutral magistrate at every step of the search process.

B. This case offers an opportunity to provide lower courts with guidance on a range of search tools that continue to present challenges after *Carpenter*.

The risks that high-tech surveillance poses to individual privacy are not limited to geofence searches. This Court has addressed the privacy concerns arising from law enforcement use of location data in both *Jones* and *Carpenter*. In *Jones*, the Court held that the physical attachment of a GPS monitoring device to a vehicle constituted a search under the Fourth Amendment. *Jones*, 565 U.S. at 404.

In *Carpenter*, the Court held that seven days' worth of data monitoring an individual's movements via cell-site location information was a search and was not subject to the third-party doctrine. *Carpenter*, 585 U.S. at 315-316.

Still, the Court's decisions in those cases left open many questions about their broader applications. *See Jones*, 565 U.S. at 424-425 (Alito, J. concurring) (observing that "if long-term monitoring can be accomplished without committing a technical trespass * * * the Court's theory would provide no protection."). In *Carpenter*, the Court stated that its "decision today is a narrow one. We do not express a view on matters not before us." 585 U.S. at 316. With such narrow rulings, lower courts are still facing increasingly difficult questions about how to define technological intrusion into Fourth Amendment protections.

One example of these technological challenges is cell-site simulators. Cell-site simulators work by "superseding the signal emitted from a service provider's cell site within an area, causing all mobile devices to register with it instead of the cell site." Jeremy H. D'Amico, *Cellphones, Stingrays and Searches! An Inquiry Into the Legality of Cellular Location Info.*, 70 U. Miami L. Rev. 1252, 1296 (2016). Because law enforcement generates the data, which can be gathered indiscriminately, some scholars argue that the use of cell-site simulators "raises the specter of an illegal general warrant." Susan Freiwald & Stephen Wm. Smith, *The Carpenter Chronicle: A Near-Perfect Surveillance*, 132 Harv. L. Rev. 205, 229 (2018); but *see United States* v. *Patrick*, 842 F.3d 540, 545 (7th Cir. 2016) (upholding the use of cell-site simulator data to execute a location warrant,

reasoning that "[a] person wanted on probable cause (and an arrest warrant) who is taken into custody in a public place, where he had no legitimate expectation of privacy, cannot complain about how the police learned his location.").

Similar issues are raised by cell tower dumps, in which law enforcement obtains an order "compelling providers to release historical cell site data for a specific tower or towers providing service to a crime scene." Freiwald & Smith, *The Carpenter Chronicle*, at 229. Because the police gather data from all cell phones within a given geographical area, this technology also "raises general warrant concerns that were not present in *Carpenter*." *Ibid.* Lower courts are divided on the degree of constitutional protection afforded historical cell site data. *Compare, e.g., In re Cell Tower Recs. Under 18 U.S.C. § 2703(D),* 90 F. Supp. 3d 673, 675 (S.D. Tex. 2015) ("cell tower logs requested here would likewise be categorized as ordinary business records entitled to no constitutional protection.") *and United States* v. *Scott*, No. 14-20780, 2015 WL 4644963, at *7 (E.D. Mich. Aug. 5, 2015)(defendant "did not have a reasonable expectation of privacy in the data that revealed the general historical location of his cell phone for, at most, a ninety-minute period on a single morning.") *with In re Application of U.S. for an Ord. Pursuant to 18 USC § 2703(D)*, 964 F. Supp. 2d 674, 677 (S.D. Tex. 2013) (holding that "cell site data are protected pursuant to the Fourth Amendment from warrantless searches.")

As surveillance technology continues to develop, lower courts will be forced to define the limits of Fourth Amendment protection. In the absence of guidance, this is likely to result in inconsistent

protections for individual rights to privacy throughout the nation. That is already the case for geofence warrants, as the circuit split and federal-state divide on this question have made clear. The Court can take the opportunity presented here to provide lower courts with valuable guidance on how to treat the fast-developing field of surveillance technology consistent with the protections of the Fourth Amendment. Such an approach would not only instruct the lower courts but would also reassure American citizens of the robustness of their constitutional protections.

Conclusion

The Court should reverse the judgment of the Fourth Circuit en banc panel.

Respectfully submitted.

JOHN W. WHITEHEAD
WILLIAM E. WINTERS
The Rutherford Institute
109 Deerwood Road
Charlottesville, VA 22911

ETHAN H. TOWNSEND
Counsel of Record
MAURA R. CREMIN
McDermott Will & Emery LLP
500 North Capitol Street NW
Washington, DC 20001
(202) 756-8000
ehtownsend@mwe.com

Counsel for Amicus Curiae