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 OF *AMICI CURIAE* THE LOCAL GOVERNMENT LEGAL CENTER IN SUPPORT OF RESPONDENT

Thomas R. McCarthy
Counsel of Record
Tiffany H. Bates
ANTONIN SCALIA LAW SCHOOL
SUPREME COURT CLINIC
CONSOVOY MCCARTHY PLLC
1600 Wilson Boulevard
Suite 700
Arlington, VA 22209
(703) 243-9423
tom@consovoymccarthy.com

Counsel for Amici Curiae

April 1, 2026

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTEREST OF *AMICI CURIAE*[1]

The Local Government Legal Center (LGLC) is a coalition of government organizations formed in 2023 to provide education to local governments regarding the Supreme Court and its impact on local governments and officials and to advocate for local government positions at the Supreme Court in appropriate cases. The National Association of Counties, the National League of Cities, and the International Municipal Lawyers Association are the founding members of the LGLC. The International City/County Management Association is an associate member of the LGLC.

The National Association of Counties (NACo) is the only national organization that represents county governments in the United States. Founded in 1935, NACo provides essential services to the nation's 3,069 counties through advocacy, education, and research.

The National League of Cities (NLC), founded in 1924, is the oldest and largest organization representing U.S. municipal governments. NLC works to strengthen local leadership, influence federal policy, and drive innovative solutions. In partnership with 49 state municipal leagues, NLC advocates for over 19,000 cities, towns, and villages where more than 218 million Americans live.

The International Municipal Lawyers Association (IMLA) is a non-profit professional organization of

---

[1] Pursuant to this Court's Rule 37.6, counsel for *amici curiae* certify that this brief was not authored in whole or in part by counsel for any party and that no person or entity other than *amici curiae* or its counsel has made a monetary contribution to the preparation or submission of this brief.

more than 2,500 local government attorneys. Since 1935, IMLA has served as a national, and now international, resource for legal information and cooperation on municipal legal matters. Its mission is to advance the development of just and effective municipal law and to advocate for the legal interests of local governments. It does so in part through filing amicus briefs before the U.S. Supreme Court, the U.S. Courts of Appeals, and state supreme and appellate courts.

The International City/County Management Association (ICMA) is a nonprofit professional and educational organization of more than 9,000 appointed chief executives and assistants serving cities, counties, towns, and regional entities. ICMA's mission is to create excellence in local governance by advocating and developing the professional management of local governments throughout the world.

Amici have a strong interest in the outcome of this case because it will determine whether or when law enforcement can use geofence warrants—an important tool used to solve crime.

INTRODUCTION AND SUMMARY OF THE ARGUMENT

A geofence is a virtual perimeter around a small geographic location during a specified time frame. *See* Brian L. Owsley, *The Best Offense is a Good Defense: Fourth Amendment Implications of Geofence Warrants*, 50 Hofstra L. Rev. 829, 832-33 (2022). Companies often use geofencing to facilitate targeted advertising by identifying smartphone users by their device IDs within a circumscribed location for a short period of time. *See id.* at 832. In recent years, law enforcement has begun using geofencing as an investigative tool, typically employed when law enforcement "knows the approximate time and location of a crime but not the identities of suspects." Peter G. Berris & Clay Wild, Cong. Rsch. Serv., LSB11274, *Geofence Warrants and the Fourth Amendment*, 1 (Jan. 22, 2026).

Indeed, geofence warrants have become an important investigative tool that law enforcement uses to solve crime. As the United States explains, a geofence warrant "helps officers to identify unknown suspects and witnesses of a crime using cellphone location information stored by a third-party company, such as Google." *See* Br. in Opp'n at 3. Law enforcement officers can use the anonymized data produced via a geofence warrant to narrow the list of potential suspects. A geofence warrant thus offers a "brief glimpse" into an individual's "whereabouts," and when properly executed, is unlikely to "offer insight into his habits, routines, and associations." Pet. App. 178a.

While geofence warrants themselves are a new phenomenon, they follow the same tried-and-true process as any other warrant. There is an affidavit of

probable cause, particularized to a discrete geographic area and time window. A detached, neutral magistrate independently reviews the warrant for sufficient probable cause before police collect any information. A back-and-forth process between Google and police then ensues, where information is gradually narrowed before being de-anonymized. The end product is information connecting a particular user or users—who opted into Google's location services—to a particular place on a particular occasion.

This process allows law enforcement to obtain evidence when traditional methods come up empty. The use of this technology also enhances the quality of evidence and reduces the potential for errors that may accompany other forms of evidence such as eye-witness testimony. And it has been used to help solve cold cases and otherwise unsolvable crimes.

Petitioner Okello Chatrie—who robbed a credit union at gun point and was identified through law enforcement's use of a geofence warrant—asks for a categorical rule eliminating the use of geofence warrants as a violation of the Fourth Amendment. Such a rule is unwarranted and would depart from this Court's case-by-case analysis attentive to the particular facts and circumstances of each search. And it would undermine the use of other important investigative tools that are rapidly evolving with new technology. Moreover, Congress is better suited to weighing the broader privacy and policy concerns raised by developing technologies like geofencing to determine whether to impose additional privacy protections on geofence warrants.

Importantly, rejecting a categorical rule in this case would not mean that geofence warrants can never be challenged. It would mean only that law enforcement may employ geofence warrants with appropriate safeguards. Here, Chatrie had consented to Google storing his location history data by opting-in to that feature. So the law enforcement officers that identified Chatrie's device ID via a geofence warrant only obtained information that Chatrie had agreed to share with a third-party (i.e., Google). And the warrant used to obtain his identity satisfied the Fourth Amendment's particularity and probable cause requirements.

The Court should affirm.

ARGUMENT

I. Geofence warrants are an important law enforcement tool used to solve crime.

Geofence warrants are an important investigative tool for law enforcement. To obtain a geofence warrant, law enforcement completes a three-step process that ultimately narrows down information about a suspect at a specific place and during a specific time. This technology has allowed law enforcement to solve crimes that would otherwise go unsolved.

A. Executing a geofence warrant is a three-step process that helps law enforcement reliably identify criminals.

Geofence warrants begin like ordinary warrants: with a judge, an affidavit, and a defined place and time. Before any data is collected, law enforcement must apply for and obtain a warrant from a neutral and detached magistrate. The officer submits an affidavit demonstrating probable cause that evidence of a

crime will be found within a defined geographic area and window of time. The magistrate independently evaluates the application and issues the warrant only if he is satisfied that the Fourth Amendment's requirements are met. No data leaves Google's servers[2] without judicial authorization. *See* Berris & Wild, *supra*, at 3.

From there, executing a geofence warrant is a three-step process.

Step One: The Anonymized Initial Request. At this step, Google searches its records and returns only anonymized device identifiers—alphanumeric codes stripped of any personally identifying information—for devices whose location-history data places them within the geofence during the specified window of time. Pet. App. 8a. At this stage, officers see nothing more than a set of anonymous codes and general location coordinates. *See id.* at 6a. No names. No subscriber information. No identifying data whatsoever. Just anonymized dots on a map. *See* Off. of the Bergen Cnty. Prosecutor, *Procedures for Requesting Geofence Warrants* (June 22, 2022), perma.cc/Y7LH-39CQ.

Step Two: Investigative Narrowing. Next, investigators review the anonymized data to determine which devices exhibit behavior consistent with the criminal activity under investigation. For example, if a robbery suspect appears on surveillance cameras fleeing in a specific direction or waiting at a specific corner before the crime, investigators look for anonymized devices that mirror those precise movements. In

---

[2] Until at least 2023, Google was (and may still be) the "primary recipient" of geofence warrants. Berris & Wild, *supra*, at 3.

many cases, law enforcement may request separate anonymized location points to limit the scope of data disclosed, ensuring that only the most relevant device data advances to further scrutiny. *See id.*

Step Three: De-Anonymizing the Narrowed Results. Only after narrowing the device list do investigators request any account-identifying information for the small subset of devices that appear relevant. Pet. App. 290a-291a. The process is incremental by design: warrant first, anonymized production second, narrowing third, and actual suspect names last.

In this case, Detective Hylton sought a geofence warrant after an armed robbery at the Call Federal Credit Union in Midlothian, Virginia. His affidavit identified a specific location, a one-hour period surrounding the robbery, and the reason to believe digital location evidence could matter—the robber appeared to be using a cellphone immediately before the crime. Pet. App. 293a-297a. After narrowing down the nineteen accounts that had been in the 150-meter radius during the hour of the robbery, Google ultimately deanonymized three accounts. Pet. App. 79a. One of those accounts belonged to Petitioner Okello Chatrie, who ultimately entered a conditional guilty plea for armed robbery and for brandishing a firearm during a crime of violence. Pet. App. 79a-80a.

This process began with judicial authorization tied to a time, a place, and a crime. It moved from broad anonymity to targeted identification—the opposite of a dragnet—and reflected a deliberate effort to minimize any intrusion on individual privacy. This process served as a digital analogue to the kind of progressive narrowing that law enforcement has long employed in

the physical world—canvassing a neighborhood, interviewing witnesses, and gradually focusing on particular individuals. But a geofence warrant produces more reliable evidence than an eyewitness canvass, with less room for the cognitive biases that plague human identification. Indeed, the use of geofenced location data provides objective, timestamped evidence of a device's physical presence at a particular location—unlike eyewitness testimony, which this Court has recognized as "frequent[ly] untrustworth[y]." *Manson v. Brathwaite*, 432 U.S. 98, 119-120 (1977) (Marshall, J., dissenting). The information gained from geofence warrants reduces the risk of wrongful accusations based on faulty human memory or suggestive identification procedures.

B. Geofence warrants help solve crimes that would otherwise go unsolved.

Geofence warrants are not a tool of first resort. They are used to gather evidence when traditional methods come up empty. "Think of a murder where the culprit leaves behind his encrypted phone and nothing else. No fingerprints, no witnesses, no murder weapon. But because the killer allowed Google to track his location, a geofence warrant can crack the case." Pet. App. 25a (Wilkinson, J., concurring). Geofence warrants fill a gap that no other technique to date can.

Sometimes called a "warrant of last resort," geofence warrants have allowed law enforcement to solve otherwise unsolvable crimes. Maverick Data Sys., *Geofence Warrants*, Warrant Builder (2023), perma.cc/C4SU-B6JN. The use of this technology enhances the quality of evidence and thus reduces the

potential for errors that may accompany other forms of evidence. *See supra*, at I.A.

Amici highlight only a few examples:

1. In November 2018, police found Mitchell Jones Jr. dead from a stab wound in his bedroom in Cobb County, Georgia. Despite a 911 call from the victim, the case went cold for months. In March 2019, detectives executed a geofence warrant targeting Google's location data. The data identified a device belonging to Dunte Lamont Holmes at the crime scene during the exact window of the murder. Further investigation revealed that Holmes had also stolen the victim's phone. This digital lead allowed police to match Holmes' DNA to blood found at the scene, resulting in a life sentence for a ruthless killer who would have otherwise escaped justice. *See* Kristal Dixon, *Cops Use Google Location Data to Solve Fatal Cobb Stabbing*, Atl. J. Const. (Jan. 6, 2020), perma.cc/XAX9-BUF8.

2. In March 2019, Abdalla Thabet was murdered during an ambush at a bank in Paramount, California. Surveillance video captured the perpetrators' gray and red sedans, but the license plates were illegible. Los Angeles County Sheriff's investigators used a geofence warrant targeting six locations Thabet had visited that morning. Google identified devices that appeared at several of these locations—a digital tail that led directly to Daniel Meza and Walter Meneses. The men pleaded guilty and no contest, respectively, and were sentenced to state prison terms. *See People v. Meza*, 312 Cal. Rptr. 3d 1, 7-8 (Cal. Ct. App. 2023).

3. In rural California, Pamela Morehouse was killed in a hit-and-run in the summer of 2018. A California Highway Patrol Officer reported there "was a

complete lack of evidence" and the case went cold for several years. Finally, officers sought a geofence warrant asking Google for devices crossing the intersection at the time of the accident. That process identified Jason Bryan Wilson, who had previously "lied to investigators" and "actively obscured his trail." Christopher Damien & Nick Penzenstadler, *Cold Cases Cracked By Cellphones: How Police Are Using Geofence Warrants to Solve Crimes*, USA Today (Sep. 12, 2022), perma.cc/3UX8-TFHG. "Without the geofence," officers stated, "this would have remained a cold case." *Id.*

4. The 2017 murder of Egypt Covington, a 27-year-old singer found bound and shot in her home, remained a total mystery for three years. Local township police failed to make an arrest until Michigan State Police obtained geofence data that local police had acquired but failed to investigate. Using the geofence data, State Police identified three men who had entered Covington's home while attempting to rob a neighbor. One investigator noted that the geofence data "was the first piece of evidence that really broke the case wide open." Three defendants ultimately pleaded guilty to second-degree murder. Sara Powers, *Three Suspects in Egypt Covington Murder Have Pleaded Guilty*, CBS News (July 21, 2023), perma.cc/R3YE-K77T; Tim Stelloh, *Cellphone Data Helped Solve a Michigan Singer's Murder, But Experts Say the Tool Will Soon Be Off-Limits*, NBC News (Mar. 22, 2024), perma.cc/69G7-DMQ9.

In each of these serious crimes, traditional investigative methods failed while a targeted, warrant-based digital tool succeeded. Without this tool, none of these violent crimes would have been solved.

II. Geofence warrants do not violate the Fourth Amendment in circumstances like those presented here.

While Chatrie asks for a brightline rule holding that geofence warrants violate that Fourth Amendment, such a categorical rule is out of step with the Court's Fourth Amendment jurisprudence. Moreover, a categorical rule eliminating geofence warrants would undermine the use of other important investigative tools. Courts could still sustain challenges to geofence warrants on an individualized basis. But geofence warrants should be permitted where adequate safeguards are employed. Here, for example, Chatrie consented to Google storing his location history and the warrant used to obtain his identity satisfied the Fourth Amendment's particularity and probable cause requirements.

A. A categorical bar on geofence warrants would be inconsistent with the Court's Fourth Amendment precedent.

This Court has consistently "eschewed bright-line" or categorical rules to resolve Fourth Amendment questions, preferring instead a case-by-case analysis attentive to the "endless variations in the facts and circumstances" of each search. *Ohio v. Robinette*, 519 U.S. 33, 39 (1996). The Fourth Amendment's "reasonableness" standard "is not capable of precise definition or mechanical application," *Bell v. Wolfish*, 441 U.S. 520, 559 (1979), and the Court has repeatedly warned against categorical pronouncements in the technology context. In *City of Ontario v. Quon*, the Court cautioned that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of

emerging technology before its role in society has become clear." 560 U.S. 746, 759 (2010).

Carpenter v. United States, 585 U.S. 296 (2018), reinforced this incremental approach. There, the Court expressly declined to grant the state a time-limited right to search a person's physical location and limited its holding to the facts before it: "We do not express a view on matters not before us," including "conventional surveillance techniques and tools, such as security cameras," or "other collection techniques involving foreign affairs or national security." *Id.* at 316. A categorical rule declaring all geofence warrants unconstitutional is the kind of sweeping pronouncement that the Court eschewed in *Quon* and *Carpenter*.

Chatrie asks this Court to do what it refused to do in those cases: announce a blanket Fourth Amendment rule on an entire category of warrant-based investigative techniques. But the Fourth Amendment has never operated that way. Whether a particular search is reasonable depends on the "totality-of-the-circumstances"—including the scope of the warrant, the particularity of its terms, and the nature of the intrusion. *See Illinois v. Gates*, 462 U.S. 213, 238 (1983); *Zurcher v. Stanford Daily*, 436 U.S. 547, 566 (1978).

State courts confronting geofence warrants have declined to adopt a blanket rule. For example, in *Wells v. State*, 714 S.W.3d 614 (Tex. Crim. App. 2025), *reh'g denied,* 721 S.W.3d 260 (Tex. Crim. App. 2025), the Texas Court of Criminal Appeals upheld a geofence warrant in a murder investigation and stressed the relevance of tight geographic and temporal tailoring. 714 S.W.3d at 625-26. The Georgia Supreme Court reached the same conclusion in *Jones v. State*, 913

S.E.2d 700 (Ga. 2025), upholding a geofence warrant that specified a 100-meter radius around the crime scene during a four-hour window. *See id.* at 703. The court found the warrant provided "specific guidance" on the information to be accessed and avoided "unfettered discretion." *Id.* And in *State v. Contreras-Sanchez*, 5 N.W.3d 151 (Minn. Ct. App. 2024), *review granted* (Minn. May 29, 2024), the court rejected a categorical challenge and upheld the warrant under ordinary probable-cause and particularity principles. 5 N.W.3d at 171.

Those decisions do not declare that every geofence warrant is valid. Rather, they establish the narrower proposition that a blanket prohibition is inappropriate. The Fifth Circuit's contrary opinion in *United States v. Smith*, 110 F.4th 817 (5th Cir. 2024), shows only that the issue is difficult, not that the categorical approach is correct. *Smith* held that geofence warrants are general warrants in every case because Google must search a large data repository at Step One. 110 F.4th at 837-38. But that reasoning treats every warrant the same, no matter how narrow. This Court should not import that rigid rule into a rapidly changing field that presents materially different facts from case to case.

B. Eliminating geofence warrants would undermine the use of other investigative tools.

This Court has repeatedly recognized that courts should tread carefully when rapidly evolving technology is at issue. In *Quon*, the Court warned that "[t]he judiciary risks error by elaborating too fully on the

Fourth Amendment implications of emerging technology before its role in society has become clear." 560 U.S. at 759. That warning has only grown more urgent. Digital investigative tools are evolving at a pace that outstrips the capacity of constitutional adjudication to keep up. A categorical rule adopted today risks becoming an ill-fitting straitjacket tomorrow.

This principle can be seen throughout the Court's jurisprudence. In *United States v. Jones*, 565 U.S. 400 (2012), the Court resolved a GPS tracking case on narrow, trespass-based grounds—deliberately declining to reach broader questions about electronic surveillance. *See id.* at 404-05. Five Justices wrote separately to flag the privacy implications of long-term location monitoring, but the majority refused to announce a sweeping rule. *See id.* at 415 (Sotomayor, J., concurring); *id.* at 424-25 (Alito, J., concurring in the judgment) (joined by Ginsburg, J., Breyer, J., and Kagan, J.).

Two years later, in *Riley v. California*, 573 U.S. 373 (2014), the Court required warrants for cell phone searches incident to arrest. *Id.* at 403. In doing so, the Court confined the holding to that context, leaving open how the Fourth Amendment applies to other forms of digital data access. *See id.* (addressing only cell phone data searched incident to arrest). And in *Carpenter*, the Court was explicit: it declined to "express a view on matters not before us," including "conventional surveillance techniques and tools, such as security cameras," "real-time CSLI," and "other collection techniques involving foreign affairs or national security." 585 U.S. at 316. Each case addressed the

technology before it; none attempted to constitutionalize a rule for the next generation of tools.

This case-by-case approach permits courts to distinguish between a geofence warrant covering a 150-meter radius for one hour—as here—and one covering an entire city for a week. It permits courts to account for the voluntariness of the data disclosure, the sensitivity of the location, and the seriousness of the crime under investigation. It allows legislatures, which possess greater institutional capacity to gather technical information and balance competing interests, to enact statutory frameworks tailored to specific technologies. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 805 (2004) ("[C]ourts should place a thumb on the scale in favor of judicial caution when technology is in flux.).

A case-by-case framework protects against the very abuse that Chatrie fears. It does not immunize geofence warrants from scrutiny. It subjects each warrant to individualized review for probable cause, particularity, and reasonableness—the same standards that govern every other warrant. What it does not do is condemn an entire investigative technique before the technology, the case law, and the legislative landscape have had time to settle. That restraint is not weakness; it is a hallmark of sound Fourth Amendment adjudication.

C. Other adequate safeguards exist for policing geofence warrants.

Chatrie and his *amici* conjure visions of geofence warrants deployed to identify churchgoers, attendees at political rallies, or visitors to sensitive locations.

Those concerns are not presented by this case, and existing constitutional protections provide ample safeguards against such abuses.

An individual can challenge any warrant as overly broad in scope. *See Groh v. Ramirez*, 540 U.S. 551, 563 (2004). A geofence warrant directed at a political rally or a house of worship would face immediate First Amendment scrutiny and would be subject to challenge as lacking probable cause or exceeding the bounds of reasonableness. The existing case-by-case framework is more than adequate to police those boundaries.

The three-step process itself serves as an additional safeguard. Because identifying information is not disclosed until step three—after law enforcement has progressively narrowed the pool of relevant accounts through two prior rounds of anonymized review—the risk that innocent individuals will be identified is substantially mitigated. Here, the process narrowed nineteen anonymous device numbers to three identified accounts. That is not a dragnet.

D. Chatrie consented to Google storing his location history as business records.

The principle that individuals generally cannot invoke a right against a search of another's property has long stood in the backdrop of the Fourth Amendment. *See Smith v. Maryland*, 442 U.S. 735, 743-44 (1979); *United States v. Miller*, 425 U.S. 435, 443 (1976). The third-party doctrine rests on the straightforward proposition that when a person voluntarily conveys information to a third party, he assumes the risk that the third party will share it with the government. *Smith*, 442 U.S. at 744.

Chatrie invokes *Carpenter* to argue that the third-party doctrine does not apply here. But by its own terms *Carpenter* was "narrow" and the "rare case" involving a "legitimate privacy interest in records held by a third party." 585 U.S. at 316, 319. In *Carpenter,* the United States did not ask for a "straightforward application of the third-party doctrine." *Id.* at 314. Instead, it sought its "significant extension" to a "distinct category of information." *Id.* And it was this "exten[sion of] *Smith* and *Miller* to cover [Carpenter's] novel circumstances" that this Court rejected—not the doctrine itself. *Id.* at 309. Put simply, the Court did not overrule *Smith* or *Miller*. It declined only to "extend[] *Smith* and *Miller* to cover [those] novel circumstances." *Id.*

The critical distinction here is that location history is opt-in and "off by default." Pet. App. 273a. A user must take several affirmative steps to enable it. *Id.* This is fundamentally different from the cell-site location information at issue in *Carpenter*, which was generated automatically whenever a phone was powered on, with no user choice. *Carpenter*, 585 U.S. at 315. The *Carpenter* majority was troubled by data collection that occurred as "the inescapable and automatic nature of" capturing one's location when using a phone. *Id.* at 320. Location history presents no such concern. Users can "participat[e] in modern society"—make calls, send texts, use apps—without enabling it. *Id.* at 315.

Some characterize location history as an inescapable feature, but that characterization doesn't withstand scrutiny. Google's location history is an optional service, not a byproduct of cellular connectivity. A user

who enables it makes a voluntary choice to allow Google to store his location data in exchange for services like traffic updates, personalized recommendations, and location-based reminders. *See* Pet. App. 168a, 270a-271a. That is a paradigmatic third-party disclosure.

As Justice Alito has explained, the general evil that the Fourth Amendment targeted was "the *means*" by which the government would acquire evidence—not "acquir[ing] evidence" itself. *Carpenter*, 585 U.S. at 369-71 (Alito, J., dissenting). Subpoenas directed to third parties, including subpoenas for business records, have a long historical pedigree and do not implicate the same concerns that animated the Fourth Amendment. *See id.* at 370-71. Here, the government obtained a judicial warrant—a more protective procedure than a subpoena—directed at business records that Chatrie voluntarily chose to create by enabling an optional service.

E. This warrant satisfied the Fourth Amendment's particularity and probable cause requirements.

The Fourth Amendment requires that a warrant "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The warrant at issue did so here. It specified a 150-meter radius around a defined set of coordinates—the Call Federal Credit Union—and a one-hour time window from 4:20 to 5:20 p.m. on May 20, 2019. Pet. App. 294a-295a; J.A.136-37.

This is like a premises warrant. When police obtain a warrant to search a house for evidence of drug

trafficking, the warrant describes the physical premises and authorizes officers to search the house—including rooms and belongings of occupants not suspected of criminal wrongdoing—for the specified evidence. *See Zurcher*, 436 U.S. at 555-56. The warrant need not identify every person inside the house, and the fact that innocent occupants' belongings may be examined in the course of executing the warrant does not render it a general warrant. *See id.*

The same logic applies here. The warrant identified a digital premises—a defined geographic area during a defined time period—and authorized a search for evidence (i.e., location data) within that premise. The fact that Google must examine its database to identify which accounts contain responsive data is no different from officers examining rooms in a house to locate the evidence described in the warrant. As the government explained in its brief in opposition in *Smith*, "the Fourth Amendment's particularity requirement focuses on the information the government *itself* gets to view or employ in its investigation, not the information exposed to private actors that is never shown to the government." Br. in Opp'n at 12 (quoting Br. in Opp'n at 12, *Smith*, No. 24-7237); *see Steagald v. United States*, 451 U.S. 204, 220 (1981).

Next, probable cause requires a "fair probability that contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238. Detective Hylton's affidavit established that (1) an armed robbery occurred at the Call Federal Credit Union on May 20, 2019; (2) surveillance footage showed the robber using a cellphone immediately before the robbery; (3) most cellphones are smartphones; and (4) Google

could track such phones through location history. Pet. App. 292a, 296a-297a; J.A. 112-113.

These facts established a fair probability that location history data would contain evidence identifying the robber—i.e., a device in the geofence at the time of the crime that could be linked to the suspect. The probable cause standard does not require certainty; it requires a "practical, nontechnical" assessment of probabilities by a common-sense magistrate. *Gates*, 462 U.S. at 231, 238. A Virginia magistrate found probable cause here. Pet. App. 294a. That determination was sound.

An officer seeking a warrant to search a house need not establish probable cause that every resident is suspected of criminal activity—only that evidence of a crime will likely be found at the premises. The same logic applies here. The warrant established probable cause that evidence of the robbery would be found within the defined geographic area and time window. That some accounts captured within the geofence would belong to innocent bystanders does not defeat probable cause any more than the presence of innocent family members in a home defeats a warrant to search that home for contraband. *See Zurcher,* 436 U.S. at 555-56.

III. Congress is best suited to handle privacy concerns created from consensual disclosures to third parties for the use of evolving technologies.

The use of geofence warrants and other rapidly evolving technology raises privacy concerns that Congress is best suited to handle. Congress—not the courts—is the appropriate body to weigh these privacy

concerns and "add additional statutory privacy protections." Berris & Wild, *supra*, at 6.

To start, Congress can adopt rules more responsive to technological changes and can provide more "detailed guidance" than the courts. *Carpenter*, 585 U.S. at 402 (Gorsuch, J., dissenting). Congress's "statutory rules governing" the powers law enforcement may use "will tend to be more sophisticated, comprehensive, forward-thinking, and flexible" than judicial precedent. Kerr, *supra*, at 859-60. And Congress "can react quickly if [its] initial efforts do not work out" or if "technology develops in a different way than anticipated." Jeffery S. Sutton, *Courts, Rights, and New Technology: Judging in an Ever-Changing World*, 8 N.Y.U. J. L. & Liberty 261, 275 (2014). That's critical "[w]hen technologies are new and their impact remains uncertain." Kerr, *supra*, at 859. And it's equally critical when such decisions "call[] for a pure policy choice … between the value of privacy in a particular setting and society's interest in combatting crime." *Carpenter*, 585 U.S. at 393 (Gorsuch, J., dissenting). Indeed, Congress has the "institutional resources designed to help [it] discern and enact majoritarian preferences." *Id.* at 392.

Courts are ill-suited for that task. "[C]onventional legal sources, like history and precedent, do not answer many of the novel questions posed at the forefront of technological changes." *See* Sutton, *supra*, at 270. And due to the ex-post nature of judgments and timing of litigation, precedential rules "tend to lag behind parallel statutory rules and current technologies by at least a decade." Kerr, *supra*, at 868. This creates "unsettled and then outdated rules that often make

little sense given current technological facts." *Id.* Uncertainty, then, can "either allow abuses or else chill practices needed to pursue important investigations." *Id.* at 859. And since courts are inherently bound by past rules, they can create a moving target in this space. "Rule too narrowly, and your fact-bound precedent will be of little value to anyone. Rule too broadly, and your decision, seemingly wise today, may make little sense tomorrow." Sutton, *supra*, at 270-71.

Congress can "add additional statutory privacy protections" for data like location information. Berris & Wild, *supra*, at 6. The Stored Communications Act, for example, "restricts when certain information may be disclosed by electronic communication services or remote computing services, which in practice typically include entities such as 'cell phone providers, email providers, or social media platforms' and cloud computing providers." *Id.* Under that law, "the government may compel such providers to share communications' content and metadata if it obtains the requisite level of legal process, which ranges from a subpoena to a warrant depending on the category of information sought." *Id.* As the Congressional Research Service has explained, Congress could amend that law to "establish protections for Location History information." *Id.*

Congress knows how to regulate within this space. Indeed, it has already regulated certain investigative tools and processes. *Amici* highlight a few examples:

1. Federal law proscribes when a provider of electronic communication may assist in a FISA investigation; prohibits the use of unlawfully intercepted com-

munications in any legal proceeding; mandates a procedure for legally intercepting a wire, oral, or electronic communication; requires agencies installing a pen register or trap-and-trace device to use technology that reasonably restricts the information obtained; and limits the use of pen registers to sixty days. *See generally* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2511(2)(a)(ii), 2515, 2518, 3121, 3123); Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197.

2. Responding to public outcry of privacy concerns, Congress has "effectively ended the NSA's bulk telephony metadata collection program." *United States v. Moalin*, 973 F.3d 977, 989, 992 (9th Cir. 2020) (citing the USA FREEDOM Act, Pub. L. No. 114-23, 129 Stat. 268 (2015) (codified 50 U.S.C. § 1861)); Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978). Congress also enacted reporting requirements for the FISA orders, employing their institutional advantage over information gathering. *See* 50 U.S.C. §§1863, 1871, 1873.

3. In the Tax Reform Act of 1976, Congress sought to "protect the civil rights, including the privacy rights, of taxpayers subjected to the IRS's aggressive use of third-party summonses." *United States v. Gertner*, 65 F.3d 963, 971 (1st Cir. 1995); *see* Pub. L. No. 94-455, 90 Stat. 1520, 1701 (codified 26 U.S.C. § 7609(f)). It mandated procedures to prevent the IRS from casting its lines out for "'fishing expeditions' that 'might unnecessarily trample upon taxpayer privacy.'" *Tiffany Fine Arts, Inc. v. United States*, 469 U.S. 310, 320 (1985) (citing S. Rep. No. 94-938, at 373 (1976); H.R. Rep. No. 94-658, at 311 (1975)).

While not exhaustive, these examples illustrate what the separation of powers confirms: Congress has an important role to play here. That role is shaped by Congress's institutional strengths. *See* Sutton, *supra*, at 276 (explaining that "the legislature … was thought of as the *primary* guardian of liberty" throughout most of the Nation's history). And it is amplified in the context of rapidly evolving technology.

CONCLUSION

For these reasons, the Court should affirm the decision below.

Respectfully submitted,

Thomas R. McCarthy
Counsel of Record
Tiffany H. Bates
ANTONIN SCALIA LAW SCHOOL
SUPREME COURT CLINIC
CONSOVOY MCCARTHY PLLC
1600 Wilson Boulevard
Suite 700
Arlington, VA 22209
(703) 243-9423
tom@consovoymccarthy.com

Counsel for Amici Curiae

April 1, 2026