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 MICROSOFT CORPORATION AS AMICUS CURIAE IN SUPPORT OF NEITHER PARTY

ADELA LILOLLARI
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109

ARI HOLTZBLATT
Counsel of Record
MICHAEL BAER
NATHANIEL W. REISINGER
SIDDHARTH VELAMOOR
WILMER CUTLER PICKERING
HALE AND DORR LLP
2100 Pennsylvania Ave., NW
Washington, DC 20037
(202) 663-6000
ari.holtzblatt@wilmerhale.com

TABLE OF CONTENTS

TABLE OF CONTENTS—Continued

TABLE OF AUTHORITIES

CASES

TABLE OF AUTHORITIES—Continued

STATUTORY PROVISIONS

TABLE OF AUTHORITIES—Continued

Page

OTHER AUTHORITIES

INTEREST OF AMICUS CURIAE

Microsoft Corporation is a leading technology company that provides products and services that empower every person and every organization on the planet to achieve more by transforming the way that they work, learn, and communicate.[1]

This case presents important questions concerning the constitutional limits on so-called "reverse warrants" that compel technology providers to search for and disclose to the government private information about their own users. Reverse warrants present unique constitutional issues as they can compel the disclosure of private information for all user accounts that meet certain criteria, rather than seeking only information related to identified accounts. Microsoft is familiar with the process and privacy implications associated with responding to such warrants. Microsoft has committed to protecting its users' private data. It therefore has a significant interest in ensuring that the government does not exercise broad, unconstrained authority to use reverse warrants to rummage through that data. Microsoft has an interest in a predictable, properly constrained regime governing such warrants—one that appropriately balances the responsibility to comply with valid legal process with its commitment to protecting users' private data.

INTRODUCTION AND SUMMARY OF ARGUMENT

This case raises important issues about the application of the Fourth Amendment in the context of an individual

---

[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.

criminal defendant and a particular warrant. But it also raises broader questions about law enforcement methods targeting innovative technology that the Court should bear in mind in deciding this case.

The kind of warrant at issue—a geofence warrant that gave the government access to precise geolocation information about Google users—is one example of what are known as "reverse warrants." These warrants invert the typical process of gathering evidence. Instead of starting with reason to believe that a particular individual (or set of individuals) possesses evidence of a crime, and then identifying in a warrant the specific individual to be searched or information to be collected, reverse warrants start with specific information that could be evidence of a crime—like the use of a cell phone at the location of a robbery—and then leverage that evidence to identify particular individuals.

Reverse warrants accomplish this by authorizing the government to demand that technology companies search for and provide details about the users or accounts that meet the parameters set down in the warrant. Here, that meant querying Google users' precise geolocation data to identify users who were within a defined geographic area near a bank robbery. In other cases, however, reverse warrants have targeted users' online search queries to identify individuals who searched for particular keywords. Regardless of the subject matter, reverse warrants ultimately seek to identify *people—i.e.*, particular users of a technology provider's product or service—based on the fact that those users fell within the reverse warrant's parameters.

Directing technology providers to hunt for a needle in a haystack of user data has obvious appeal for law enforcement. But if not subject to reasonable, judicially

supervised constraints under the Fourth Amendment, this tactic will endanger users' privacy interests and threaten to embroil technology companies in determinations about whether the government has requested an appropriately narrow amount of information. Microsoft takes no position on whether the particular warrant in this case complied with the Fourth Amendment. But it has a strong interest in ensuring that the rule announced here properly balances its users' privacy interests, as the Fourth Amendment requires. To that end, Microsoft respectfully suggests that the Court adhere to the following three principles when deciding this case.

First, users maintain a reasonable expectation that the private information they store in the cloud when using devices like cell phones, tablets, and computers—including through the applications that they access through those devices—will remain private and protected from government intrusion by the Fourth Amendment.

Because this user information can be personal—particularly when it is aggregated in the hands of the government—its privacy should not be undermined by application of the third-party doctrine. When Microsoft's users use its products, services, and platforms to conduct their everyday affairs and business, they trust Microsoft to maintain the privacy of their private data—and indeed, that data remains theirs, and Microsoft designs its products, services, and platforms to protect that privacy. This makes sense because devices and applications augment users' capabilities and empower them to do more while enhancing the security of their information. These devices and applications, and by extension the technology companies that provide them, are unlike the "third parties" to whom the third-party doctrine applies. This is because using the cloud or other

online services is not analogous to handing over information to an individual, like a bank teller or phone operator, and is in any event ubiquitous and necessary to daily life.

Second, if a reverse warrant intrudes on any user's reasonable expectation of privacy, then the government must have probable cause to search *each* individual who fits the parameters identified in the warrant. The ultimate targets of reverse warrants are individuals. Under the Fourth Amendment, law enforcement must establish probable cause specific to those individuals before it may uncover private information about them. Any lesser showing would eviscerate the Fourth Amendment's protection of "people, not places" through individualized probable cause. *Katz* v. *United States*, 389 U.S. 347, 351 (1967). After all, the object of a reverse warrant is to uncover information, like location history or search queries, for particular (but as yet unidentified) individuals. The government must therefore demonstrate that it has probable cause to support a digital search of each individual that falls within a reverse warrant's parameters.

Third, the Court should clarify that a new warrant is required whenever the government conducts a new search. And it should affirm that neutral, detached magistrates must determine the scope and manner of searches, rather than leaving this sensitive exercise to the discretion of either the government or technology companies. While technology companies like Microsoft are of course well-positioned to provide a magistrate with information about the scope of a particular reverse warrant's parameters—and how many individuals it might sweep into the government's net—neutral magistrates should ultimately gatekeep the probable cause determination.

BACKGROUND

A. Technology Companies Like Microsoft Empower Their Users

The modern technological landscape has changed dramatically in a short period of time. Companies like Microsoft provide revolutionary products and services to meet the evolving needs of their users. Users depend on these products and services for a variety of purposes—from enabling entrepreneurs and nonprofits to operate organizations worldwide, to helping individuals make their lives more functional at home, school, and work, to allowing people to connect with others across the globe, and to permitting developers to create and offer new technology.

When Microsoft's customers use its services, they trust that Microsoft will keep their private information private and secure. Microsoft runs on trust, and it takes its privacy commitments to its customers seriously. Microsoft makes clear to its users the importance it places on its users' privacy and its willingness to defend those privacy interests from government intrusion. For example, Microsoft specifically promises its users that it "will protect [their] rights if a government request is made for data."[2]

B. Reverse Warrants Seek To Identify Individual Users Of Technology

Reverse warrants, like the one at issue here, "operate differently than traditional warrants." *People* v. *Seymour*, 536 P.3d 1260, 1268 n.1 (Colo. 2023) (en banc). In a typical case, "investigators first identify a suspect or suspects, then obtain a warrant to search them or their property for

---

[2] *Privacy at Microsoft*, Microsoft, https://www.microsoft.com/en-us/privacy.

evidence." *Id.* But reverse warrants "start with a potentially incriminating piece of evidence," like a search for "the address where [an] alleged arson occurred," and then "request a list of users *implicated* by that evidence." *Id.* (emphasis added).

For instance, a reverse warrant based on precise geolocation information seeks to discover all users appearing within a specified location during a specified time range (the "geofence"). The geofence warrant in this case identified a geographic area by drawing a 300-meter diameter circle, encompassing 17.5 acres of an urban area, that included the bank that was robbed and a nearby church. Pet. App. 294a. The warrant sought Google's Location History for every device within the geofence for a one-hour period the day of the robbery. Pet. App. 295a.

Other reverse warrants have sought to uncover all users that searched for a particular term online. *See, e.g.*, *Seymour*, 536 P.3d at 1268 (describing warrant that "requested a list of any users who had searched one of nine variations of '5412 N. Truckee St.,'" over a 15-day period). But the concept could be applied to other forms of user data.

Some reverse warrants target a narrow set of users, like an online search for a single residential address in a rural area. Others, like a geofence in a dense area, or a reverse keyword search using generic terms, seek to sweep more broadly. But the key commonality is that they target data processed by cloud computing companies on behalf of their customers. And because the ultimate aim of reverse warrants is to reveal information about every individual who fits the warrant's parameters, they directly implicate the privacy of technology company users.

ARGUMENT

I. USERS MAINTAIN A REASONABLE EXPECTATION OF PRIVACY IN PRIVATE INFORMATION WHEN USING THE CLOUD

The Fourth Amendment's protection against unreasonable searches and seizures serves "'to safeguard the privacy and security of individuals against arbitrary invasions by government officials.'" *Carpenter* v. *United States*, 585 U.S. 296, 303 (2018). As such, a search subject to the Fourth Amendment occurs when the government "violate[s] a person's 'reasonable expectation of privacy.'" *United States* v. *Jones*, 565 U.S. 400, 405-406 (2012). In assessing whether a search occurred under this test, a person must "have exhibited an actual (subjective) expectation of privacy," and that expectation must be "one that society is prepared to recognize as 'reasonable.'" *Katz*, 389 U.S. at 361 (1967). Generally, what someone "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* at 351-352.

A. The Power And Reach Of New Technology Does Not Erode Reasonable Expectations Of Privacy In Private Information

For decades, the Court has justifiably taken care not to let the capabilities of new technology unduly narrow the scope of what the Fourth Amendment protects. In multiple cases, the Court has held that when technology gives the government or businesses access to private information that was not previously available, individuals still maintain a reasonable expectation of privacy in that sensitive information.

In *Kyllo* v. *United States*, the Court considered whether thermal imaging software that measures heat

emanating from a house is a "search." 533 U.S. 27 (2001). There, the government argued that homeowners had no reasonable expectation of privacy in information that was exposed to the public through the exterior of the home. *Id.* at 35. The Court rejected that argument, holding that using Thermovision imaging constituted a search. In so holding, the Court explained that the government's "approach would leave the homeowner at the mercy of advancing technology." *Id.* at 35-36, 40. Then, in *Jones*, a majority of the Court found that long-term GPS monitoring of a suspect constituted "a degree of intrusion that a reasonable person would not have anticipated." 565 U.S. at 430 (Alito, J., concurring in the judgment); *id.* at 415 (Sotomayor, J., concurring). In reaching that conclusion, those five justices recognized that the technology in GPS-tracking devices "make[s] long-term monitoring relatively easy and cheap"—far exceeding what "[t]raditional surveillance" could ordinarily accomplish. *Id.* at 420 (Alito, J., concurring in the judgment); *id.* at 415 (Sotomayor, J., concurring).

In a similar vein, the Court in *Riley* v. *California* found that because modern cell phones "hold for many Americans 'the privacies of life,'" phones' contents are not subject to the exception to the warrant requirement for searches incident to arrest. 573 U.S. 373, 403 (2014). "The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." *Id.* And in *Carpenter*, the Court recognized that the government's collection of cell-site location information ("CSLI") over the course of seven days invaded the defendant's reasonable expectation of privacy. 585 U.S. at 313. In reaching that conclusion, the Court faulted the government for "fail[ing] to contend with the seismic shifts in digital technology that made

possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years." *Id.*

Across these cases, the Court has recognized that searches can intrude on a reasonable expectation of privacy regardless of whether the government "employs its own surveillance technology" or "leverages the technology" of a business. *Carpenter*, 585 U.S. at 309-10; *see also Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) (noting that although *Jones* involved the government attaching a GPS tracker, "the government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones"). What matters is the government's intrusion into an individual's private sphere, not the path the government takes to accomplish it.

B. Users Reasonably Expect That Private Information Will Remain Private Even In The Cloud

The Court should continue to consider individuals' practical, day-to-day uses of new technology when considering whether information the government seeks through reverse warrants intrudes on those users' reasonable expectation of privacy.

With respect to data showing a user's location, "[a] majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements." *Carpenter*, 585 U.S. at 310; *see Jones*, 565 U.S. at 429-430 (Alito, J., concurring in judgment; *id.* at 415 (Sotomayor, J., concurring). Like in *Carpenter*, the location tracking technology in this case relies on a person's cell phone and "faithfully follows its owner beyond public

thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." 585 U.S. at 311.

But the potential intrusion on privacy by the government is just as great, if not greater, in settings beyond location in which law enforcement might seek to use reverse warrants. While precise geolocation might indirectly reveal intimate information about a person's life, other reverse warrants could directly reveal to the government "an individual's private interests or concerns." *Riley*, 573 U.S. at 395. For instance, someone experiencing a crisis of faith might one day use their device to research resources offering spiritual guidance or find directions for the address of a new synagogue, but then the next might use their device to explore atheism or seek to participate in a virtual discussion with apostates.

Users should not have to choose between using technology that empowers them to do more and subjecting their innermost thoughts to government scrutiny free of constitutional constraints. Government access to this data would reflect "unprecedented" law enforcement "access to individuals' digitized thoughts." *Seymour*, 536 P.3d at 1284 (Marquez, J., dissenting). Accordingly, however the Court resolves this case, it should affirm that users reasonably expect that the government will not have ready access to their digitized private thoughts.[3]

---

[3] That the Stored Communications Act (SCA) might independently require the government to obtain a warrant to access this information does not alter the importance of affirming that individuals do not lose their reasonable expectation of privacy in private information merely because they used devices, services, or platforms developed by technology companies. The SCA expressly

C. The Third-Party Doctrine Should Not Be Applied Broadly To Defeat Users' Reasonable Expectations Of Privacy

The Court should not extend the third-party doctrine to deprive users of their reasonable expectation that their private data will remain protected from government intrusion even when the data is processed in the cloud. Even if it is true that users lack a "legitimate expectation of privacy" in information "exposed to [bank] employees" in the ordinary course of business, *United States* v. *Miller*, 425 U.S. 435, 442 (1976), or in "the [phone] numbers they dial," *Smith* v. *Maryland*, 442 U.S. 735, 743 (1979), the same cannot be said for the extensive private data users now entrust to technology companies. The Court should not extend a doctrine that emerged in a largely pre-digital world to the everyday uses of cell phones, tablets, and computers on which the public depends.

Miller and *Smith* do not require otherwise, particularly because they were grounded in analogies to exposing information to *people—i.e.*, actual third parties—that have no bearing on information users enter into the devices and

---

allows the government to obtain even the contents of certain communications without a warrant under some circumstances, including through a mere administrative subpoena for communications that have been stored for more than 180 days. *See* 18 U.S.C. § 2703(a), (b)(B). Accordingly, whether seeking that information constitutes a search subject to the Fourth Amendment—a query that turns on a user's reasonable expectation of privacy—may determine whether a warrant is in fact required by the SCA in a given case. And of course, because a warrant can issue only if the search complies with the requirements for individualized probable cause and approval by a neutral magistrate, *see infra* Sections II, III, a reverse warrant sought pursuant to the SCA would have to adhere to whatever the Court says in this case about the contours of those requirements.

applications that are indispensable to their ability to function in the modern world. Put differently, technology companies like Microsoft have a fundamentally different relationship with their users than the banks and phone companies of the 1970s did with their customers. In *Miller*, the fact that the records at issue were "exposed to [bank] employees in the ordinary course of business" led the Court to find that "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by *that person* to the Government." 425 U.S. at 442-443 (emphasis added). And in *Smith*, the Court emphasized that the "switching equipment that processed [the phone] numbers" dialed was "merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber." 442 U.S. at 744. Even though "the telephone company ha[d] decided to automate," such that customer information was exposed to a machine rather than a person, the automated process was doing work that traditionally had involved interacting with a phone company employee—a setting in which it would be clear that a customer lacked a reasonable expectation of privacy. *Id.* at 745.

But in contexts like email or cloud storage, there is no analog to the bank teller, phone operator, or similar individual. *Cf. Carpenter*, 585 U.S. at 313-314 ("[Cell phone companies] are not your typical witnesses" because, "[u]nlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible."). Indeed, the third-party doctrine came into force at a time when it was not *conceivable* that a customer would use technology for every facet of their personal and professional lives—and that the government could then take advantage of today's ubiquitous reliance on technology to circumvent users' reasonable expectation of privacy in their private data. *Cf. Riley*, 573 U.S. at 396-397 (cell

phone "contains a broad array of private information never found in a home in any form"). The third-party doctrine thus should not be extended to a setting that is at odds with the understanding of privacy that serves as the doctrine's foundation.

The Court has already recognized this reality. In *Carpenter*, it held that some data "shared" with telecommunications companies was not subject to the third-party doctrine, because, in part, there was a "world of difference between the limited types of personal information" addressed in third-party doctrine cases like *Miller* and *Smith*, "and the exhaustive chronicle of location information casually collected by wireless carriers today." 585 U.S. at 314.

But the same principle applies more broadly to other private information that users may communicate, generate, or store using devices and applications developed by technology companies. As Justice Sotomayor observed in *Jones*, the premise that an individual forfeits any reasonable expectation of privacy in information merely because she "voluntarily" conveys it to a third party "is ill suited to the digital age." 565 U.S. at 417 (concurring). That observation has only become truer with time. People increasingly use technology that depends on (or empowers users themselves to manage) detailed, personal information, while still expecting that information to remain private.

Where users reasonably consider that personal information private, they hold that expectation without regard to the third-party doctrine. To that end, Microsoft has committed to "protect the privacy and confidentiality of

[user] data."[4] Indeed, it specifically extends that commitment to "protect[ing] [user] rights if a government request is made for data."[5] Microsoft and its users thus share the expectation that customers' private information remains private from government intrusion even when customers are using Microsoft's products and services.

Although courts have appropriately suggested that certain specific information about users, like the contents of their emails, is outside the scope of the third-party doctrine, *see United States* v. *Warshak*, 631 F.3d 266, 288 (6th Cir. 2010); *United States* v. *Maher*, 120 F.4th 297, 308 (2d Cir. 2024), the Court need not rely on such distinctions to reject the application of the third-party doctrine to information sought by reverse warrants. Parsing the difference in a user's expectations about whether the government will be able to access the contents of private emails, versus precise location data, is increasingly beside the point in a world where most people use their cell phones, devices, and online services for all those tasks and more. Indeed, users increasingly turn to technology companies like Microsoft to *achieve* privacy, not to discard it. *See supra* at p.5.

Applying the third-party doctrine to sensitive information, over which individuals reasonably expect privacy and which is conveyed or generated through the daily use of technology, would thus transform what for many individuals is at times the most private of activities—*i.e.*, their use of a personal device—into one that is stripped of key

---

[4] *Privacy at Microsoft*, *supra*; *Microsoft Privacy Report*, Microsoft, https://www.microsoft.com/en-us/privacy/privacy-report (Jan. 2026).

[5] *Privacy at Microsoft*, *supra*.

Fourth Amendment protections. The Court should avoid that result.

II. REVERSE WARRANTS MUST BE SUFFICIENTLY PARTICULAR AND SUPPORTED BY PROBABLE CAUSE THAT IS INDIVIDUALIZED TO EACH PERSON SEARCHED

The Fourth Amendment expressly requires that "a warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity." *Kentucky* v. *King*, 563 U.S. 452, 459 (2011). These requirements ensure that a warrant is "carefully tailored to its justifications," such that "the scope of a lawful search is 'defined by the object of the search and the places in which there is probable cause to believe that it may be found.'" *Maryland* v. *Garrison*, 480 U.S. 79, 84 (1987). Thus, when the government uses a reverse warrant to conduct a search for private user information, it must be constrained by the distinct but related requirements of particularity and individualized probable cause, so that any "searches deemed necessary [are] as limited as possible." *Coolidge* v. *New Hampshire*, 403 U.S. 443, 467 (1971).

Both requirements demonstrate the importance of specificity when it comes to warrants. The "particularity" requirement limits "the authorization to search to the specific areas and things for which there is probable cause to search." *Garrison*, 480 U.S. at 84. It was "the founding generation's response to the reviled 'general warrants' … of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley*, 573 U.S. at 403; *see also Garrison*, 480 U.S. at 84 ("manifest purpose of … particularity requirement was to prevent general searches"). Particularity is the reason that "'probable cause to believe that a stolen lawnmower may be

found in a garage will not support a warrant to search an upstairs bedroom'" and that "'probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase.'" *Garrison*, 480 U.S. at 84-85 (quoting *United States* v. *Ross*, 456 U.S. 798, 824 (1982)).

Individualized probable cause provides a further—but distinct—Fourth Amendment constraint when a person (or persons) will be searched. If a search or seizure of a person requires probable cause, then it "must be supported by probable cause particularized with respect to that person." *Ybarra* v. *Illinois*, 444 U.S. 85, 91 (1979). This constraint "cannot be undercut or avoided" even if there "coincidentally … exists probable cause to search or seize another *or to search the premises where the person may happen to be*." *Id.* (emphasis added). As the Court explained in *Ybarra*, "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." *Id.* Indeed, "[a]n individual's presence in an area of expected criminal activity, standing alone" is not even "enough to support a reasonable, particularized suspicion that the person is committing a crime" for purposes of a *Terry* stop, much less the probable cause required for a warrant. *Illinois* v. *Wardlow*, 528 U.S. 119, 124 (2000); *see also United States* v. *Jaramillo*, 25 F.3d 1146, 1151 (2d Cir. 1994) ("[A]ny invasion of a person's Fourth Amendment interests must be justified at least by 'specific and articulable facts' directed to *the person* whose interests are to be invaded." (emphasis added)). This principle is foundational to the Fourth Amendment, which "'protects people, not places.'" *Jones*, 565 U.S. at 405-406 (quoting *Katz*, 389 U.S. at 351).

The showing necessary to demonstrate this individualized probable cause will depend on the facts of a particular case, given that probable cause is a "practical and common-sensical standard" that is assessed by looking "to the totality of the circumstances." *Florida* v. *Harris*, 568 U.S. 237, 244 (2013). And to be sure, evidence may well support probable cause to search or seize multiple persons. In *Maryland* v. *Pringle*, the Court held there was probable cause to arrest an occupant of a car where cash and bags of drugs were found, even though there was no evidence that distinguished Pringle (the arrestee who brought the Fourth Amendment challenge) from his two co-passengers with respect to the contraband. 540 U.S. 366, 371-373 (2003). The Court found that it was "entirely reasonable" to infer that "any or all three of the occupants" knew about and had control over the drugs. *Id.* at 372.

In reaching that conclusion, the Court distinguished the facts of *Pringle* from *Ybarra*. The warrant in *Ybarra* authorized the search of "a tavern and its bartender for evidence" of drugs, but when the police entered the tavern, they "conducted patdown searches of the customers present." *Pringle*, 540 U.S. at 372. Those pat down searches were unlawful "absent individualized suspicion." *Id.* at 373. But the arrest in *Pringle* was permissible because the three occupants of the car "were in a relatively small automobile, not a public tavern," and the "quantity of drugs and cash in the car indicated the likelihood of drug dealing" that the three men were engaged in together. *Id.* In other words, because there was probable cause to suggest *each* of the car's occupants had committed a crime—and no basis to single out one over the others—there was probable cause to arrest Pringle. *See id.* at 374.

These principles apply with equal force to Fourth Amendment searches conducted pursuant to reverse warrants. Because the government conducts a search with respect to every individual within the parameters of the warrant whose reasonable expectation of privacy it invades, *see supra* Section I, the warrant's parameters must be sufficiently particularized as to the specific evidence sought and "must be supported by probable cause particularized" to each person swept in. *Ybarra*, 444 U.S. at 91. That is true even though user information will often (but not always) be stored in a database belonging to a technology company. The Court said as much in *Carpenter*. It explained that even though CSLI "records are generated for commercial purposes," that fact "does not negate Carpenter's anticipation of privacy in *his* physical location." 585 U.S. at 311 (emphasis added); *see also id.* at 313 (rejecting argument that "cell-site records are fair game because they are 'business records'" of cell phone companies).

Carpenter thus confirms that although technology companies may sometimes be the repository for the relevant information the government seeks, it is the individual users who face an intrusion into their reasonable expectation of privacy. Reverse warrants reinforce this point. They seek to reveal personal information about *each* user—in a manner linked to that person's particular account or device—who falls within the warrant's parameters. To expose this individualized information, the government must therefore have individualized probable cause.

The government cannot avoid these constraints by analogizing to circumstances in which private information is inadvertently exposed during an otherwise lawful search. When the government carries out a search, it is often true that "innocuous documents will be

examined" or that innocent telephone conversations may be overheard. *Andresen* v. *Maryland*, 427 U.S. 463, 482 n.11 (1976). But those collateral intrusions on privacy are not the object of the search; rather, they occur within the confines of a properly warranted search "to determine whether" the reviewed documents or conversations "are, in fact, among those [items] authorized to be seized." *Id.* In the context of reverse warrants, however, revealing to the government the personal information of users who meet the reverse-warrant parameters—such as presence within a geofence or a history of searching a particular phrase—is the whole point of the search. Even though the government may not know the identity of those individuals when it serves a reverse warrant, the government intrusion on their privacy is still the aim.

Lower courts addressing geofence warrants have highlighted some of the factors that shape whether the government has demonstrated individualized probable cause and described the areas to be searched with particularity. For instance, a magistrate judge in an Illinois case declined to approve a warrant for three geofences that each spanned more than seven acres of land, where most of geofenced area "encompasse[d] structures and businesses that would necessarily have cell phone users who are not involved in these offenses." *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 *3 (N.D. Ill. July 8, 2020). The proposed warrant was thus significantly overbroad, particularly given that the "government's evidence of probable cause [was] solely focused on one user of a cellular telephone." *Id.* Similarly, a Kansas magistrate judge rejected a geofence warrant when the "geofence boundary" was drawn broadly enough to encompass two public streets

and at least one business unrelated to the crime. *In re Search of Info. Stored at Premises Controlled by Google, LLC*, 542 F. Supp. 3d 1153, 1158 (D. Kan. 2021). This meant the warrant would "potentially include the data for cell phone users having nothing to do with the alleged criminal activity." *Id.* Additionally, the application did not "adequately justify the [one-hour] time period requested." *Id.* In circumstances like those, it cannot be said that there is a "fair probability" that "evidence of a crime will be found" in the location data of each person whose cell phone is within the geofence. *Illinois* v. *Gates*, 462 U.S. 213, 238 (1983).

By contrast, in cases where courts have approved geofence warrant applications, judges have focused on the ways in which the warrants' parameters narrowly targeted the likely criminals and avoided ensnaring innocent third parties. For instance, one magistrate judge approved a geofence warrant as part of an arson investigation where "the geofence zones" were "constructed to focus on the arson sites and the streets leading to and from those sites." *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning an Arson Investigation*, 497 F. Supp. 3d 345, 358 (N.D. Ill. 2020). Importantly, the geofence zones excluded "[r]esidences and commercial buildings along the streets." *Id.* And because "the crimes occurred in the early hours of the morning when commercial businesses are usually closed and unoccupied," the warrants were even less likely to sweep in persons with no connection to the criminal activity. *Id.*

In sum, whenever the execution of a reverse warrant constitutes a search under the Fourth Amendment, there must be probable cause to search each individual who would fall within the warrant's parameters, and the place to be searched must be defined with particularity.

Those requirements mean the government must carefully craft the terms of any reverse warrant that will intrude on a reasonable expectation of privacy. When evidence supports a broad finding of probable cause, it may be appropriate for the government to broaden its lens. But when the evidence suggests that the warrant's parameters will capture individuals with "mere propinquity to others independently suspected of criminal activity," the government cannot meet its burden to justify a search. *Ybarra*, 444 U.S. at 91.

III. Reasonable Constraints On Reverse Warrants, Overseen By Neutral Magistrates, Are Necessary To Prevent Overbroad Searches And Unjustified Access To Private Information

The Fourth Amendment is an essential bulwark against the risk that law enforcement could abuse their authority in seeking information covered by geofence warrants or other reverse warrants. And the judgment of neutral magistrates, which must be interposed whenever the government conducts a new search, is critical to curtailing such abuses.

"[T]he Constitution requires 'that the deliberate, impartial judgment of a judicial officer … be interposed between the citizen and the police.'" *Katz*, 389 U.S. at 356-357 (quoting *Wong Sun* v. *United States*, 371 U.S. 471, 481-482(1963)). Unless a warrant is authorized by "the neutral and detached magistrate required by the Constitution, the search stands on no firmer ground than if there had been no warrant at all." *Coolidge*, 403 U.S. at 453. This requirement "ensure[s] that a search is not carried out" absent "an independent determination that there is probable cause," and "limits the intrusion on privacy by specifying the scope of the search." *Birchfield* v. *North Dakota*, 579 U.S. 438, 469 (2016). And that

determination must be made every time the government seeks to conduct a new search. *See Berger* v. *New York*, 388 U.S. 41, 57 (1967) (observing that a warrant that "authorized one limited intrusion" cannot serve "as a passkey to further search").

Moreover, the Fourth Amendment's requirement of warrants approved by a neutral magistrate ensures that "nothing is left to the discretion of the officer executing the warrant." *Marron* v. *United States*, 275 U.S. 192, 196 (1927). Minimizing law enforcement discretion guards against "the wide-ranging exploratory searches the Framers intended to prohibit." *Garrison*, 480 U.S. at 84. And it is why the Court has been careful not to let law enforcement's legitimate interest in catching criminals justify techniques that would knowingly subject too many people to searches without a sufficient nexus to particular criminal activity. *See City of Indianapolis* v. *Edmond*, 531 U.S. 32, 41 (2000) ("We have never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing.").

Cabining law enforcement discretion is particularly important in the context of reverse warrants. In a typical search, the risk of exploratory rummaging is real but generally cabined. An overbroad warrant might result in the search of a duplex when there was probable cause as to only one unit, or the seizure of an entire file cabinet when law enforcement should have been limited to the contents of specific folders. But the searches law enforcement may try to carry out through reverse warrants are not necessarily so limited, in light of the number of people who use a given platform or product. Even small tweaks to the parameters of a warrant can thus increase by an order of magnitude the number of innocent people who are swept up in a search "without regard to

their connection with the crime [being] investigat[ed]." *Berger*, 388 U.S. at 59.

The Court should decline to open that door. Instead, it should affirm that the Fourth Amendment's core safeguards—like the requirements of individualized probable cause and the sign-off of a neutral magistrate—are not rendered toothless by the realities of the modern digital age.

CONCLUSION

For the foregoing reasons, the Court should decide this case consistent with the principles described in this amicus brief.

Respectfully submitted.

ADELA LILOLLARI
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109

ARI HOLTZBLATT
Counsel of Record
MICHAEL BAER
NATHANIEL W. REISINGER
SIDDHARTH VELAMOOR
WILMER CUTLER PICKERING
HALE AND DORR LLP
2100 Pennsylvania Ave., NW
Washington, DC 20037
(202) 663-6000
ari.holtzblatt@wilmerhale.com

MARCH 2026