No. 25-112

In the

Supreme Court of the United States

OKELLO CHATRIE,
Petitioner,
v.
UNITED STATES OF AMERICA,
Respondent.

On Petition for Writ of Certiorari to the
United States Court of Appeals for the Fourth Circuit

BRIEF OF *AMICI CURIAE* SOFTWARE & INFORMATION INDUSTRY ASSOCIATION AND COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION IN SUPPORT OF NEITHER PARTY

Anne Voigts
Counsel of Record
Mauni Jalali
Pillsbury Winthrop Shaw Pittman LLP
2400 Hanover Street
Palo Alto, California 94304-1115
T: 650.233.4500/F: 650.233.4545
E: anne.voigts@pillsburylaw.com
mauni.jalali@pillsburylaw.com
Attorneys for Software & Information Industry Association and Computer & Communications Industry Association

TABLE OF CONTENTS

Table of Authorities

Page(s)

Cases

Statutes and Codes

Rules and Regulations

Other Authorities

Interest of *Amici Curiae*

The Software & Information Industry Association ("SIIA") is the principal trade association for those in the business of information. SIIA's membership includes nearly 400 software companies, platforms, data and analytics firms, and digital publishers that serve nearly every segment of society, including business, education, government, healthcare, and consumers. It is dedicated to creating a healthy environment for the creation, dissemination, and productive use of information. SIIA protects the rights of its members to use software as a tool for the dissemination of information.[1]

SIIA and its members have a particular interest in fostering an environment that promotes innovation while protecting consumer trust. Trust is foundational to innovation and the adoption of new technologies. Users rely on SIIA members' services with the understanding that their data is kept private and will not be shared with third parties—including the Government—absent lawful process and constitutional safeguards.

The Computer & Communications Industry Association ("CCIA") is an international, not-for-profit association that represents a broad cross-section of communications, technology, and Internet industry firms that collectively employ more than 1.6 million

---

[1] No party or counsel for a party authored this brief in whole or in part, and no one other than *amici*, their members, or their counsel funded the preparation or submission of this brief. See Sup. Ct. R. 37.6.

workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. For more than 50 years, CCIA has promoted open markets, open systems, and open networks, including as a party to or amicus in litigation. CCIA regularly supports appropriate legal safeguards, both constitutional and statutory, for personal data and information. A list of CCIA members, which includes Google, LLC, is available at https://www.ccianet.org/members.

This case directly implicates *amici*'s interests. Because the Court's decision in this case will shape the framework governing compelled disclosure of online data for years to come, *amici* respectfully submit this brief to assist the Court in considering the broader technological, legal, and practical implications of the question presented.

Introduction and Summary of Argument

This case poses the question whether the Government may, consistent with the Constitution, compel a technology service provider to search through the private and personal data of hundreds of millions of users in the hopes of identifying unknown suspects to a potential crime. Stated differently, what constitutional and statutory safeguards protect Americans from unreasonable searches of information about their person?

How this Court resolves the constitutional and statutory questions presented will directly affect both the Fourth Amendment landscape and the continued vitality of online services on which modern society

depends. *Amici* agree with Petitioner about the proper result: digital dragnets are no exception to the Fourth Amendment's prohibition on general warrants even where, as here, they involve information individuals have shared with a third-party. *Amici* submit, however, that this Court should reach that result by looking to privacy law as the proper rubric for analysis. Under Fourth Amendment history, tradition and jurisprudence, privacy law best drives the analysis because it fully protects individual and collective expectations about personal information such as location data, is more in keeping with Fourth Amendment jurisprudence, and is less likely to lead to unanticipated legal consequences.

The Fourth Amendment was crafted by the founding generation in "response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley v. California*, 573 U.S. 373, 403 (2014). "Opposition to such [general] searches was in fact one of the driving forces behind the Revolution itself," *id.*, and while that opposition arose in the context of physical searches, the constitutional principles it gave rise to apply with full force to digital searches too.

Accordingly, the Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. And where reasonableness requires a warrant, the Constitution demands that the warrant "particularly describ[e] the place to be searched, and the persons or

things to be seized." *Id.* The word "particularly" was the Framers' answer to the general warrant. It ensures that the Government identifies *whom* it wishes to search, and *what* it wishes to seize, and that it does before it searches, not after.

A geofence request inverts that constitutional sequence and at a scale the Founders would have been hard pressed to imagine.[2] This type of "reverse warrant" names no suspect. It identifies no particular person's records. It does not ask for confirmation that a particular person was in a particular place at a particular time. Instead, it directs a private company to search the location history of over 500 million people—and the records of their movements in both public and profoundly private spaces—in the hopes that a needle exists and might be found in a world full of digital haystacks. Any suspect is identified (if at all) only at the end of the process—which is to say, after the search of everyone else is already complete. This is exactly what the Fourth Amendment was designed to prevent, and it is carried out by commandeering a private intermediary to ransack the personal data of hundreds of millions of people.

Amici submit this brief to make three points.

First, a governmental demand for location history is unquestionably a "search" within the meaning of the Fourth Amendment because it reveals data in which individuals have a reasonable expectation of privacy.

---

[2] In submitting such a request, the Government seeks to know who was within a "geofence," a defined physical area during a specific period of time.

That individuals have shared such data with third parties like Google does not strip away that constitutional protection. Location history is among the most granular and revealing surveillance tools in existence, here logging a user's precise position every two minutes from the moment it is enabled. And while Petitioner contends in the alternative that property provides an alternate basis for invoking the Fourth Amendment, privacy provides a clearer, more uniform, and more administrable answer to the constitutional question.

Second, because this is a search, the Fourth Amendment's protections and requirements apply with full force at each step to every search. More specifically, the Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," and requires warrants approved by a neutral and detached magistrate, based "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

Third, the Stored Communications Act ("SCA") independently requires a warrant, because location history data constitutes "contents" of electronic communications within the meaning of 18 U.S.C. § 2510(8). The Court may resolve the case on that statutory ground alone, but Congress's independent judgment that this data warrants the law's highest protection also separately confirms that the expectation of privacy in geolocation data is one society recognizes as reasonable. *Carpenter v. United*

States, 585 U.S. 296, 304 (2018). This Court should recognize it too.

Argument

I. A Search of Location History Requires a Warrant

Both the Fourth Amendment and the SCA, 18 U.S.C. §§ 2701–2713, require that searches like the ones here be carried out only with a warrant supported by probable cause and approved of by a neutral and detached magistrate. The constitutional requirement arises from the fact that geofence requests constitute "searches." By contrast, the statutory one arises from the fact that location history data constitute the "contents" of electronic communications. But both paths lead to the same conclusion: the Government needs a particularized warrant for every such search.

A. A Fourth Amendment Search Occurs Where an Action Invades a Reasonable Expectation of Privacy

The forced disclosure of location history to the government is unquestionably a search. As this Court has repeatedly recognized, the Fourth Amendment "seeks to secure 'the privacies of life' against arbitrary power" and "a central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'" *Carpenter*, 585 U.S. at 305 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886) and *United States v. Di Re*, 332 U.S. 581, 595 (1948)).

Accordingly, in *Katz v. United States*, 389 U.S. 347, 351 (1967), this Court recognized that "the Fourth Amendment protects people, not places," and thus determined that what a person "seeks to preserve as private, *even in an area accessible to the public*, may be constitutionally protected" (emphasis added). Thus, in *Katz*, the Court determined that the Government's actions in electronically listening to and recording the petitioner's words in a public telephone booth "violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment." *Id.* at 353. It stated that "[w]herever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures." *Id.* at 359.

After *Katz,* courts have applied the reasonable expectation of privacy test articulated in Justice Harlan's concurrence to determine whether a governmental request rises to the level of a search. *United States v. Jones*, 565 U.S. 400, 406 (2012); *Katz,* 389 U.S. at 361 (Harlan, J., concurring) (asking first whether a person has "exhibited an actual (subjective) expectation of privacy" and, second, whether that expectation is "one that society is prepared to recognize as 'reasonable'"). And in the context of cell-site location information ("CSLI"), this Court has held that individuals can retain this reasonable expectation of privacy—and thus their Fourth Amendment rights—in information they disclose to third parties, such as cell phone service providers. *Carpenter*, 585 U.S. at 313–16.

As discussed below, application of the "reasonable expectation" test shows that individuals have a similarly protected right in their location history, and that, as a result, the Government must obtain a judicial warrant before requiring companies to disclose users' location history or unmasking their identities to law enforcement.

B. Individuals Have a Reasonable Expectation of Privacy in Their Location History

The Government's position that individuals have no expectation of privacy in their location history is unsound. Individuals *do* have a reasonable expectation of privacy in their location history, and the fact that the information is shared with a third party does *not* defeat that expectation.

Start with the information itself: Location history is a "virtual journal of [a user's] whereabouts over a period of time." JA-16; *United States v. Chatrie*, No. 3:19-cr-00130-MHL (E.D. Va. Dec. 20, 2019). Even when that period of time is short, the information location history can expose is deeply personal—documenting a visit to "the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, [or] the gay bar." *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) (*quoting People v. Weaver*, 909 N.E.2d 1195, 1199 (N.Y. 2009)).

And even where individual data points might not reveal anything particularly personal, the accretion of

those points over time unquestionably does. "Location History appears to be the most sweeping, granular, and comprehensive tool—to a significant degree—when it comes to collecting and storing location data." *United States v. Chatrie*, 590 F. Supp. 3d 901, 907 (E.D. Va. 2022). That data can pinpoint the location and movements of millions of people, 24/7 for years, in public and private spaces alike, so long as they carry their cell phone with them.[3] And that in turn "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations,'" which "hold for many Americans the 'privacies of life.'" *Carpenter*, 585 U.S. at 311 (quoting *Jones*, 565 U.S. at 415).

In fact, location history data is far more revealing than the CSLI that *Carpenter* concluded was entitled to constitutional protection. CSLI typically reflects a device's location on the order of dozens to hundreds of city blocks in urban areas, *id.* at 336 (Kennedy, J., dissenting), while location history can estimate a user's position to within a matter of meters. *Chatrie*, 590 F. Supp. 3d at 909. If seven days of CSLI provided the "detailed, encyclopedic, and effortlessly compiled" record that *Carpenter* found constitutionally protected, 585 U.S. at 309, then location history—

---

[3] As this Court has recognized, cell phones have become "'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." *Carpenter*, 585 U.S. at 298. Further, with the proliferation of smartphone-connected wearables, such as smart watches, location history and other historical movement data may also capture those moments where a cell phone is left behind.

which tracks users at a precision that is orders of magnitude greater—*a fortiori* warrants at least the same degree of protection. The Fifth Circuit reached precisely this conclusion, recognizing that "[g]iven the intrusiveness and ubiquity" of location history data, users retain a reasonable expectation of privacy in that data. *United States v. Smith*, 110 F.4th 817, 836 (5th Cir. 2024).

Neither advances in technology, nor the fact that the technology in question is in the hands of private companies, nor the fact that geofence requests may involve more limited intrusions across a larger number of individuals, nor even the Government's analogies to other investigative techniques make these demands for Location History any less of a search, let alone cure the constitutional problems inherent in them.

First, those "historical expectations of privacy do not change or somehow weaken simply because we now happen to use modern technology to engage in activities in which we have historically maintained protected privacy interests." *United States v. Davis*, 785 F.3d 498, 524–25 (11th Cir. 2015) (Rosenbaum, J., concurring), *abrogated on other grounds by Carpenter*, 585 U.S. 296. In *Kyllo v. United States*, 533 U.S. 27, 34 (2001), this Court expressly rejected the idea that advances in technology should be allowed "to erode the privacy guaranteed by the Fourth Amendment."

That principle applies with equal force to protect users' historical expectations of privacy, including but not limited to their movements within their own homes, against governmental overreach where that

technology is in the hands of private companies. Nothing about the fact that the search is executed by private entities—or private entities' tools—changes that analysis. "Although the Fourth Amendment does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative, the Amendment protects against such intrusions if the private party acted as an instrument or agent of the Government." *Skinner v. Ry. Lab. Execs' Ass'n*, 489 U.S. 602, 614 (1989). Indeed, the fact that Congress itself imposed a warrant requirement in the SCA further demonstrates that the "expectation of privacy is one that society is prepared to recognize as reasonable." *Carpenter*, 585 U.S. at 304.

Nor can the Government "avoid *Carpenter*'s warrant requirement by using many small intrusions over a large population (as it does with geofence warrants) rather than a few large intrusions over a small population (as it did in *Carpenter*)" because "a geofence violates the reasonable expectation of privacy of each user swept up in its bounds." Haley Amster & Brett Diehl, *Against Geofences*, 74 STAN. L. REV. 385, 407–08 (2022); *see Carpenter*, 585 U.S. at 311–12 (holding that individuals maintain a reasonable expectation of privacy in records of their physical movements as captured through location data); *Smith*, 110 F.4th at 837–38 (holding geofence warrants are unconstitutional general warrants lacking particularity). Unlike the CSLI requests in *Carpenter*, which targeted the records of specifically identified suspects, a geofence request sweeps across the location history records of *every* user who has opted into the service—in this case, over hundreds of millions of

people. This digital dragnet—compelling a private company to sift through the intimate location records of hundreds of millions of people to identify unknown suspects without any individualized suspicion—represents a qualitatively and quantitatively different intrusion on privacy that is far more sweeping than anything this Court confronted in *Carpenter*.

Finally, the Government has compared location history to other "markers" left at a public crime scene that do not require a warrant, like tire tracks or boot prints. Brief for the United States in Opposition at 11, *United States v. Chatrie*, No. 25-112 (U.S. Nov. 24, 2025). This is a misdirection. That one can glean that a suspect has been at a crime scene from all three does not make them equal. To identify a tire track or a boot print at a public crime scene requires only that one walk through public spaces and use the senses available to a person to observe the present. It cannot compare to a geofence search of historical data collected around the clock over the course of years that is not available to the public. Otherwise, one could also identify whether an individual has been at a crime scene by reading her diary or eavesdropping on her private conversations—but these things are clearly protected by the Fourth Amendment.

C. Under *Carpenter*'s Balancing Test, the Third-Party Doctrine Does Not Negate a User's Reasonable Expectation of Privacy in Their Location History

"People often do reasonably expect that information they entrust to third parties, especially

information subject to confidentiality agreements, will be kept private." *Carpenter,* 585 U.S at 389 (Gorsuch, J., dissenting). While courts have divided over the application of the third-party doctrine post-*Carpenter*, correctly understood, the third-party doctrine does not undercut *Carpenter*'s constitutional reasoning or the result of applying that reasoning here. Matthew Tokson, *The Aftermath of* Carpenter*: An Empirical Study of Fourth Amendment Law, 2018–2021*, 135 HARV. L. REV. 1790, 1807–21, 1836–39 (2022). *Carpenter* provided much needed clarification about how the third-party doctrine applies in light of technological advancements that have altered the landscape of third-party involvement in daily life.

In *Carpenter*, the Court declined to apply the third-party doctrine to CSLI—which is maintained by and thus shared with third-party wireless carriers—concluding that there is a "world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today." 585 U.S. at 314. Accordingly, the *Carpenter* Court reinterpreted *Miller* and *Smith* as applying a balancing test: these cases were not just about whether an individual had shared information, but also about the nature of the documents as weighed against any legitimate expectation of privacy in the information conveyed. Laura K. Donohue, *Functional Equivalence and Residual Rights Post-*Carpenter*: Framing A Test Consistent with Precedent and Original Meaning*, 2018 SUP. CT. REV. 347, 372–73 (2018); *Carpenter*, 585 U.S. at 313–15. *Miller* centered on "negotiable instruments to be used in commercial

transactions," while the telephone records in *Smith* provided little by way of "identifying information." Donohue, *supra*, at 373; *Carpenter*, 585 U.S. at 314. By contrast, the CSLI in *Carpenter* occupied its own, distinct category, given: (a) the number of people implicated (*Carpenter*, 585 U.S. at 312, 313), (b) the volume of information (*id.* at 300–01), (c) the revealing nature of that information (*id.* at 309, 312, 315), (d) the lack of resource constraints in obtaining it (*id.* at 310–11), (e) the retrospective nature of the information (*id.* at 312), (f) the near perfect recall (*id.* at 313–14), (g) the potential length of time for which information can be obtained (*id.* at 312), and (h) the increasing precision (*id.* at 313). Donohue, *supra*, at 373–74.

Applying those factors here makes it clear that the third-party doctrine does not do away with either individuals' reasonable expectation of privacy in their location history or the ensuing need for a warrant that satisfies the Fourth Amendment's strictures. The Government has suggested that because location history is "opt-in," users have meaningfully consented to Government access. BIO at 10–11. But as this Court recognized in *Carpenter*, cell phones and the services they provide are "'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society," 585 U.S. at 298, and users who enable location history to obtain basic functionality like traffic updates and phone-finding services do not thereby assume the risk that the Government will ransack their comprehensive location records without first obtaining a constitutionally adequate warrant. *See Smith*, 110

F. 4th at 836 ("[T]he fact that approximately 592 million people have 'opted in' to comprehensive tracking of their locations itself calls into question the 'voluntary' nature of this process. In short, 'a user simply cannot forfeit the protections of the Fourth Amendment for years of precise location information by selecting "YES, I'M IN" at midnight while setting up Google Assistant, even if some text offered warning along the way.'"); *Matter of Search of Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 737 (N.D. Ill. 2020) ("The Court finds it difficult to imagine that users of electronic devices would affirmatively realize, at the time they begin using the device, that they are providing their location information … in a way that will result in the government's ability to obtain – easily, quickly and cheaply – their precise geographical location at virtually any point in the history of their use of the device.").

The Fourth Amendment was ratified by a generation that entrusted its most private correspondence to third-party letter carriers. That generation rightly did not understand these acts of entrustment as acts of constitutional surrender. *See Ex parte Jackson*, 96 U.S. 727, 733 (1877); Akhil Reed Amar, The Bill of Rights: Creation and Reconstruction 64–77 (1998); Pauline Maier, Ratification: The People Debate the Constitution, 1787–1788, at 257–319 (2010). The same principle holds true today.

The smart home example underscores the need to carefully balance these constitutional factors in determining whether the third-party doctrine should apply. "The emergence of home automation—

otherwise known as the smart home—is a natural step in the rapid growth of the 'Internet of Things'—the proliferation of everyday products that connect to the internet." Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924, 1939 (2017); *see Kyllo*, 533 U.S. at 34 (warning that failure to protect minimal privacy expectations in the home "would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment"). But the rise of the Internet of Things has resulted in a world where personal and sensitive data "gathered by an ever-ballooning array of devices, from vehicles to appliances to pacemakers . . . is disseminated across a multitude of third parties" to facilitate the use of those products or services. *If These Walls Could Talk*, *supra*, at 1939. This includes smart home voice assistants that an individual may choose to use and to let listen to, record, and store data reflecting what they hear within the home. *Id.* at 1939–41. Similarly, individuals may choose to use smart security cameras that record and store high-fidelity audiovisual feeds of the inside of their users' homes. *Id.* at 1941. The home is historically the heart of Fourth Amendment protections, but a mechanical and categorical application of the third-party doctrine in such circumstances could eviscerate those protections. *Kyllo*, 533 U.S. at 34; *If These Walls Could Talk*, *supra*, at 1925–26. With the evolution and integration of technology as a cornerstone of everyday life, traditional application of the third-party doctrine "risks swallowing the Fourth Amendment whole." *If These Walls Could Talk, supra,* at 1945.

Indeed, as technology becomes ever more embedded in Americans' daily lives, courts must confront a practical reality: information that individuals reasonably regard as private is routinely conveyed to third-party service providers as a simple function of how modern technology operates. Wireless carriers have access to cell phone users' CSLI; social media websites and applications have access to location history; companies that store laptop or cellphone backups have access to the digital contents of private devices, including users' photos, videos, messages, app data, device settings, home screen layout, and app organization; email service providers have access to users' private correspondence; smart home systems keep logs of in-home use of light switches, thermostats, and appliances, and may record audio and video within a home; doorbell cameras, smart locks, and security systems log comings and goings of residents and visitors; and wearable devices collect private health data, including sleep schedules, activity levels, and vital signs. Under a mechanical application of the third-party doctrine, individuals who used any of those technologies would forfeit any expectation of privacy in their data, which is necessarily stored and processed by third parties. Participating in modern society should not come at such a constitutional cost.

D. Because These Are Searches, They Require Warrants For Each Search

Properly characterizing these digital dragnets as searches within the meaning of the Fourth Amendment comes with constitutional consequences.

Because required disclosure of location history constitutes a search, it requires a warrant for each search. *Carpenter*, 585 U.S. at 316. And each of those warrants must satisfy the Fourth Amendment's requirements of particularity and probable cause. In other words, as noted above, to comply with the Fourth Amendment, geofence warrants must be based upon probable cause and "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

Particularity is not a preference. It is a constitutional requirement, and "a search conducted pursuant to a warrant that fails to conform to the particularity requirement of the Fourth Amendment is unconstitutional." *Groh v. Ramirez,* 540 U.S. 551, 559, 564–65 (2004). Accordingly, this Court has "long held" that a particular warrant not only prevents general searches but also "assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search." *Groh*, 540 U.S. at 561; *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971) (particularity guarantees that intrusions are "as limited as possible"). That the Government may ultimately exercise restraint in their search does not retroactively validate their conduct—such restraint must be imposed by judicial officers, not law enforcement or private entities. *Katz*, 389 U.S. at 356–57.

Geofence requests present an old problem (general warrants) dressed up in new clothing (the nature of the technology used to carry them out in a manner and at a scale the Founders could not have

contemplated). But to the extent they pose novel logistical challenges, the principles of constitutional analysis compel the same result. By their very nature, geofence warrants authorize "broad searches of entire location history databases, simply on the off chance that somebody connected with a crime might be found." Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2518 (2021); *see also Smith*, 110 F.4th at 822–25. Commentators have noted "direct parallels" between geofence warrants and the practice of general warrants—which specify only an offense and leave "to the discretion of executing officials the decision as to which persons should be arrested and which places should be searched"—to which the Fourth Amendment is a direct response. *Geofence Warrants and the Fourth Amendment*, *supra*, at 2518; *see also Steagald v. United States*, 451 U.S. 204, 220 (1981); *Coolidge*, 403 U.S. at 467 ("Here, the specific evil is the 'general warrant' abhorred by the colonists, and the problem is not that of intrusion per se, but of a general, exploratory rummaging . . . .").

Probable cause exists where law enforcement has a reasonable belief that an offense has been or is being committed "and that evidence bearing on that offense will be found *in the place to be searched*." *Safford Unified Sch. Dist. No. 1 v. Redding*, 557 U.S. 364, 370 (2009) (emphasis added). That in turn requires some degree of specificity; this Court has previously found no probable cause for an arrest where an informant's accusation "merely invited the officers to roam . . . some 30 blocks" in search of a suspect. *Wong Sun v. United States*, 371 U.S. 471, 480–81 (1963). Thus, it

is not sufficient constitutional justification to claim that a search of the location history for over 500 million users might ultimately lead law enforcement to identify a suspect.

Moreover, a multi-step procedure that does not require law enforcement to return to the judge to identify, with particularity, from which users they will seek expanded location history data over a greater time period and search area and, even more concerningly, which users they will unmask, obtaining those users' "date of birth if available, account time and account number, email addresses associated with the account . . . , telephone numbers associated with the account . . . ," JA-130 to JA-131, cannot be squared with the Constitution. (It also imposes a significant burden on private companies.)

Nor does a request's limited duration satisfy particularity, and any argument to the contrary misapprehends both the nature and the scope of the intrusion. As a threshold matter, *Carpenter* did not hold that the Government may freely obtain location so long as it does not exceed some durational threshold, and its logic does not support such a rule. 585 U.S. at 310–11. The constitutional concern, rather, is the Government's ability to "travel back in time to retrace a person's whereabouts," *id.* at 312, and the "detailed, encyclopedic, and effortlessly compiled" nature of the resulting record. *Id.* at 309. Two hours of location history data, logging a user's precise position every two minutes, pinpointing the floor of a building on which the user is standing—can reconstruct a person's movements in extraordinary

and intimate detail. And more fundamentally, measuring the intrusion by the data *ultimately* obtained about the petitioner ignores the scope and number of searches required to reach that point, beginning with a warrantless rummaging through the location records of over 500 million people.

E. Privacy Law Provides the Appropriate Rubric for the Constitutional Question Here

A Fourth Amendment search occurs when the Government infringes on either a property interest, or a reasonable expectation of privacy, but this Court need not—and should not—resolve the constitutional question here under property law. Where, as is the case here, the challenged conduct involves compelled access to digital records rather than a physical trespass, it is possible (and indeed easier) to decide the case based on reasonable expectations of privacy without first determining who "owns" the underlying data.

Typically, a property-based test has been used in cases involving physical intrusions on land or chattel. It works significantly less well in the context of digital data or information, which is more akin to a telephone call (that can be eavesdropped on) rather than a filing cabinet, car, or apartment (that can be physically intruded upon). *See Katz*, 389 U.S. at 351.

It must not be assumed that property law is clearer and more resistant to manipulation than conceptions of privacy and reasonable expectations thereof. It is not. "Property is as capacious,

multifaceted, and potentially complicated as privacy, with numerous forms of ownership that are divisible and combinable across people and time." Michael C. Pollack & Matthew Tokson, *Decentering Property in Fourth Amendment Law*, 92 U. CHI. L. REV. 705, 708 (2025); *see Katz*, 389 U.S. at 353 (discrediting "the premise that property interests control"); *Kyllo*, 533 U.S. at 32 ("We have since decoupled violation of a person's Fourth Amendment rights from trespassory violation of his property."); *see also Tahoe-Sierra Pres. Council, Inc. v. Tahoe Reg'l Plan. Agency,* 535 U.S. 302, 318 (2002) ("Property interests may have many different dimensions. For example, the dimensions of a property interest may include a physical dimension (which describes the size and shape of the property in question), a functional dimension (which describes the extent to which an owner may use or dispose of the property in question), and a temporal dimension (which describes the duration of the property interest)."). And troublingly for a property-law-centered approach to the Fourth Amendment, "some of the most pressing Fourth Amendment questions—now and in the foreseeable future—involve electronic data and other forms of information largely outside the realm of property law." Pollack & Tokson, *supra*, at 709. For example, "even now, decades after email became a fundamental part of our lives, the question of who actually owns email accounts has proven stubbornly difficult to resolve." *Id.* at 754. Grounding Fourth Amendment protection in property entitlements would therefore risk resolving core constitutional safeguards on unsettled questions of "data ownership," and even permit the mere fact of

third-party storage to do the work that *Carpenter* refused to let the third-party doctrine do.

Moreover, a property-law-centered approach raises real issues of administrability and disuniformity not least because property law is "the canonical example of the local." Maureen E. Brady, *The Illusory Promise of General Property Law*, 132 YALE L.J. FORUM 1010, 1022–42 (2023). A Fourth Amendment regime based on property raises a slew of questions about how one decides when and what property rights attach, and it leaves the answers—at least in the first instance—to a law enforcement officer to determine whether and what property rights attach to a particular set of data that is maintained by any given entity and subject to any given agreements. If they guess incorrectly and do not seek a warrant, they risk suppression of evidence.

Fourth Amendment inquiries are often fact-specific, but they are best carried out by applying clear, consistent legal principles to those varying facts. Put differently, though the facts may differ, the legal principles should not. But in the world of digital information and data, property is less of a rigid entitlement than it has been in days past as to rights to tangible property. Service providers and users often share partial, overlapping, and purpose-specific rights in data by contract, license, and evolving terms of service. These divisible "rights" are sometimes subject to unilateral modification, rendering them a poor constitutional yardstick. Further, "government surveillance itself has become decoupled from property over the last century, and particularly in the digital era," where "the government's property

intrusions are purely incidental to gathering sensitive data about individuals." Pollack & Tokson, *supra*, at 709–10.

In a situation involving "a microphone that touches an apartment's heating duct while it secretly records the occupant's personal conversations," "[m]aking the Fourth Amendment turn on the grazing of the heating duct, rather than the recording of people's conversations, badly misses the point." *Id.* at 710. Indeed, the Court in *Katz* criticized the property-focused formulation of the issues in a case involving reasonable expectation of privacy in a telephone call made in a public telephone booth. 389 U.S. at 349–50. It noted that these formulations led to a disproportionate emphasis on the characterization of the telephone booth. *Id.* at 351. Had *Katz* turned on a rigid property-centered-approach, the Government's intrusion may have been allowed to stand. Indeed, "the Court of Appeals rejected the contention that the recordings had been obtained in violation of the Fourth Amendment, because '(t)here was no physical entrance into the area occupied by, (the petitioner).'" *Id.* at 348–49.

This Court should also eschew a property-based approach here that could spawn unintended consequences well outside the Fourth Amendment realm. For one, a property-law-centered approach would require courts to determine property rights in uncharted territories such as email, social media accounts, web browsing data, search engine queries, and more—determinations with wide-ranging effects well beyond the Fourth Amendment realm. *See also* Daniel J. Solove, *Understanding Privacy*, 84 U. CHI. L.

REV. 61, 103 n.136, 106–116 (2017); *id.* at 110 (to consider data as property "would require embracing features of ownership that are fundamentally inconsistent with what it means to call something property.").

Accordingly, the better way to conceptualize this analysis is through privacy concerns. Such a formulation is not new, and reasonable expectations of privacy are increasingly standardized, even across time periods. *See Davis*, 785 F.3d at 524–25. In 1886, this Court found that compulsory production of private papers to establish a criminal charge was a search within the Fourth Amendment even without "the breaking of his doors, and the rummaging of his drawers." *Boyd*, 116 U.S. at 630. "Breaking into a house and opening boxes and drawers are circumstances of aggravation; but any forcible and compulsory extortion of a man's own testimony, or of his private papers to be used as evidence to convict him of crime, or to forfeit his goods, is within the condemnation of that judgment." *Id.* Eighty years later, this Court reaffirmed the principle that the Fourth Amendment is not constrained by property rights in *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294 (1967): "We have recognized that the principal object of the Fourth Amendment is the protection of privacy rather than property, and have increasingly discarded fictional and procedural barriers rested on property concepts." *Id.* at 304.

Indeed, this Court has previously referred to a constitutional privacy "interest in avoiding disclosure of personal matters." *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134, 138 (2011) (noting

that *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977); *Nixon v. Administrator of General Services*, 433 U.S. 425, 457 (1977), referred to such a right and "assum[ing], without deciding, that the Constitution protects [such] a privacy right").[4] *Whalen* concerned New York's practice of collecting "the names and addresses of all persons" prescribed dangerous drugs with both "legitimate and illegitimate uses." 429 U.S. at 591. In discussing that claim, the Court said that "[t]he cases sometimes characterized as protecting 'privacy'" actually involved "at least two different kinds of interests": one, an "interest in avoiding disclosure of personal matters"; the other, an interest in "making certain kinds of important decisions" free from government interference. *Id.*, at 598–600. Shortly thereafter, this Court acknowledged a constitutional "interest in avoiding disclosure" in *Nixon*, 433 U.S., at 457, when former President Nixon brought Fourth and Fifth Amendment challenges to the Presidential Recordings and Materials Preservation Act, a statute that required him to turn over his Presidential papers and tape recordings for archival review and screening. 433 U.S., at 455–65. And subsequent cases have alluded to a right to informational privacy as against the Government. *Department of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 762–63 (1989); *New York v. Ferber,* 458 U.S. 747, 781, n.10, (1982). Whether or not such a right exists independently, those cases all

---

[4] The Court has repeatedly recognized that the Government has significantly greater leeway in its dealings with citizen employees (as in *Nelson*) than it does when it brings its sovereign power to bear on citizens at large (as here). *Borough of Duryea, Pa. v. Guarnieri,* 564 U.S. 379, 392 (2011).

support applying *Katz*'s reasonable expectations of privacy test, rather than property law, to the questions here.

This case arose out of privacy concerns; it therefore should be resolved based on them. That would be consistent with this Court's prior jurisprudence from before *Katz* through *Carpenter*, dealing with government intrusions on intangibles such as private telephone communications and CSLI through a privacy—not a property—lens.

F. Alternatively, This Court Need Not Answer the Constitutional Question Because the SCA Separately Requires the Government To Obtain a Warrant Here

This Court has long adhered to the principle that "[i]f a case can be decided on either of two grounds, one involving a constitutional question, the other a question of statutory construction or general law, the Court will decide only the latter." *Ashwander v. TVA*, 297 U.S. 288, 347 (1936) (Brandeis, J., concurring). Here, even assuming for the sake of argument that a geofence request does not implicate the Fourth Amendment—a conclusion amici respectfully submit would be incorrect—the Stored Communications Act independently requires the Government to obtain a warrant before asking Google to disclose its users' location history data. The Court may therefore resolve this case on statutory grounds without reaching the constitutional question. The SCA's treatment of location history as "contents" is itself powerful evidence that the "expectation of privacy is one that

society is prepared to recognize as reasonable." *Carpenter*, 585 U.S. at 304.

1. The SCA's Tiered Framework Imposes a Warrant Requirement for the "Contents" of Electronic Communications

The Stored Communications Act, 18 U.S.C. §§ 2701–2713, governs how electronic service providers handle their users' stored electronic communications. The statute establishes a tiered framework keyed to the nature of the information sought. For the "contents" of electronic communications, information reflecting the "substance, purport, or meaning" of a communication, 18 U.S.C. § 2510(8), the SCA imposes the law's most stringent protection: the Government must obtain a search warrant supported by probable cause. 18 U.S.C. § 2703(a), (b)(1)(A). By contrast, non-content "records" of electronic communications—such as basic subscriber information, session times, or metadata reflecting the characteristics rather than the substance of a communication—may be obtained through lesser forms of legal process, including court orders under § 2703(d) or administrative subpoenas. 18 U.S.C. § 2703(c), (d); *see In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014) (distinguishing "contents" from "record information regarding the characteristics of the message that is generated in the course of the communication").

The SCA question therefore turns on whether the location history data are "contents" or merely "records."

2. Location History Data Are "Contents" Within the Meaning of the SCA

The SCA defines an "electronic communication" as a "transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part" by an electronic system. 18 U.S.C. § 2510(12). And it defines the "contents" of such a communication as "any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8).

Location history satisfies both SCA definitions. When a user's device transmits location data—derived from GPS, Bluetooth, Wi-Fi, and cellular signals—to Google's servers for processing and storage, this transmission is a "transfer of signs, signals, [and] data" by an electronic system within the meaning of § 2510(12). The location data so transmitted constitute "contents" because the user's physical location *is* the "substance, purport, or meaning" of the communication. *Id.* § 2510(8). The user's whereabouts are the entire point of the data transfer: they are what populates the user's Timeline, enables personalized recommendations, and allows the user to retrace her steps. When a user communicates her location through the location history service, that location is the "intended message conveyed by the communication," *In re Zynga Privacy Litig.*, 750 F.3d at 1106—not ancillary "record information regarding the characteristics of the message that is generated in the course of the communication," *id.* Location history therefore carries the same import—the same

expectation of privacy——as any other subset of location data.

This conclusion follows directly from the principle, now well established, that the content/non-content distinction turns not on the *type* of data (such as whether it is location data), but on the *function* the data performs in the particular communication. As the Third Circuit held in *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125 (3d Cir. 2015): "[A]ddresses, phone numbers, and URLs may be dialing, routing, addressing, or signaling information, but only when they are performing such a function. If a[] . . . URL is instead part of the substantive information conveyed to the recipient, then by definition it is 'content.'" *Id.* at 137. The Third Circuit explained that "there is no general answer to the question of whether locational information is content. Rather, a 'content' inquiry is a case-specific one turning on the role the location identifier played in the 'intercepted' communication." *Id.*

Applied here, the conclusion is inescapable. Unlike CSLI—which consists of time-stamped records automatically generated by wireless carriers as a byproduct of maintaining the cellular network, *Carpenter*, 585 U.S. at 300–01, and which courts have accordingly treated as non-content records, *see United States v. Graham*, 824 F.3d 421, 433 (4th Cir. 2016) (en banc) (describing CSLI as "non-content information" because it constitutes "information that facilitate[s] personal communications, rather than part of the content of those communications themselves"), *abrogated on other grounds by Carpenter*, 585 U.S. 296—Location

history data is neither automatically generated nor incidental to some other communication. A user who enables location history is not placing a phone call or sending a text message, with location data thrown off as a byproduct; she is affirmatively communicating her location so that it can be processed, stored, and presented back to her. The location data does not perform any "routing" or "addressing" function—it does not facilitate the delivery of some other message to its intended destination. It *is itself* the substantive message being conveyed.

3. Because Location History Data Are "Contents," the SCA Requires a Warrant

Because location history data constitutes "contents" of electronic communications under the SCA, the Government must obtain a search warrant supported by probable cause before compelling Google to disclose it. 18 U.S.C. § 2703(a), (b)(1)(A) (incorporating requirements of Fed. R. Crim. P. 41). This is so regardless of whether a geofence request constitutes a "search" for Fourth Amendment purposes. The SCA imposes its own, independent warrant requirement for contents—a requirement that exists precisely because Congress determined that the substance of a person's electronic communications warrants the highest available protection from Government intrusion. The nature of the data demands no less.

Congress's deliberate classification of communication "contents" as deserving the law's highest protection reflects and confirms the societal

expectation that such information will be kept private. The SCA thus provides both an independent statutory ground for requiring a warrant and powerful confirmation that location data, including location history, deserves protection from intrusion.[5]

Conclusion

The Fourth Amendment was born of a conviction that Government intrusion must have limits—that there are private spaces, private papers, and private movements that the state may not peer into without cause or constitutional constraint. The question now is whether those principles will hold in the digital age, or whether the Government may circumvent the Fourth Amendment simply by directing its search through a private company's servers rather than a citizen's front door.

The answer is clear. The text of and the principles undergirding the Fourth Amendment protect a person's right against Government intrusion in data and information just as much as in land and papers. It protects that right based on reasonable

---

[5] As noted above, and as this Court recognized in *Carpenter*, the fact that Congress "imposed a warrant requirement in the SCA further demonstrates that the 'expectation of privacy is one that society is prepared to recognize as reasonable.'" 585 U.S. at 304.

expectations of privacy. The Court should adopt this express holding within this case to provide necessary clarity to U.S. law enforcement, businesses, and residents.

Respectfully submitted,

Anne Voigts
Counsel of Record
Mauni Jalali
Pillsbury Winthrop Shaw Pittman LLP
2400 Hanover Street
Palo Alto, California 94304-1115
T: 650.233.4500/F: 650.233.4545
E: anne.voigts@pillsburylaw.com
mauni.jalali@pillsburylaw.com

Attorneys for Software & Information Industry Association and Computer & Communications Industry Association

Dated: March 9, 2026