No. 25-112

IN THE

Supreme Court of the United States

OKELLO T. CHATRIE,

Petitioner,

v.

UNITED STATES,

Respondent.

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

BRIEF OF PROFESSOR ORIN S. KERR AS AMICUS CURIAE IN SUPPORT OF RESPONDENT

ORIN S. KERR
Counsel of Record
559 Nathan Abbott Way
Stanford CA 94305
(650) 498-8125
orin@orinkerr.com

April 1, 2026

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D.C. 20002

TABLE OF CONTENTS

TABLE OF CONTENTS—Continued

TABLE OF AUTHORITIES

CASES Page(s)

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

INTEREST OF *AMICUS CURIAE*[1]

Orin S. Kerr is a Professor at Stanford Law School and a Senior Fellow at the Hoover Institution. He has written extensively about the Fourth Amendment and digital technology, including in a recent book, *The Digital Fourth Amendment: Privacy and Policing in Our Online World* (2025). The interest of amicus is the sound development of the law.

SUMMARY OF ARGUMENT

The challenge of new technology is a recurring theme in Fourth Amendment law. This case raises a host of new and important questions, and this brief hopes to help frame the issues and provide directions for answering them.

The first set of questions considers whether obtaining Chatrie's Location History records was a Fourth Amendment "search" of his "papers." There are two different arguments to evaluate. The first is the virtual private locker question. Did Chatrie store his Location History records in a virtual private locker with Google, such that he had Fourth Amendment rights in the contents of the virtual locker just as he

---

[1] Pursuant to Supreme Court Rule 37.6, amicus affirms that no counsel for a party authored the brief in whole or in part and that no counsel or a party made a monetary contribution intended to fund the preparation or submission of the brief. Stanford University provides financial support for activities related to faculty members' research and scholarship, which may help defray the costs of preparing this brief. (Neither Stanford nor any institution at Stanford is a signatory to this brief, and the views expressed here are solely those of the amicus curiae.) Otherwise, no person or entity other than the amicus curiae has made a monetary contribution intended to fund the preparation or submission of this brief.

would with an equivalent physical locker? This brief concludes that the answer is likely no. Although the record is murky on the point, Chatrie likely lacked the control over the records needed to have Fourth Amendment rights in them.

The second search argument considers whether Chatrie had Fourth Amendment rights under the limits placed on the third-party doctrine by *Carpenter v. United States*, 585 U.S. 296 (2018). This brief argues that he did not. *Carpenter* does not apply because Chatrie voluntarily opted in to have Google create and store his Location History records.

The next set of issues considers the lawfulness of the warrant, assuming that one was needed. The brief argues that a properly drawn geofence warrant can satisfy the Fourth Amendment. The Fourth Amendment does not present an all or nothing choice between zero protection and absolute protection. Where the law requires a warrant, it also provides a means to draft a lawful warrant.

On the specifics of the warrant in this case, the warrant was properly drawn as to Step 1 because it was sufficiently narrow in both time and space. The constitutionality of the warrant at Step 2 is uncertain, however. It is not clear that the Fourth Amendment allows multi-stage warrants, and the particularity of Step 2 debatable. Chatrie may not have raised these issues as to Step 2, however, so they may be waived.

The fact that this case reaches the Court so late in the Term, and that it raises so many complex issues, suggests that there may be value in pointing to a resolution that might plausibly reach consensus. If so, amicus suggests that the Court might want to resolve this case by focusing primarily on the warrant issues.

The legality of the warrant implicates fewer contested questions and has a more complete factual record. For the sake of completeness, however, this brief covers both issues.

ARGUMENT

I. OBTAINING CHATRIE'S LOCATION HISTORY RECORDS WAS LIKELY NOT A FOURTH AMENDMENT SEARCH OF HIS PAPERS.

The Fourth Amendment prohibits "unreasonable searches and seizures" of individuals' "persons, houses, papers, and effects." This section offers a way to understand that language, and it then analyzes two bases for claiming protection here: first, the virtual locker argument, and second, the *Carpenter* equilibrium-adjustment argument.

Ultimately, Chatrie likely lacked Fourth Amendment protection in the Location History records. The virtual locker argument is plausible in the abstract, but the factual record does not seem to support it sufficiently to meet Chatrie's burden of proof. The *Carpenter* equilibrium-adjustment argument should fail because Location History was a voluntary opt-in service that did not cause a significant shift in the government's investigative powers.

A) The Fourth Amendment Applies Equally to Physical Intrusion Into Protected Spaces and their Modern-Day Technological Counterparts.

There is a lot of doctrinal confusion about what counts as a "search" of an individual's "persons, houses, papers, and effects." At a basic level, you may wonder, what is the test? Is it about privacy? Property?

Something else? Is there one test, or two—and if there are two, how are they different?

The best way to think about this is that a "search" of "persons, houses, papers, and effects" is naturally answered in two ways. The first is the traditional test of actual physical intrusion. At the time of the Fourth Amendment's enactment, a "search" of a "house" would have been understood to mean physical entry into the house and rifling through things inside; a "seizure" of "papers" would have been understood to mean taking possession of those things to remove them. That was the context of the great cases that inspired the Fourth Amendment's enactment, and those were the words used in those decisions. *See, e.g., Entick v. Carrington*, 19 Howell's State Trials 1029 (1765) (under a general warrant, officers could not "search, seize, and carry away all the papers of the subject"); *Wilkes v. Wood*, 98 Eng. Rep. 489, 498 (1763) ("The defendants claimed a right, under precedents, to force persons houses, break open escrutores, seize their papers, &c. upon a general warrant[.]").

In the middle of the twentieth century, before *Katz v. United States*, 389 U.S. 347 (1967), the Court had settled on a bright-line rule for interpreting this traditional form of search: Unlicensed physical intrusion into a house, person, paper, or effect, "by even a fraction of an inch," is a search. *United States v. Silverman*, 365 U.S. 505, 512 (1961). This test is based not on property law, but rather on the mechanics of physical intrusion. *See id*. at 512 (noting that the test "does not turn upon the technicality of a trespass," but rather "an actual intrusion into a constitutionally protected area").

The physical intrusion test continues today in cases like *United States v. Jones*, 565 U.S. 400 (2012),

Florida v. Jardines, 569 U.S. 1 (2013), and *Grady v. North Carolina*, 575 U.S. 306 (2015) (per curiam). *See generally* Orin S. Kerr, *The Two Tests of Search Law: What is the* Jones *Test, and What Does That Say About* Katz*?*, 103 Wash. U. L. Rev. 309, 325-33 (2025) (hereinafter, *Two Tests of Search Law*).

The major question of Fourth Amendment law in the twentieth century was whether to recognize searches *beyond* the eighteenth-century facts of physical intrusion into enumerated areas. The problem was that new technologies allowed technological equivalents of physical intrusion without the actual intrusion occurring. *See Olmstead v. United States*, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting). As the Court eventually recognized, failing to recognize searches in the absence of physical intrusion would "permit police technology to erode the privacy guaranteed by the Fourth Amendment," reducing the Fourth Amendment to a nullity in an age of modern technological surveillance. *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (Scalia, J.).

The Court extended Fourth Amendment protection beyond physical intrusion in *Katz v. United States*. *See Katz*, 389 U.S. at 353 ("[T]he reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."). It came to phrase the test for searches outside physical intrusion using the language suggested by Justice Harlan's *Katz* concurrence. Justice Harlan summarized then-existing caselaw as holding that "electronic as well as physical intrusion" can be a search, and that a non-physical search occurred when it violated an "expectation of privacy . . . that society is prepared to recognize as 'reasonable.'" *Id.* at 360-61 (Harlan, J., concurring).

At first blush, Justice Harlan's "reasonable expectation of privacy" test sounds weird and even non-legal. But contrary to first impressions, the "reasonable expectation of privacy" test does not call on judges to ruminate about philosophy or import their policy preferences. When the *Katz* test is accurately understood in historical context, it merely identifies the technological equivalents of traditional physical searches—an inquiry necessary to ensure the Fourth Amendment retains its role in a technological age. *See Carpenter v. United States*, 585 U.S. 296, 305 (2018); *Kyllo*, 533 U.S. at 39.

Put another way, the *Katz* privacy test is just a way to identify what counts as a "search" of "persons, houses, papers, and effect" in our modern world of hidden bugging devices, thermal imaging, cell phone tracking, and Internet surveillance. It identifies "the modern-day technological equivalent of physical entry at the time of the founding." Orin S. Kerr, Katz *as Originalism*, 71 Duke L.J. 1047, 1064-65 (2022) (hereinafter, Katz *as Originalism*).

This history is important because it focuses the Court on the correct constitutional question. Geofencing plainly does not involve physical intrusion. The government does not break into Google and rifle through its servers. The proper question here is about technological equivalence. Is collecting Location History records a modern-day parallel to a physical intrusion into an individual's person, house, papers, or effects?

Under this approach, it is wrong to focus on technical questions of what infringed property rights or on broad abstractions about privacy. The pre-*Katz* test from *Silverman*, subsequently restored, wisely rejected property law and technical trespass doctrine as a guide. That test is only about physical intrusion,

which is not implicated by geofencing. *See Silverman*, 365 U.S. at 511-12; *Two Tests of Search Law* at 314-22.

Further, the *Katz* "reasonable expectation of privacy" test "is not a free-floating or circular standard" about privacy, "but rather a more specific idea rooted in Fourth Amendment history" that ensures that technological analogues to traditional physical intrusion are recognized under the Fourth Amendment. Katz *as Originalism* at 1057. Answering whether a search occurred here therefore should depend heavily on identifying analogies and equivalents to maintain the role of the Fourth Amendment in a world of new technology. *See also Kyllo*, 533 U.S. at 34 (use of a thermal imager without physical intrusion is a search to "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted").

B) Although Individuals Have Fourth Amendment Rights in Their Online Virtual Private Lockers, Chatrie Likely Lacked the Needed Control Over His Records.

Under the approach outlined above, there are two basic theories that might give Chatrie Fourth Amendment rights in his Location History records. The first theory is that the records collected were held for Chatrie in a virtual private locker. This is Chatrie's best argument for Fourth Amendment protection, and it is at least plausible. But I am not persuaded that the record supports it.

The argument in favor of protection starts as follows. When a person rents or borrows space for their own use from another, that space becomes a place where they can have Fourth Amendment rights. That

place might be a phone booth during a call, as in *Katz*; a hotel room, as in *Stoner v. California*, 376 U.S. 483 (1964); a piece of luggage stored on a bus, as in *Bond v. United States*, 584 U.S. 395 (2009); or a rental car, as in *Byrd v. United States*, 584 U.S. 395 (2018).

The same principle applies to sealed containers held by third parties, such as packages in the mail or storage lockers provided by a locker company. A person who sends a sealed package has rights in the contents of the package during transit, even though it is held by the post office. *See Ex Parte Jackson*, 96 U.S. 727, 733 (1878) (sealed letter); *United States v. Van Leeuwen*, 397 U.S. 249, 251 (1970) (sealed package). *Cf. Carpenter*, 585 U.S. at 399-400 (Gorsuch, J., dissenting) (suggesting that a bailment may create Fourth Amendment rights).

These principles apply equally to the digital world under *Katz*. If users remotely store their computer files with a third-party Internet provider, they ordinarily retain Fourth Amendment rights in the contents of those stored files. *See, e.g., Heidi Grp., Inc. v. Tex. Health & Human Servs. Comm'n*, 138 F.4th 920, 935 (5th Cir. 2025) (Oldham, J.) (files in a Dropbox account); *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) (stored emails). Digital files stored in an online virtual locker are just as constitutionally protected as physical items stored inside a physical locker.

So far, so good. The question is, do Location History records fit this framework? The issue is control. In cases on rented and borrowed spaces, rights are rooted in "lawful possession and control" over the space. *Byrd*, 584 U.S. at 407. Some company may own the space or thing, but users put what they want there and use it as their own private space. *See id*. Did Google users have enough control over their Location History

records so that they could be considered stored in a virtual private locker?

Chatrie has the burden of proof on this issue. *See Rakas v. Illinois*, 439 U.S. 128, 130 n.1 (1978). The record is surprisingly sparse on the details, as the virtual locker theory was not a focus of the proceedings below. The facts relied on by Chatrie appear to be found primarily in Google's amicus brief filed in the Fourth Circuit. *See* Pet. Br. at 15-16 (citing J.A. 19-20). Assuming that an appellate amicus brief can establish facts, I find Google's explanation likely insufficient to satisfy Chatrie's burden of proof.

According to Google, users could turn Location History on or off. They could view their Location History records, and they could also delete particular records. J.A. 18-20. But as I understand the record, that was it. Google's network generated the records and saved them on its servers. Users had no ability to store other records in Location History. Users could not redraw the records to change where Location History said their phone had been. Further, Google does not say how Google may have used the data: It was "primarily" for the user, Google says, J.A. 20, not explaining more. On the whole, this does not seem to be a virtual private locker where users controlled what contents were stored inside.

Chatrie makes the virtual private locker argument by invoking what it terms a "property" interest in records, relying on Google's privacy policy, pointing to statutory privacy laws, and by claiming that users had full control over Location History. Pet. Br. at 15-22.

As explained above, whether Chatrie had a property interest in the records is not the correct question. *See Silverman*, 365 U.S. at 511-12; *Jones v. United States*,

362 U.S. 257, 266-67 (1960). Google's privacy policy and statutory privacy laws are likewise irrelevant. The privacy policy does not matter because private contracts can neither extinguish nor create Fourth Amendment rights. *See* Orin S. Kerr, *Terms of Service and Fourth Amendment Rights*, 172 U. Pa. L. Rev. 287 (2024). Legislative privacy laws make no difference because, among other things, they do not reflect the judgments that are relevant to Fourth Amendment law. *See* Orin S. Kerr, *The Effect of Legislation on Fourth Amendment Protection*, 115 Mich. L. Rev. 1117 (2017).

The issue of control is the key one. On this question, we are all stuck trying to interpret Google's vague claim that users could "edit" Location History records. J.A. 16, 20. I *think* "edit" just means that users could delete particular records and not delete others, not that it could actually redraw what the data said. If so, Chatrie has not met his burden of establishing a virtual private locker. At the same time, if the Court interprets that word differently, it might lead to more support for Chatrie's argument.[2]

[2] The United States relies heavily on *United States v. Knotts*, 460 U.S. 276 (1983), reasoning that because the information revealed was ultimately about Chatrie's location in non-private spaces, there was no search. If the Court accepts the virtual private locker argument, however, *Knotts* is irrelevant. When applying the Fourth Amendment, it matters how the government obtained the information, not just what information was obtained. Breaking into a home to read the local newspaper left on the kitchen table is still a search, even though the newspaper is publicly available. *See Kyllo*, 533 U.S. at 35 n.2.

C) Chatrie Does Not Have Fourth Amendment Rights Under *Carpenter v. United States* Because He Voluntarily Opted to Turn On Location History.

A second argument for Fourth Amendment protection is based on *Carpenter v. United States*, 585 U.S. 296 (2018). In my view, this rationale does not support Fourth Amendment protection because Chatrie voluntarily opted in to have Google create and store Location History records.

First, some background. The relevant analogy here is not to documents stored in a private locker, but rather to sending communications to a third party. The basic principle is rooted in one of the Supreme Court's first Fourth Amendment decisions, *Ex Parte Jackson,* from 1878. Although sealed letters receive Fourth Amendment protection, Justice Field explained, sent materials that are "open to inspection, such as newspapers, magazines, pamphlets, and other printed matter, purposely left in a condition to be examined" do not. *Jackson*, 96 U.S. at 733.

In the twentieth century*, Ex Parte Jackson*'s notion that a person has no Fourth Amendment rights in what they knowingly expose to a third party was applied to speech to undercover agents, *see Hoffa v. United States*, 385 U.S. 293 (1966); account records provided to a bank, *see United States v. Miller*, 425 U.S. 435 (1976); and numbers dialed to place a telephone call, *see Smith v. Maryland*, 442 U.S. 735 (1979).

In 2018, however, the Court placed a limit on the third-party doctrine in *Carpenter*. Faced with the prospect that "mechanically applying" the doctrine would vastly expand government surveillance power given "seismic shifts in digital technology," 585 U.S. at

313-14, the Court limited the doctrine to prevent subjecting individuals to "tireless and absolute surveillance." *Id*. at 312. Thus, *Carpenter* was an example of what I have called "equilibrium adjustment," a recurring practice in which the Court adjusts Fourth Amendment doctrine to maintain the historical role of the Fourth Amendment in the face of dramatic technological change. *See generally* Orin Kerr, *The Digital Fourth Amendment: Privacy and Policing in Our Online World* 151-62 (2025).[3]

The question becomes how Location History records fit this framework: Are they covered by the traditional rule from *Ex Parte Jackson*, or are they covered by the equilibrium-adjustment exception in *Carpenter*? The answer depends on how you read *Carpenter*, something that has divided lower courts and academics alike.

My own understanding of *Carpenter* is that it does not apply when users voluntarily opt in to data collection. *See Digital Fourth Amendment* at 161-62. *Carpenter* prevents individuals from having to choose between "participation in modern society" and being subject to "absolute surveillance." *Carpenter*, 585 U.S. at 315, 312. If people for whatever reason wish for their cell phone provider to generate precise records of their whereabouts—not because the company needs it, but because the user turns that feature on for themselves—that is a choice that does not implicate the "seismic shifts in digital technology" that animated *Carpenter*.

As the government's brief explains, Chatrie had to take a series of steps to opt in to having Google create Location History records for him. *See* U.S. Br. at 23. It

---

[3] This Chapter is available online at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6312039.

is not entirely clear how many people decided to opt in, or what would have motivated them. The district court reported that "[a]pproximately one-third of all active Google users have Location History enabled on their accounts." *United States v. Chatrie*, 590 F. Supp. 3d 901, 909 (E.D. Va. 2022). It is not clear, however, what percentage of people have active Google accounts; if the percentage is domestic or global; or if it refers to accounts that were enabled generally or to phones used with it on (as was necessary to generate records).

Either way, turning Location History on was just an option, not an obligation. It's hard to know why people took this step. Some people may have found it a neat feature. Some may have assumed they would benefit from it somehow. Whatever the reason, people certainly didn't need to have Google create these records and store them on Google's servers. And as we know, Google no longer even supports its users doing so, as now the Location History records can be stored only on the user's phone.

The voluntary nature of Location History has potentially important practical consequences for its usefulness as an investigative tool in the time period when Google stored those records. To be blunt, Location History geofencing may have been mostly a dud. This is an exclusionary rule case, so it involves a successful investigation: The government found their bank robber. But that success appears to have been unusual. Although geofence warrants became a significant percentage of the warrants served on Google for a spell, *see* Zack Whittaker, *Google Says Geofence Warrants Make Up One-Quarter of all US Demands*, TechCrunch, August 19, 2021, there are surprisingly few prosecutions on the books that appear to involve evidence from geofence warrants.

What explains that? My impression is that Location History geofencing rarely worked. In cases where investigators obtained geofence warrants, the people who committed crimes generally had not taken all the steps to enable the feature on phones registered to them needed to make geofence warrants a consistently useful tool for investigators.

This is not in the record, so caution is warranted. But Mr. Richard Salgado, who helped create Google's geofence warrant policy and implemented it when he was Google's Director of Law Enforcement & Information Security, has stated publicly that successful investigations such as *Chatrie* were very uncommon. As Mr. Salgado wrote in an email to undersigned amicus, included with his permission, geofence warrants were not "much more than investigative lottery tickets." Email from Richard Salgado to Orin Kerr, March 23, 2026. According to Mr. Salgado, "many warrants were abandoned before reaching step 3 and the success stories are rare." *Id*.

If Mr. Salgado is right, geofencing for Location History records rarely helped investigators identify suspects. The service did not cause the seismic shift that triggers *Carpenter*.[4]

[4] This suggests that Chatrie would have had a significant basis for arguing that the warrant lacked probable cause entirely, as the odds of identifying the bank robber were low. We can imagine possible reasons why that argument went unmade: the success rate of geofencing was unknown; there is tension between arguing lack of probable cause and arguing in favor of finding a search under *Carpenter*; and the good-faith exception of *United States v. Leon,* 468 U.S. 897 (1984), makes probable cause defects exceedingly difficult to challenge.

D) The Court Should Not Rely on the Short-Term Nature of the Information, or the Anonymity at Early Stages, to Determine Whether There Was a Search.

The government largely argues that no search occurred because the records collected only covered a few hours in time and were at least initially anonymized. *See* U.S. Br. at 16-21. Although amicus generally agrees with the United States that no search occurred, these particular arguments do not provide a sound basis for decision.

The notion that a surveillance practice could be a non-search for a period of time, but then eventually become a search when undertaken long enough, has been called the "mosaic theory." *See generally* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311 (2012) (hereinafter, *Mosaic Theory*). As proposed, the mosaic theory would say that only a little surveillance is not a search even when a lot of it would be. *See id.* at 320-28. *Carpenter* left undecided whether this approach should be adopted, *see* 585 U.S. at 310 n.3, and lower courts have divided on whether to recognize it.

The Court should firmly reject the short-term/long-term distinction and the mosaic theory that animates it. Fifteen years of experience with the mosaic theory has shown that the principle is impossible to administer coherently. *See Digital Fourth Amendment* at 174-84. No one knows how much is too much, and how long is too long. Any proposed prophylactic line is readily gamed, triggering the need for additional prophylactic lines to honor the principle of the first one. For example, if the search line is triggered by obtaining one week of records, can the government get 6 days and 23 hours of records each time and then just

repeat that? Can they wait a week and try again? There are no obvious answers to these "vexing problems." *Jones*, 565 U.S. at 412.

Lower courts that have tried to implement the mosaic theory have created a we-know-it-when-we-see-it jurisprudence, in which appellate courts look back at the record and say whether they feel something search-like happened. *See Digital Fourth Amendment* at 180-84. In part, this is because the mosaic theory requires courts to answer a long list of unanswerable questions. *See Digital Fourth Amendment* at 174-77; *Mosaic Theory* at 328-53. But it is also explained by a more fundamental flaw: "The invasiveness of new facts always depends on what else we know. And this makes it exceedingly difficult to say when a mosaic exists." *Digital Fourth Amendment* at 178.

This Court has consistently rejected Fourth Amendment standards that "would launch courts on a difficult line-drawing expedition" and raise so many conceptual questions as to "keep defendants and judges guessing for years." *Riley v. California*, 573 U.S. 373, 401 (2014). *See, e.g., Kyllo*, 533 U.S. at 39; *New York v. Belton*, 453 U. S. 454, 458 (1981). The proposed short-term/long-term distinction deserves the same rejection.

The government's suggestion that obtaining anonymized records is not a search at Steps 1 and 2, *see* U.S. Br. at 18, should also be avoided. The focus on anonymity is also based on mosaic thinking, specifically that anonymized data does not provide enough information in context to seem like an invasion of privacy. But the proposed distinction falls apart on inspection, as records about an account can be easily linked to a name. *See Digital Fourth Amendment* at 177-80. As Justice Scalia emphasized in *Arizona v.*

Hicks, 480 U.S. 321, 325 (1987), "[a] search is a search, even if it happens to disclose nothing but the bottom of a turntable."

If a search occurred, it happened at Steps 1 and 2 (when records of geofencing were obtained) but not at Step 3 (when the government merely obtained unprotected account information).

II. THE WARRANT LIKELY SATISFIED THE WARRANT CLAUSE.

The Fourth Amendment permits geofence warrants. Further, the warrant was sufficiently narrowly drawn as to satisfy the particularity requirement as to Step 1. The harder question is whether Step 2 was constitutional.

A) The Fourth Amendment Permits a Sufficiently Narrow Warrant for Geofencing Records.

The Fourth Amendment states that every warrant must "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. Amend. IV. At the time of the Fourth Amendment's enactment, warrants were obtained only for physical items such as stolen goods. Back then, applications of the particularity requirement were "precise and clear." *Stanford v. Texas*, 379 U.S. 476, 481 (1965). First, the officer physically entered the place and searched it. Second, the officer found the person or thing and took it away, seizing it.

The modern extension of the Fourth Amendment beyond physical intrusion raises puzzles for how to draft warrants, however. The mechanics of the warrant process are often different. Some surveillance practice leads to certain data coming into the

government's possession. What is the "place" to be searched? What is the "thing" to be seized? And how narrow must the warrants be?

The Court encountered these questions before when it extended the Fourth Amendment to bugging practices in the 1960s and beeper tracking in the 1980s. The approach of those precedents is instructive, as they teach that a narrowly drawn geofence warrant can be constitutional.

The first case is *Berger v. New York*, 388 U.S. 41 (1967), which grappled with how to draft a warrant to bug a person's house with an audio-recording device. The defendant argued that no warrant "can be drawn so as to meet the Fourth Amendment's requirements" for bugging, given that a secret microphone indiscriminately swept up every conversation in the room. *Id*. at 63. The Court disagreed, reasoning that the Fourth Amendment "does not make the precincts of the home or the office . . . sanctuaries where the law can never reach[.]" *Id*.

Berger instead provided guidance on how to draft a warrant sufficiently tailored to allow bugging. The "thing to be seized" was the "conversations" collected, and particularity required narrowing restrictions on bugging warrants such time limits. *Id*. at 58-59. For example, surveillance had to stop after the information was found. *See id*. at 59-60. Also, renewals for additional bugging time required fresh probable cause. *See id.* at 59.

The Court returned to warrants for technological surveillance in *United States v. Karo*, 468 U.S. 705 (1984). *Karo* involved the secret use of battery-operated radio beepers that broadcast their location. In *United States v. Knotts*, 460 U.S. 276 (1983), the

Court had ruled that no search occurred when a beeper was secretly broadcasting its location out on public roads. *Karo* placed a limit on this holding, concluding that a search occurred when suspects brought the beeper inside a home. *See Karo*, 468 U.S. at 715-16.

As in *Berger*, however, a party in *Karo* argued that no warrant could be drafted for such indiscriminate surveillance. It was not possible to satisfy the particularity requirement for a warrant to use a beeper, the government argued, as the place to be searched was inherently unknown. Indeed, it was precisely that information that investigators were trying to obtain. *See id*. at 718.

Echoing *Berger*, *Karo* rejected the claim that no warrant could be drafted:

> It will still be possible to describe the object into which the beeper is to be placed, the circumstances that led agents to wish to install the beeper, and the length of time for which beeper surveillance is requested. In our view, this information will suffice to permit issuance of a warrant authorizing beeper installation and surveillance.

Id.

The takeaway from *Berger* and *Karo* is that extending the scope of Fourth Amendment protection to new surveillance practices does not simultaneously render those practices warrant-proof. The choice in surveillance law is not zero protection or absolute protection. Particularity limits the scope of surveillance rather than blocks it. "If a valid public interest justifies the intrusion contemplated," it must be possible "to issue a suitably restricted search warrant." *Camara v. Municipal Court*, 387 U.S. 523, 539 (1967).

The novel particularity problems of modern surveillance practices do not create "sanctuaries where the law can never reach." *Berger,* 388 U.S. at 63.[5]

The same principle has been adopted in the analogous setting of warrants for records of white-collar crimes. There, investigators must seize many records and look through them to "piec[e] together many bits of evidence." *Andresen v. Maryland*, 427 U.S. 463, 480 n.10 (1976). This reality does not make warrants to search through the records unlawful, the Court has stressed, as the particularity requirement "may not be used as a shield to avoid detection when the State has demonstrated probable cause[.]" *Id.*

Under these principles, it is possible to draft a particular warrant for geofencing records.

B) Geofence Warrants Are Not Inherently General Warrants.

Chatrie argues that geofence warrants are inherently general warrants because, in executing them, Google directed a scan through a massive database. Because Google scanned through records associated with millions of accounts to identify responsive records, Chatrie claims, any Location History warrant was inherently unconstitutional. *See* Pet. Br. at 34-36, 40-41. This argument echoes the Fifth Circuit's reasoning

---

[5] The Court has recognized one circumstance where even a valid warrant is not enough. *Winston v. Lee*, 470 U.S. 753 (1985), holds that "compelled surgical intrusion into an individual's body for evidence" can sometimes be unreasonable even with a warrant, a matter to be decided on a case-by-case basis. *Id*. at 760. *Lee* has no application here. Collecting records about the location of a cell phone does not implicate the "dignitary interests in personal privacy and bodily integrity" justifying that special rule. *Id*. at 761-62.

in *United States v. Smith*, 110 F.4th 817 (5th Cir. 2024), featured prominently in Chatrie's Petition for Certiorari.

The Court should reject Chatrie's argument and make clear that the Fifth Circuit's reasoning is invalid. As I have detailed, the Fourth Amendment implications of scanning through databases are defined by what the scan reveals in light of its filter setting, not the raw data that the filter scans through. *See* Orin S. Kerr, *Data Scanning and Fourth Amendment*, 67 B.C. L. Rev. 431 (2026) (hereinafter *Data Scanning*). "Courts should not be dazzled by the size of databases that are scanned through, but whose secrets are not exposed to human observation." *Id.* at 477.

When Google scanned through its location database for locations inside the geofence, the scanning through data outside the geofence that did not register a hit was not "searched" under the Fourth Amendment for the same reason a negative field test for drugs or absence of a dog's alert is not a search. No particular information could be revealed, as the fact that a phone somewhere on the planet was outside a particular geofence "reveals nothing of special interest." *United States v. Jacobsen,* 466 U.S. 109, 123 (1984) (negative field test for drugs). *See also Illinois v. Caballes*, 543 U.S. 405, 408 (2005) (dog that sniffs but does not alert).

This follows from the nature of scanning technology. A mechanistic computer scan through a database is merely a tool that checks for a match and moves on when no match occurs. *See Data Scanning* at 436-37. "A digital filter is dumb. It blindly checks for a match with the filter, much like a key to a door checks for a match with a lock." *Id*. at 459. The use of the scanning tool does not search all of the data scanned through any more than the attempted insertion of a key into a

lock sees the inside of the lock or what is behind the door. *See id.* at 466.

More broadly, a private company's decision to arrange its data so that finding a match requires checking large amounts of data for responsive records should not create a "shield" against a warrant any more than a company's arranging its paper documents so that many must be scanned through to find responsive records. *Andresen,* 427 U.S. at 480 n.10. "The size of the database searched is a matter of network design, not the scope of any privacy invasion." *Data Scanning* at 467.

Google could have designed its network differently, and it would have made no difference to the government—which presumably would not have even known about the difference. "[T]he Fourth Amendment should not regulate private company network administration decisions, nor hinge permitted government power on those private choices." *Id*. *See also Smith,* 442 U.S. at 744–45 ("We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.").

Further, the fact that geofence warrants reverse the typical process—instead of having a suspect and getting a warrant to learn more about them, these warrants go from a known crime to find a suspect—makes no difference. The Fifth Circuit found this fatal in *Smith*, concluding that "the quintessential problem with these warrants is that they *never* include a specific user to be identified[.]" 110 F.4th at 837. But the Fifth Circuit's view was soundly rejected by this Court in *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978), which allowed a warrant to search a college newspaper office for pictures taken by reporters

covering a student protest to identify the protesters. *See id*. at 555-63.

For these reasons, geofence warrants are not inherently general warrants. A sufficiently narrow geofence warrant satisfies the particularity requirement of the Fourth Amendment.[6]

C) Particularity Is Satisfied by a Geofence Warrant Sufficiently Limited in Time and Physical Space—Established Here as to Step 1.

The Fourth Amendment should be interpreted to impose two particularity limits on the scope of a geofence warrant: Time and physical space. Under this standard, Step 1 of the warrant satisfied the particularity requirement. The discussion below develops and applies these two requirements.

(1) The Time Limit

The first limit is time. To satisfy the particularity requirement, the warrant ordinarily should only cover records from a temporal window around the specific known crime. *Cf. Berger*, 388 U.S. at 58-60; *Karo*, 468 U.S. at 718.

Geofence warrants are particularly conducive to time limits. Like the warrants required in *Carpenter*, geofence warrants are retrospective. They look back at a past event when a known crime occurred, looking for location records from that window, creating an obvious limit on the scope of records. *See United States v. Ford*,

---

[6] Chatrie compares a warrant for location data with a warrant for contents of unknown accounts, suggesting that they must have the same constitutional implications. *See* Pet. Br. at 40. The latter raises very different constitutional concerns, however. *See Data Scanning* at 471-72.

184 F.3d 566, 576 (CA6 1999) ("Failure to limit broad descriptive terms [in warrants for documents] by relevant dates, when such dates are available to the police, will render a warrant overbroad.").

This does not mean the time period should be limited to the exact moment of the crime. Geofence warrants attempt to identify a suspect and any co-conspirators. Those individuals may be present at the scene for a spell before the crime, may act in concert shortly after, and then may depart. Obtaining records that paint a collective picture of entry onto the scene, presence, and then departure can help identify those involved in a way that particularity should encompass. *Cf. Messerschmidt v. Millender*, 565 U.S. 535, 552 (2012).

The time window of the warrant here satisfies that standard. The government was investigating a bank robbery in a rural area. Geofencing could show the suspect and co-conspirators arriving at the scene, coordinating, and leaving. A time period of an hour or two around that time is a reasonable window.

(2) The Spatial Limit at Step 1

The second limit should be the coverage of the geofence in physical space. The traditional physical concept of geographic coverage is the most sensible standard because geofencing records are fundamentally about a device's location. The records report the physical place where particular devices were reported to be.

Because physical location is what matters, limiting the geofence by physical area matches the scale of the surveillance in the same way that time does. *Cf. Karo*,

468 U.S. at 714-15 (concluding that although use of a radio beeper that reveals its public location on public roads is not a search, use of a beeper to reveal its location in the home is a search). Much like a warrant for physical entry into a space, the size of the space to be searched determines the scope of the search allowed.

The scope of the geofence warrant at Step 1, which picked up the phones within a 150-meter radius around the bank, satisfies this standard. When a bank robbery is committed, it is to be expected that the robber came from somewhere, committed the robbery at the known time, and then fled after. Co-conspirators would be expected to so something similar in the general area, such as waiting in a getaway car nearby. A 150-meter radius is sufficient to flag which of the phones exhibited movement characteristic of involvement in the crime, and is therefore a proper spatial limit. *See Camara,* 387 U.S. at 539 (approving "area" safety inspection warrants as sufficiently particular).

D) Chatrie's Contrary Arguments About Particularity at Step 1 are Unpersuasive.

Chatrie makes two arguments against this conclusion. First, Chatrie argues that the place that a warrant must search is a particular account, and that it is invalid for the government to get a warrant to search for information about multiple accounts. *See* Pet. Br. at 37-41, 45-49. In effect, Chatrie treats each piece of responsive data as information from inside a distinct virtual house associated with a distinct device, limiting each warrant to one virtual account house.

This does not work for three reasons. First, it fails as a matter of precedent. *Karo's* reasoning was not

that a new and different beeper warrant was required each time the beeper entered a different home. Rather, *Karo* approved a beeper warrant to be used for a period of time to report back on the beeper's location inside any private place the beeper happened to go during that period. *See, e.g., United States v. Burnett*, No. 12-CR-00042, 2013 WL 12430549, at *4 (D.D.C. 2013) (tracking warrant allowed tracking in multiple protected locations).

Second, as a matter of technology, the location data here was held by Google. Even if the Court concludes that the data is protected under a virtual private locker theory, it is a fiction that each item of data was 'inside' an associated account, such that Google was 'entering' different accounts as it scanned through the database. The scanning through Google's database could only reveal what phones were present in a physical area. *See Data Scanning* at 464-65.

Third, the entire purpose of a geofence warrant is to go from a known crime to a particular account. If a warrant is needed to take that step, it should be possible under the warrant clause to take it. Otherwise, the database would create "sanctuaries where the law can never reach," an approach the Court has rejected. *Berger,* 388 U.S. at 63. *See also Andresen*, 427 U.S. at 480 n.10.

Next, Chatrie argues that the warrant was overbroad because it did not establish probable cause for each individual phone revealed to be in the geofence. *See* Pet. Br. at 49-51. Chatrie draws this reasoning from *Ybarra v. Illinois*, 444 U.S. 85 (1979), in which the Court created a special rule for physical searches of people when a warrant is executed. When executing a search warrant at a place with many people inside, *Ybarra* held, the government cannot physically search the people inside unless there is

probable cause that each person to be searched is involved in the crime. *See id.* at 91-92.

But this is irrelevant. *Ybarra* created a special rule governing physical searches of people at the place where a search occurs. *See id*. But when the government obtains geofence records, it merely collects records about the location of phones. No person is physically searched, so *Ybarra* does not apply. Learning that a particular phone is within the area of the geofence is much like the officers entering the bar in *Ybarra* and seeing the particular customers there. Both are permitted by the warrant that is sufficiently narrow as to its physical area.

E) The Constitutionality of the Warrant at Step 2 Is Unclear.

Although Step 1 of the warrant was constitutional, Step 2 of the warrant process raises two separate concerns.

The first concern is the multi-step procedure itself. Created by Google, the process seems to assume a several-stage process of negotiation between Google and investigators as to what additional records to seek and which records to obtain at three different points. Google's process effectively required investigators to seek multi-stage warrants and placed magistrate judges in the position of signing them—turning Google's corporate policy into a judicial order.[7] The

[7] In theory, governments could have challenged Google's process by obtaining a non-compliant warrant—or an order under the Stored Communications Act—and challenging Google's failure to comply. But this would have been difficult. Investigators generally aim to solve cases quickly, not to pause investigations for several years to litigate warrant procedures. Also, state governments that obtained most geofence warrants

multi-stage process was plainly created in good faith and for a commendable reason: to protect privacy by reducing how much investigators learn about innocent persons present.

With that said, it is not clear that the Fourth Amendment permits multi-stage warrants. Warrant execution is normally up to the government, not the magistrate judge. As stated in *Dalia v. United States*, 441 U.S. 238, 257 (1979), "it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant," subject to a general rule of reasonableness. Magistrate judges are not supposed to manage the process ex ante. *See, e.g., United States v. Grubbs*, 547 U.S. 90, 97-99 (2006) (Scalia, J.); *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 327 (1979).

The better and more constitutional path may have been to only have a single-stage geofence warrant procedure—just get all the location information in the geofence at once—and to deal with the problem of information relating to innocent persons by imposing use restrictions that amicus has argued the Fourth Amendment requires on non-responsive data collected by digital warrants. *See generally* Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex. Tech L. Rev. 1 (2015).

If the Court does not share these concerns about the multi-step nature of the warrant process, there is the additional question of whether the warrant was

---

may have lacked authorities to compel Google's assistance. *Compare United States v. New York Telephone Co*., 434 U.S. 159, 171-78 (1977). It appears that, as a practical matter, Google could direct investigators to follow its procedure.

particular at Step 2. In particular, it's possible that extending the spatial area of the phones spotted at Step 1 is problematic. It's a novel question: When the government obtained the location of the phones from within the geofence for one hour (from Step 1), and then learned where some of those phones had been even outside the geofence for two hours (at Step 2), do you consider that just a slight expansion from the initial scope at Step 1? Or is that a major expansion, as now it tells you the location of those phones in *any location* for that two-hour window? Broadening the time from one hour to two hours seems only a small change, but it is unclear what to make of the particularity question as to physical areas at Step 2.

With that said, it is not clear that Chatrie has made this argument in his discussion of Steps 2 and 3, *see* Pet. Br. at 52-55, so perhaps it is waived.

CONCLUSION

It is likely that no search occurred, although it depends on how the Court construes the record on the virtual locker question. It is also likely that the warrant was constitutional, although it depends on how the Court construes Step 2 and whether that issue was waived.

Respectfully submitted,

ORIN S. KERR
Counsel of Record
559 Nathan Abbott Way
Stanford CA 94305
(650) 498-8125
orin@orinkerr.com

April 1, 2026