**No. 22-4489**

# In the United States Court of Appeals for the Fourth Circuit

UNITED STATES OF AMERICA,

*Plaintiff-Appellee*,

v.

OKELLO T. CHATRIE,

*Defendant-Appellant*.

On Remand from the
United States Supreme Court
No. 25-112

## BRIEF OF PROJECT FOR PRIVACY & SURVEILLANCE ACCOUNTABILITY, INC. AS *AMICUS CURIAE* SUPPORTING DEFENDANT-APPELLANT AND REVERSAL

Gene C. Schaerr
Erik S. Jaffe
Justin A. Miller
SCHAERR | JAFFE LLP
1717 K Street NW, Suite 900
Washington, DC 20006
Telephone: (202) 787-1060
gschaerr@schaerr-jaffe.com

*Counsel for Amicus Curiae*

SEPTEMBER 8, 2026

## STATEMENT REGARDING ORAL ARGUMENT

*Amicus* Project for Privacy and Surveillance Accountability, Inc. respectfully asks that this Court allow it to participate at oral argument, where it could develop the principles set forth in this brief and further explain why this warrant reproduces the Founding-era general-warrant defect by using each search to select the accounts the next search would reach.

## TABLE OF CONTENTS

STATEMENT REGARDING ORAL ARGUMENT ..... i

TABLE OF AUTHORITIES ..... iii

INTRODUCTION, INTEREST, AND SOURCE OF AUTHORITY OF *AMICUS CURIAE* ..... 1

SUMMARY OF ARGUMENT ..... 3

ARGUMENT ..... 5

I. The Warrant Clause Requires the Warrant—Not the Results of Its Execution—to Identify the Object and Scope of the Search in Advance. ..... 5

A. General warrants unconstitutionally leave the choice of the places to be searched to the executing officer. ..... 5

B. Modern particularity doctrine keeps that choice with the magistrate ..... 6

II. The Original Meaning of the Warrant Clause Forbids Using a Search to Identify Its Own Targets ..... 8

A. A geofence warrant inverts the ordinary rule that the object of the search is described by the warrant, not discovered during the search. ..... 8

B. Broad investigation is not a broad search of protected records. ..... 10

C. Narrowing and anonymization after acquisition cannot supply the particularity the warrant lacked ..... 12

III. This Warrant Used Each Search to Determine the Accounts the Next Search Would Reach. ..... 13

CONCLUSION ..... 15

CERTIFICATE OF COMPLIANCE ..... 17

## TABLE OF AUTHORITIES

**Cases** **Page(s)**

*Groh v. Ramirez*,
540 U.S. 551 (2004) ..... 7, 12

*Kentucky v. King*,
563 U.S. 452 (2011) ..... 1

*Lo-Ji Sales, Inc. v. New York*,
442 U.S. 319 (1979) ..... 7

*Marron v. United States*,
275 U.S. 192 (1927) ..... 3, 7

*Maryland v. Garrison*,
480 U.S. 79 (1987) ..... 8

*Owens ex rel. Owens v. Lott*,
372 F.3d 267 (4th Cir. 2004) ..... 11, 14

*Schmidt v. City of Norfolk*,
No. 26-1227 (4th Cir.) ..... 3

*Stanford v. Texas*,
379 U.S. 476 (1965) ..... 6, 10

*Steagald v. United States*,
451 U.S. 204 (1981) ..... 6

*United States v. Di Re*,
332 U.S. 581 (1948) ..... 12

*United States v. Smith*,
110 F.4th 817 (5th Cir. 2024) ..... 13

*United States v. Zelaya-Veliz*,
94 F.4th 321 (4th Cir. 2024) ..... 9

*Ybarra v. Illinois*,
444 U.S. 85 (1979) ..... 11, 14

*Zurcher v. Stanford Daily*,
436 U.S. 547 (1978) ..... 11

**Rules**

Fed. R. App. P. 29 ..... 1

Fed. R. Crim. P. 41 ..... 9

## INTRODUCTION, INTEREST, AND SOURCE OF AUTHORITY OF *AMICUS CURIAE*[1]

The Supreme Court has decided that government officers conducted a Fourth Amendment search when they used a geofence warrant to acquire Chatrie's location history from a third-party provider, leaving a single question for remand: Was the search warrant here reasonable, meaning that "each of its steps was properly described with particularity and found to be supported by probable cause[?]" *Chatrie v. United States*, 146 S.Ct. 2193, 2199–200 (2026).

The answer is "no" because this warrant reverses a basic command of the Warrant Clause. A search for evidence of crime is reasonable only where "probable cause is properly established and the scope of the authorized search is set out with particularity." *Kentucky v. King*, 563 U.S. 452, 459 (2011); *see Chatrie*, 146 S.Ct. at 2215. This warrant fails at each step because the warrant—not the officer, and not the search itself—must identify the object of the search before the search begins.

---

[1] The parties consented to *Amicus* filing a brief. *See* Fed. R. App. P. 29(a)(2). No party or their counsel authored this brief in whole or part. No entity or person, aside from *Amicus,* its members, or its counsel, made any monetary contribution intended to fund this brief's preparation or submission.

*Chatrie*, 146 S.Ct. at 2216. That object, in the digital context, includes the account or repository whose protected records the government will acquire. Once a warrant describes that location with particularity, officers executing the warrant may determine which items within it are evidence. But the Constitution forbids the reverse. An indiscriminate dragnet search can neither supply the particularity that identifies the object of the search nor the probable cause that justifies searching that particular object.

For these reasons, a geofence warrant reverses the ordinary constitutional sequence. An ordinary investigation moves from suspicion to probable cause, to a warrant describing a particular place, and then to a search of that place. But the geofence process runs in the opposite direction. The government first compels Google to apply specified criteria to its Location History database, then acquires—and thereby searches—users' protected records returned by those criteria. And finally, it uses those records to select accounts for further searches. Probable cause does not precede the search and direct it; instead, the search results backfill a justification that the Constitution requires beforehand.

The Project for Privacy and Surveillance Accountability, Inc. ("PPSA"), a nonprofit, nonpartisan organization dedicated to protecting Americans' privacy against unwarranted government surveillance, has a particular interest in the resolution of the issue presented. PPSA studies and litigates the application of the Fourth Amendment to new investigative technologies, and it submits this brief to offer the Court a single, narrow principle that resolves the question left open on remand: A magistrate must fix the object and permissible scope of the search *before* execution begins. Particularity must be satisfied *ex ante*, not through *post hoc* narrowing. This principle also resolves many questions regarding other emerging technologies, such as the license-plate reader case scheduled for oral argument the same week as this case. *See Schmidt v. City of Norfolk*, No. 26-1227 (4th Cir.).

## SUMMARY OF ARGUMENT

The Warrant Clause reserves to a neutral magistrate the antecedent choice of where the government may search. Even a warrant that precisely describes an offense and is supported by probable cause remains a general warrant if it allows officers to select which places to search. *Marron v. United States*, 275 U.S. 192, 196 (1927). For that

reason, this warrant is defective: It specifies time and general geography but leaves to the executing officer the choice of which protected accounts within those bounds to acquire.

Nor does precision about *how* a search is conducted provide the necessary particularity about *which* account may be searched. Officers may sort evidence within a home or account that the warrant identifies beforehand; they may not use a dragnet search of protected records to select the accounts to be further searched. Because a search has occurred, at the latest, when the government acquires the data, later narrowing, anonymization, or a small return cannot supply the particularity missing at the outset.

This warrant followed exactly that forbidden sequence. At Step 1, the government acquired—and thereby searched—the location history of the users the geofence returned, without probable cause particular to any of them; Step 2 used those returns to select accounts for a broader search; and Step 3 identified accounts the earlier searches had selected. Each non-particularized search thus generated the narrower objects of the next search, rather than executing a warrant that had identified the

particularized object beforehand. That general-warrant structure is forbidden by the Fourth Amendment.

## ARGUMENT

This warrant fails for a straightforward reason: It reversed the sequence the Warrant Clause requires. A magistrate must fix the object and permissible scope of the search *before* execution begins. Here, the geofence warrant reverses that constitutional sequence by using each non-particularized acquisition to select the accounts for the next search.

### I. The Warrant Clause Requires the Warrant—Not the Results of Its Execution—to Identify the Object and Scope of the Search in Advance.

Two principles establish that a warrant must particularly describe the object and permissible scope of the search before execution begins: The Fourth Amendment's general-warrant prohibition and its modern particularity doctrine, each of which reserves the antecedent choice of where to search to the magistrate rather than the police.

#### A. General warrants unconstitutionally leave the choice of the places to be searched to the executing officer.

The Fourth Amendment was adopted to remedy the evil of general warrants and writs of assistance that gave executing officers vast discretion. Historically, the general warrant "specified only an offense . . .

and left to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched," while writs of assistance "noted only the object of the search . . . and thus left customs officials completely free to search any place where they believed such goods might be." *Steagald v. United States*, 451 U.S. 204, 220 (1981). Officials armed with this discretion "set forth in quest of unknown offenders," holding "in their hands the liberty of every man whom they were pleased to suspect." *Stanford v. Texas*, 379 U.S. 476, 483 (1965).

The Founders' objection to general warrants and writs was not merely their sweeping scope; it was who decided where the government would search. *See Stanford*, 379 U.S. at 481; *Steagald*, 451 U.S. at 220. The warrant or writ identified an offense while leaving the officer to choose the places to be searched and objects to be seized. A warrant could thus be specific about the crime and still be a general warrant, because the officer—not the magistrate—selected the targets during execution. *See Steagald*, 451 U.S. at 220.

### B. Modern particularity doctrine keeps that choice with the magistrate.

The Fourth Amendment reverses the overbroad discretion of general warrants and writs of assistance. It requires the warrant itself

to describe particularly the place to be searched and the persons or things to be seized, so that a neutral magistrate—not the officer in the field—determines the warrant's scope in advance. The Fourth Amendment's particularity requirement thus "makes general searches . . . impossible" precisely because, as to the place and object of the search, "nothing is left to the discretion of the officer executing the warrant." *Marron*, 275 U.S. at 196.

The requirement also operates *ex ante*: the Fourth Amendment does not "countenance open-ended warrants, to be completed while a search is being conducted." *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 325 (1979). And the limits must appear in the warrant itself: "The Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents." *Groh v. Ramirez*, 540 U.S. 551, 557 (2004). An officer's own restraint is no substitute, because "the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer." *Id.* at 561.

To be sure, requiring the magistrate to make the antecedent choice does not freeze execution in place. Officers reasonably executing a valid warrant may respond to facts learned during execution. But later-

discovered facts cannot cure a warrant that was invalid when issued. *Maryland v. Garrison*, 480 U.S. 79, 85–89 (1987). The distinction therefore is between adjusting the execution of a search already validly authorized and using execution to supply the information necessary to authorize the search itself. *See id.* at 87 n.13. The Fourth Amendment allows the first but not the second.

## II. The Original Meaning of the Warrant Clause Forbids Using a Search to Identify Its Own Targets.

Applying these principles here, the geofence warrant in this case violated the Warrant Clause in three related ways. It improperly used a search's execution to select the accounts to be searched; used protected records to develop the cause ordinarily developed through investigation; and relied on post-acquisition narrowing to supply the needed particularity missing at the outset.

### A. A geofence warrant inverts the ordinary rule that the object of the search is described by the warrant, not discovered during the search.

Ordinary warrant execution finds evidence within a place or account the warrant already identifies. In the digital context, an account is the repository to be searched, and responsive records are the things sought within it. Thus, a warrant for digital records must particularly

describe the account or repository whose protected records the government may acquire. Such a warrant need not predict what the search will reveal; but it must particularly identify where the government may search.

A geofence warrant inverts that rule. The problem is not the use of a filter *per se*, but what work the filter performs. Officers may use filters within an account or repository the warrant has already identified to determine which materials fall within the warrant. But here the government acquired—and thereby searched—the location history of the users returned by the geofence, then used those results to determine which accounts would be searched next. The filter thus helped select the objects of later searches rather than merely identify evidence within an object the warrant had already described.

Rule 41's two-step process confirms the distinction. Officers may copy electronically stored information and later review it for responsive material. *See* Fed. R. Crim. P. 41(e)(2)(B); *United States v. Zelaya-Veliz*, 94 F.4th 321, 338 (4th Cir. 2024). But that process determines what may be seized within a repository that the warrant has already identified; it does not determine which repository may be searched. Here, the opposite

occurred: The government used records acquired at one stage to select the accounts subjected to the next search.

Nor can the government use geographic precision to answer the constitutional problem. Like a warrant naming only a particular neighborhood rather than a specific home, a warrant for electronic records could describe an offense precisely and still be a general warrant because it left the executing officer to choose the particular objects to be seized and houses to be searched. For that reason, the warrant in *Stanford* was a general warrant, even if it "sufficiently specified the offense . . . and was issued upon probable cause," because it still did not particularly describe the things to be seized. *Stanford*, 379 U.S. at 480–81. So too here. The government's precision goes to selecting accounts it has already acquired. The Warrant Clause requires the warrant to identify the search's *object* with particularity.

### B. Broad investigation is not a broad search of protected records.

True, investigations often begin without a suspect. And when they do, police lawfully may canvass neighborhoods, interview witnesses, and review public evidence to develop a suspect, because none of those methods are Fourth Amendment searches. After *Chatrie,* however, the

government's acquisition of protected location history *is* a search. *See Chatrie*, 146 S.Ct. at 2215. Thus, police may investigate public digital records to determine whom they have cause to search. But they may not search protected records to determine whom they have cause to search.

The probable-cause problem is distinct. Mere proximity to "suspected … criminal activity," does not establish probable cause to search a person's protected records. *See Ybarra v. Illinois*, 444 U.S. 85, 91 (1979); *Owens ex rel. Owens v. Lott*, 372 F.3d 267, 276–77 (4th Cir. 2004).

The Supreme Court's decision in *Zurcher v. Stanford Daily*, 436 U.S. 547, 554–55 (1978) is different. That case concerned a search, pursuant to a warrant, for evidence located in a discrete place owned by a third party, not a search of each person's protected records. *Id.* But here the government acquires each returned user's own protected record of movements. The relevant question is therefore whether cause existed to search those protected records, not merely whether a crime occurred somewhere within the geofence.

This constitutional objection leaves ordinary investigation and targeted digital warrants untouched. It forbids only using a search of

protected records to supply the particularity required before the search. And it does not prevent evidence lawfully discovered during a valid search from generating new probable cause. It forbids the reverse: An unjustified search cannot validate itself through what it turns up. Nor can that search supply the particularity or probable cause for a further search whose object the warrant never independently described. Such information would be fruit of a poisoned tree.

### C. Narrowing and anonymization after acquisition cannot supply the particularity the warrant lacked.

Nor can post-acquisition restraint cure missing particularity. Here, the fact that the government's process returned nineteen accounts, narrowed them to nine and then three, and initially anonymized them cannot supply the antecedent description the warrant omitted. *See Groh*, 540 U.S. at 561 (magistrate, not police, imposes restraints).

Put simply, the government's narrowing and anonymization arguments fail because a search "is good or bad when it starts," and whether something is a search does not depend on "what it turns up." *United States v. Di Re*, 332 U.S. 581, 595 (1948). A tailored set of results is not a tailored search. And, as the Fifth Circuit observed, narrow results do not make the underlying search narrow. *United States v. Smith*, 110

F.4th 817, 837–38 (5th Cir. 2024). If the warrant did not describe the accounts the government could acquire, later restraint cannot describe them retroactively—and that is doubly true where the narrowing was performed not by a magistrate but during execution.

Anonymization is no different. It limits what the government sees, but does not satisfy the Warrant Clause by identifying, in advance, whose records may be searched. Because the Fourth Amendment search occurs, at latest, when the government acquires the protected location history—not later, when police attach a name to those records—anonymity at the moment of acquisition fails to supply the constitutionally required particularity. *See Chatrie*, 146 S.Ct. at 2214–15.

## III. This Warrant Used Each Search to Determine the Accounts the Next Search Would Reach.

This same structural problem ties together the defects in all three steps of the search at issue here: Each search supplied the accounts the next search would reach.

**Step 1.** The warrant described a 150-meter radius that swept in a neighboring church and its parking lot, and a one-hour window on a weekday afternoon. Appellant's Suppl. Br. 8, 24. But it identified no account—and at that time the government lacked probable cause to

search any particular user's Location History. *Id.* at 7; *see Ybarra*, 444 U.S. at 90–91; *Owens*, 372 F.3d at 276–77. The government then acquired—and thereby searched—the location history of the nineteen users the geofence returned. Those searches supplied the pool from which officers selected the Step 2 accounts.

**Step 2.** The warrant then let officers select, from the Step 1 returns, a subset of accounts for a broader acquisition of data—two additional hours of location history, reaching outside the geofence and into private residences, a school, and a hospital. Appellant's Suppl. Br. 25. The warrant did not describe those accounts; officers selected them from Step 1's returns. The Step 1 searches thus supplied the accounts subjected to the Step 2 searches.

**Step 3.** The warrant finally allowed officers to obtain subscriber identifying information for three of the remaining accounts, including Appellant's. *Id.* at 8, 28. As to how officers would choose, the warrant "said very little," directing only that they would "attempt to narrow down the list." *Chatrie*, 146 S.Ct. at 2215–16. Again, the warrant did not identify those accounts beforehand; the earlier searches did.

The defect here, then, is not the warrant's use of multiple stages, but its failure to supply constitutionally adequate particularity and probable cause for the returned users' protected records, and for selecting the accounts subjected to the later searches. At Step 1, the government acquired protected location history without probable cause particular to any returned user. At Steps 2 and 3, the warrant left officers to select from the earlier returns the accounts subjected to further searches. Each stage thus supplied information used to determine the accounts the next search would reach. The process thus *generated* its own objects instead of simply executing a warrant that had described them. After *Chatrie,* the Warrant Clause requires the opposite sequence.

## CONCLUSION

The Fourth Amendment permits police to investigate until they have probable cause to search a particular place or account and seize a particular object. It does not permit them to search protected records to determine whom they have cause to search. Because this warrant used each search to select the accounts the next search would reach, it violated the Warrant Clause, and the judgment should be reversed.

Dated: September 8, 2026

Respectfully submitted,

*/s/ Gene C. Schaerr*

Gene C. Schaerr
Erik S. Jaffe
Justin A. Miller
SCHAERR | JAFFE LLP
1717 K Street NW, Suite 900
Washington, DC 20006
Telephone: (202) 787-1060
gschaerr@schaerr-jaffe.com

*Counsel for Amicus Curiae*

## CERTIFICATE OF COMPLIANCE

The foregoing Brief of Project for Privacy & Surveillance Accountability, Inc., as *Amicus Curiae* Supporting Defendant-Appellant and Reversal complies with this Court's supplemental briefing order, because, excluding the parts of the document exempted by Fed. R. App. P. 32(f), this document does not exceed 15 pages.

This brief also complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Century Schoolbook font.

*/s/ Gene C. Schaerr*
Gene C. Schaerr

Dated: September 8, 2026