No. 25-112

In the Supreme Court of the United States

OKELLO CHATRIE,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

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

BRIEF OF THE CATO INSTITUTE AS *AMICUS CURIAE* IN SUPPORT OF PETITIONER

Matthew P. Cavedon
Counsel of Record
Brent Skorup
Laura A. Bondank
CATO INSTITUTE
1000 Mass. Ave., N.W.
Washington, DC 20001
(706) 309-2859
mcavedon@cato.org

Dated: March 2, 2026

QUESTION PRESENTED

Whether the execution of the geofence warrant violated the Fourth Amendment.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTEREST OF *AMICUS CURIAE*[1]

The Cato Institute is a nonpartisan public policy research foundation founded in 1977 and dedicated to advancing the principles of individual liberty, free markets, and limited government. Cato's Project on Criminal Justice was founded in 1999 and focuses on the scope of substantive criminal liability, the proper and effective role of police in their communities, the protection of constitutional and statutory safeguards for criminal suspects and defendants, citizen participation in the criminal justice system, and accountability for law enforcement officers.

Cato's interest in this case arises from its mission to support the rights that the Constitution guarantees to all citizens. *Amicus* has a particular interest in this case as it concerns the continuing vitality of the Fourth Amendment and meaningful restraints on the exercise of government power.

[1] Rule 37 statement: No part of this brief was authored by any party's counsel, and no person or entity other than *amicus* funded its preparation or submission.

SUMMARY OF ARGUMENT

In May 2019, a gunman robbed the Call Federal Credit Union in Midlothian, Virginia. After investigations stalled, law enforcement secured a "geofence warrant" directing Google to produce Location History records for every device within a 300-meter diameter of the bank. Pet. Opening Br. 8. The ensuing process followed Google's internal procedure for processing geofence requests. *Id.*

At Step 1, Google provided anonymized Location History information for all devices within the geofence for the 30 minutes before and 30 minutes after the robbery. *Id.* at 8. This yielded records of 19 Google users. *Id*. at 9. Law enforcement reviewed those records, and then, at their discretion, proceeded to Step 2. *Id.* At Step 2, law enforcement narrowed their focus to nine accounts from Step 1 and demanded records of those users' movements over a two-hour period, both inside and outside of the initial geofenced area. *Id.* After reviewing those users' movements, law enforcement proceeded to Step 3. They again narrowed their focus and requested from Google identifying information about three users. *Id.* One of the users identified in this final step was Petitioner Okello Chatrie.

After obtaining his Location History records and identifying information from Google, the government indicted Chatrie on robbery and firearms charges. *Id.* at 9. He moved to suppress his Location History records, arguing that the geofence warrant violated his Fourth Amendment rights. *Id.* The district court concluded that the warrant may have violated the Fourth Amendment but declined to suppress the evidence under the good-faith exception. *Id.* at 9–10.

A divided Fourth Circuit panel affirmed on different grounds, with the majority holding that—despite the multiple rounds of review of Google users' Location History records—no search occurred, reasoning that Chatrie had voluntarily exposed his Location History to Google under the third-party doctrine. *Id.* at 10. Following rehearing en banc, the Fourth Circuit affirmed again—this time in a single-sentence *per curiam* opinion. *Id.* However, the court divided 7-7 on whether a Fourth Amendment search had occurred, resulting in, as one judge put it, "a labyrinth of . . . nine . . . advisory opinions." *United States v. Chatrie*, 136 F.4th 100, 108 (2025) (en banc) (Diaz, C.J., concurring).

Lower courts are plainly struggling to apply the Fourth Amendment in this context. *Amicus* writes separately to emphasize three areas in which guidance from this Court is urgently needed in cases involving digital records.

First, in determining whether a search occurred, the panel relied solely on *Katz v. United States*, 389 U.S. 347 (1967), and the reasonable-expectation-of-privacy test. This Court should instruct lower courts that their first duty is to rigorously apply the original public meaning of "search." A "search" occurs when the government undertakes an investigatory act designed to reveal private information. That is precisely what the government did at each step of this geofence process.

Second, in applying *Katz*, many judges below tersely dismissed the notion that Chatrie had a property interest in his Location History records. Yet under state law and Google's user agreements, Chatrie may own his Location History records. Property rights lie at the heart of the Fourth Amendment, and they do

not dissolve merely because one's records are stored by a third party.

Finally, this Court should clarify that in cases like this—where information is disclosed in multiple stages—each step constitutes a new search. Each step yields new records and new information and therefore requires separate review and authorization by a neutral magistrate. Warrants issued to technology companies for users' records—to build leads and suspect lists—are rapidly becoming an important tool for law enforcement. If a single warrant can authorize successive and increasingly invasive searches of millions of people's digital records, the Fourth Amendment's guarantee to be secure in our "persons, houses, papers, and effects, against unreasonable searches and seizures" will be rendered hollow.

After clarifying these issues, this Court should reverse the judgment below.

ARGUMENT

I. THIS COURT SHOULD CLARIFY THAT EXAMINING OR INSPECTING A PERSON'S DIGITAL RECORDS IS A SEARCH.

The Fourth Amendment protects the people's right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. Yet since Justice Harlan's concurrence in *Katz v. United States*, lower courts have reflexively turned to the "*Katz* test," asking whether an individual had a "reasonable expectation of privacy" in the place or thing examined. That inquiry often devolves into an abstract balancing of privacy interests. As this Court observed in *Kyllo*, the result can be counterintuitive—under *Katz*, at times "a search is

not a search" for purposes of the Fourth Amendment. *Kyllo v. United States*, 533 U.S. 27, 32 (2001).

This Court should instruct lower courts to begin not with *Katz*, but with the original public meaning of "search." The Constitution's meaning is anchored in the ordinary understanding of its terms at the time of adoption. *See* Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1185 (2016). At the Founding—and today—to "search" meant "'[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as to *search* the house for a book; to *search* the wood for a thief.'" *Kyllo*, 533 U.S. at 32 n.1 (citing N. WEBSTER, AN AMERICAN DICTIONARY OF THE ENGLISH LANGUAGE 66 (1828) (reprint 6th ed. 1989)).

Thus in common parlance and understanding—an understanding shared by the Founders—an investigatory act carried out with the purpose of revealing private information is a *search*.

This common understanding of the word "search" can be traced back to English common law. In *Entick v. Carrington*, 95 Eng. Rep. 807 (1765), state officers raided homes in search of materials connected to John Wilkes' pamphlets attacking governmental policies and the King himself. Entick, an associate of Wilkes, sued after officers forcibly entered his home, broke into desks and boxes, and seized his charts and pamphlets. *Id.* at 807–08. In his opinion, Lord Camden denounced the officers' use of a general warrant to "search" Entick's property, pointing to the officers' "breaking into [] drawers and boxes" and "ransacking all the rooms in his house, and prying into all his private affairs." *Id.* at 814. The evil was not merely physical trespass; it was the invasive inspection of private papers.

Entick was "welcomed and applauded by the lovers of liberty in the colonies" and guided the Framers in crafting the Fourth Amendment. *Boyd v. United States*, 116 U.S. 616, 626 (1886). As this Court explained in *Boyd*, "every American statesman, during our revolutionary and formative period as a nation, was undoubtedly familiar with this monument of English freedom," and considered it "sufficiently explanatory of what was meant by unreasonable searches and seizures." *Id.* at 627. Founding-era sources confirm that "search" was understood in its ordinary sense: to examine or inspect for the purpose of discovery. *See* John G. Wrench, *The Original Meaning of "Searches,"* INST. FOR JUST. 15–16 (Feb. 26, 2026).[2]

This Court has repeatedly returned to the original public meaning of "search" when confronting new investigative techniques. In *Ex parte Jackson*, 96 U.S. 727 (1878), this Court held that a search occurred when post office employees opened and examined letters to uncover obscene materials. *Id.* at 733. *Ex parte Jackson* also teaches that an individual does not forfeit his property interest merely by entrusting letters or records to a third party—even the government itself. "Letters and sealed packages . . . in the mail are as fully guarded from examination and inspection . . . as if they were retained by the parties forwarding them in their own domiciles." *Id*. Thus, the constitutional violation lay in the government's inspection of private papers without judicial authorization.

Similarly, in *Arizona v. Hicks*, 480 U.S. 321, 324–25 (1987), officers conducted a search when they moved stereo equipment to read a hidden serial

[2] Available at https://tinyurl.com/ykvtaahw.

number. *Id.* The equipment was already in plain view; what transformed the act into a search was the purposeful exposure of hidden information. *Id.* Lower courts have applied similar reasoning in modern digital search cases. *See United States v. Musgrove*, 845 F. Supp. 2d 932, 949 (E.D. Wis. 2011) (finding a search when officers touched a computer to remove the screensaver, which "put into view the Facebook wall, which was not previously in view"); *United States v. Bell*, No. 15-10029, 2016 U.S. Dist. LEXIS 52651, at *6–7 (C.D. Ill. 2016) (opening a flip phone constituted a search because the officer "exposed to view concealed portions of the object—i.e., the screen").

The plain meaning of "search" has also guided this Court's decisions in cases involving modern surveillance technology. In *Kyllo*, 533 U.S. at 34–35, the Court held that the use of a thermal imager to detect heat signatures within a house was an unlawful warrantless search. Writing for the majority, Justice Scalia grounded the Court's analysis in the constitutional text, looking at whether use of the thermal imager revealed information "that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area.'" *Id.* at 34 (quoting *Silverman v. United States*, 365 U.S. 505, 512 (1961)). In doing so, the Court "assured preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Id.* at 34; *see also id.* at 32 n.1 (defining "search" and noting that the "search" meant the same thing "[w]hen the Fourth Amendment was adopted" as it does today).

This Court would not be breaking new ground by returning to the original public meaning of "search." *Kyllo* is just one example of how the digital age has

created new techniques for revealing evidence or fruits of a crime. New technologies—from GPS trackers to cell-site simulators to "search history records" and facial recognition software—expand the government's ability to monitor Americans in ways the Founders could never have anticipated. Yet that novelty is precisely why a return to first principles is necessary. When doctrine drifts from the constitutional text, courts are left to improvise. A stable, text-based definition of "search" provides a principled limit.

The core principle is straightforward: when the government undertakes an investigatory act aimed at discovering private or concealed information, it conducts a search within the meaning of the Fourth Amendment. The means through which that examination occurs—whether by opening a sealed envelope or aiming a thermal imager at a house—does not change the character of the act if it is performed with the purpose of revealing concealed information. *Compare Jackson*, 96 U.S. at 727 *with Kyllo*, 533 U.S. at 27.

II. AMERICANS OWN MANY OF THEIR DIGITAL RECORDS—EVEN THOSE THAT ARE STORED WITH TECH COMPANIES.

Both the panel majority decision and a seven-judge concurrence on the en banc court rejected Chatrie's argument that he owns his Location History records. In each instance, the claim was dispatched briefly, dismissively, and in a footnote. *Chatrie*, 136 F.4th at 141 n.21 (Richardson, J., concurring); *United States v. Chatrie*, 107 F.4th 319, 332 n.20 (2024). That cursory treatment reflects a deeper problem: courts too often default to *Katz* and the third-party doctrine without seriously engaging defendants' property-based claims

to their own digital records—even when those records are merely stored with companies like Google.

A. This Court Has Revived the Property Approach in Fourth Amendment Cases.

Before Justice Harlan's concurrence in *Katz v. United States*, courts evaluating warrantless searches focused primarily on property interests. *See Olmstead v. United States*, 277 U.S. 438, 458–66 (1928) (citing cases). While the reasonable expectation of privacy test quickly became the default, this Court has been clear that *Katz* did not wholly supplant the traditional property-based approach. *United States v. Jones*, 565 U.S. 400, 407 (2012).

Jones made that point unmistakable. There, the defendant challenged the government's warrantless installation of a GPS tracking device on his vehicle. *Id.* at 403. Rather than rely on *Katz*, the Court returned to first principles. It held that the government violated the Fourth Amendment by physically trespassing on personal property to obtain information. *Id.* at 410.

Jones thus revived property as a touchstone of the Fourth Amendment. Writing for the majority, Justice Scalia explained: "*Katz* did not erode the principle 'that, when the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment.'" *Id.* at 407 (quoting *United States v. Knotts*, 460 U.S. 276, 286 (1983)) (Brennan, J., concurring)). To hold otherwise would be to "narrow the Fourth Amendment's scope." *Id.* at 408. The Court reemphasized the importance of analyzing property concepts in Fourth Amendment search cases just one year after *Jones*. In *Florida v. Jardines*, 569

U.S. 1 (2013), the Court again endorsed the property-based approach as a complement to *Katz*. *Id*. at 11.

Although *Jones* and *Jardines* reaffirmed the importance of property, lower courts continue to default to the *Katz* test—and the derivative "third-party doctrine"—in cases involving sensitive records. This doctrine rests on the premise that people forfeit Fourth Amendment protection in information voluntarily conveyed to third parties. *See United States v. Miller*, 425 U.S. 435 (1976) (holding that a depositor had no legitimate expectation of privacy concerning certain financial records held by a bank); *Smith v. Maryland*, 442 U.S. 735 (1979) (holding that a suspect had no legitimate expectation of privacy in phone numbers he "conveyed" to a phone company via dialing phone numbers).

But this Court has not upheld a warrantless search or seizure under the third-party doctrine in the decades since *Smith* and *Miller*. And to the extent that the third-party doctrine remains viable, the Court has made clear that the government's analogies to the pre-digital, "manual" era of government surveillance often do not apply when applied to modern digital records. *See Riley v. California*, 573 U.S. 373, 386 (2014); *Carpenter v. United States*, 585 U.S. 296, 312 (2018).

This Court should direct lower courts to apply the property-based approach, which "keeps the easy cases easy." *Jardines*, 569 U.S. at 11. That framework asks a straightforward question: was "a house, paper, or effect" yours under the law? *Carpenter*, 585 U.S. at 397 (Gorsuch, J., dissenting). While *Katz* provides "one way to prove a Fourth Amendment interest, it has never been the only way." *Id.* at 405. The courts below lost sight of that principle.

B. Google's User Agreement and Privacy Policy Suggest that Users Own Their Location History Records.

This Court has long recognized that the Fourth Amendment protects our property. *Soldal v. Cook County*, 506 U.S. 56, 62 (1992) ("[O]ur cases unmistakably hold that the Amendment protects property as well as privacy."). Accordingly, when a defendant asserts a property interest—as Chatrie does—the court must ask: does the individual have a property interest in the items searched or seized? If so, a warrant is required. Yet the courts below hastily invoked the third-party doctrine to declare Chatrie's property interest nonexistent.

Modern digital services are governed by contracts, and contracts allocate property rights. Like many service providers, Google's terms of service allocate property rights in the data, records, and communications produced by customers in the use of its services.

In *People v. Seymour*, 536 P.3d 1260, 1273 (Colo. 2023)—a case closely analogous to this one—the Colorado Supreme Court held that the defendant owned his Google search history records based on the rights afforded to him by Google's terms of service. Relying on Google's privacy policies and user agreements, the court concluded that the defendant—not Google—owned his search history because the contract terms granted the defendant the right "to exclude and to control the dissemination and use of [his] digital data." *Id.* Thus, the government "meaningfully interfered with [Seymour's] possessory interest" when it copied his digital records by infringing on his "rights to exclude and to control the dissemination and use" of his records. *Id.*

Seymour is instructive because the agreement governing the defendant's use and possession also afforded him the right to control access to the property. The case also shows that just because a third party lawfully *possesses* property doesn't mean the possessor *owns* the property. *See Carpenter*, 585 U.S. at 400 (Gorsuch, J., dissenting) (discussing bailment concepts and digital records).

The same reasoning applies here. Users may retain a property interest in their Google Location History even though Google stores the data.[3] When people enable location tracking, they share and produce personal information that can be sensitive, intimate, and privileged. *See* Pet. Opening Br. 4 (explaining how Location History tracks users). Google's user agreements and privacy policies reflect that sensitivity by allocating to users substantial rights to control and manage their data.

At any time, Google users may request a copy of their Location History, delete their data, or withdraw or restrict consent for the processing of their location information.[4] In other words, users have the right to

---

[3] In 2023, Google changed how it stores users' Location History records. Now, instead of being stored in Google's "Sensorvault," Location History is stored directly on users' devices. Pet. Opening Br. 5.

[4] Users who have opted in to Google's "Timeline" feature may review and manage their location history at any time. Timeline users may also manage and delete all or part of their location history at any time. *Manage your Timeline data*, GOOGLE, https://tinyurl.com/3xvfvbra (last visited Feb. 24, 2026). Users choose how long Timeline data is saved—with options to automatically delete data after 3, 18, or 36 months or to keep data until the user manually deletes it. *How Google uses location information,* GOOGLE

control how and when others access their information. That authority to control and exclude is the essence of property.

It is notable that Google, in its *amicus* brief to the district court, described Location History as "a history or journal that Google users can choose to create, edit, and store to record their movements and travels." JA-16. It has explained that Location History is stored "primarily for the user's own use and benefit," and is stored "in accordance with the user's decisions." JA-20. *Cf. Seymour*, 536 P.3d at 1273 ("Google's licensing agreement makes clear that it does not own its users' content. Instead, users own their Google content, which, according to testimony from a Google policy specialist, includes their search histories.").

The property principles that apply to tangible effects and papers also apply to their digital equivalents. When contracts confer rights to control, exclude, copy, and delete digital records, they recognize an ownership interest. It appears Google's agreements vest those rights in users like Chatrie. If so, the government cannot seize, copy, or otherwise access such records without first obtaining a warrant.

C. Most States Expressly Recognize that Users Own Their Digital Records.

Contract law is not the only source of law recognizing users' ownership of their digital records. State

---

PRIVACY & TERMS, https://tinyurl.com/3m2m6e4c (last visited Feb. 24, 2026). Google users may also review, manage and delete location and other information gathered by Web & App Activity and may control which apps have permission to use device location on Android devices. *Id.*

positive law reinforces that conclusion. Although the details vary, a majority of states now define electronic data and digital records as a form of personal property.

Positive law has "illuminate[d] the meaning of constitutional provisions" since the Founding. Trevor Burrus & James Knight, Katz *Nipped and* Katz *Cradled:* Carpenter *and the Evolving Fourth Amendment*, 2017–2018 CATO SUP. CT. REV. 79, 106 (2018). In the context of the Takings Clause, the definition of "property" is shaped by "existing rules or understandings that stem from an independent source such as state law." *Bd. of Regents of State Colleges v. Roth*, 408 U.S. 564, 577 (1972). The Takings Clause was not meant to be limited to the types of property that existed at the Founding—rather it was meant to protect private property *generally*. *See* William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1843 (2016). By using positive law as a guide, the Court has better preserved the original purpose of the Takings Clause and allowed the definition of property to accord with contemporary understanding.

The same reasoning applies under the Fourth Amendment. Today, more than half of states have enacted or amended laws to treat digital records and data as personal property.[5] Many of these laws make it

[5] *See* ALA. CODE § 13A-8-111(18) (2024); ARK. CODE § 5-41-102(10) (2024); COLO. REV. STAT. § 18-5.5-101(8) (2024); CONN. GEN. STAT. § 53-451(12) (2024) ("'Property' means . . . computer data . . . and all other personal property regardless of whether they are . . . tangible or intangible . . . ."); DEL. CODE tit. 11, § 931(15) (2024) ("'Property' means anything of value, including data."); GA. CODE § 16-9-92(13) (2023) ("'Property' includes computers, computer networks, computer programs, data, financial instruments, and

illegal for private actors to access or convert another person's digital data. By explicitly defining digital records as "property" and by enacting digital privacy statutes that give users the right to obtain, control, and delete their personal information, states have recognized that users often own their digital records.[6]

---

services."); HAW. REV. STAT. § 708-800 (2025) ("'Property' . . . includes property that is stored in an electronic medium and is retrievable in a perceivable form."); 720 ILL. COMP. STAT. 5/15-1 (2006) ("'[P]roperty' means anything of value [and] includes . . . computer programs or data . . . ."); IOWA CODE § 702.14 (2025) ("'Property' is anything of value, whether publicly or privately owned, including but not limited to computers and computer data . . . ."); KAN. STAT. § 21-5839 (2025) ("'[P]roperty" includes . . . information, [and] electronically produced or stored data . . . ."); KEN. REV. STAT. § 434.840 (2025) (similar); LA. REV STAT. § 14:73.1 (2019); ME. R. CRIM. PROC. 41(d) (2017); MD. CODE, CRIM. LAW § 7-101 (2025); MASS. GEN. LAWS ch. 266, § 30(2) (2025); MINN. STAT. § 609.87(6) (2024); MISS. CODE § 97-45-1(u) (2024); MONT. CODE § 45-2-101(61) (2023); NEV. REV. STAT. § 205.4755 (2024); N.J. REV. STAT. § 2C:20-1(g) (2024); N.Y. PENAL LAW § 156.00(3) (2025); N.C. GEN. STAT. § 14-453(8) (2012); N.D. CENT. CODE § 12.1-06.1-01(3)(h) (2023); OHIO REV. CODE § 2901.01(10)(a) (2023); OR. REV. STAT. § 164.377(j) (2024); S.C. CODE § 16-16-10(f) (2002); TENN. CODE § 39-14-601(17) (2024); TEX. PENAL CODE § 33.01(16) (2023); UTAH CODE § 76-6-702(5) (2023); VT. STAT. tit. 13, § 4101(8) (2024); WIS. STAT. § 943.70(1)(h) (2025); WYO. STAT. § 6-3-501(a)(x) (2024).

[6] Even under the *Katz* test, it seems likely a search occurred as Chatrie has an expectation of privacy in his Location History. The Virgina Consumer Data Protection Act (CDPA) gives residents like Chatrie certain rights over their personal data and establishes responsibilities and privacy protection standards for companies. VA. CODE §§ 59.1-577–59.1-581 (2022). The statute requires companies to assist users in exercising their rights by obtaining consent before processing sensitive information, disclosing when it will be sold, and allowing them to opt-out of data collection. It also gives users the right to request the deletion of

It is unclear which state's law governs Google's terms of service obligations because the courts below did not resolve that issue. However, in Virginia—the state where this case arose—digital records like Location History satisfy the definition of "property."[7] As Justice Gorsuch explained, "if state legislators or state courts say that a digital record has the attributes that normally make something property," that provides "a sounder basis for judicial decisionmaking than judicial guesswork." *Carpenter*, 585 U.S. at 402 (Gorsuch, J., dissenting).

When courts assess the scope of Fourth Amendment protection, they must rely on stable and legitimate sources of law. By relying on "democratically legitimate sources of law" this Court ensures that judges do not replace sound legal analysis with "their own biases or personal policy preferences." *Id.* at 398 (quoting Todd E. Pettys, *Judicial Discretion in Constitutional Cases*, 26 J.L. & POL. 123, 127 (2011)). Both contract law and positive law confirm that users have a cognizable property interest in their digital records. Accordingly, when the government wishes to examine someone's personal digital records—even when they are stored by a tech company—a warrant is required.

---

personal data provided by or obtained about the user. *Id.* at § 59.1-577.

[7] VA. CODE § 18.2-152.2 (2010) ("'Property' shall include . . . computer data . . . and all other personal property regardless of whether they are . . . [t]angible or intangible; . . . [i]n transit between computers or within a computer network or between any devices which comprise a computer; or . . . [l]ocated on any paper or in any device on which it is stored by a computer or by a human . . . .").

III. A WARRANT IS REQUIRED EVERY TIME THE GOVERNMENT CONDUCTS A SEARCH OF DIGITAL RECORDS.

The warrant at issue in this case drew a geofence with a 300-meter diameter around the bank where the robbery occurred. Pet. Opening Br. 8–9. It also authorized a three-step process by which law enforcement would request and obtain Location History from Google. Each step sought new information, yet at no point were the successive requests submitted to a neutral magistrate for additional scrutiny. *Id.* at 9.

At each step of the geofence process officers performed an investigatory act designed to obtain new private information—a "search" in the plainest sense of the term. Under the Fourth Amendment, each search must be preceded by review for particularity and probable cause by a neutral magistrate. That requirement was not satisfied here.

A. The Government Conducted Multiple Searches in This Case.

"[C]ourts have recognized that no warrant can authorize the search of everything or everyone in sight." *United States v. Smith*, 110 F.4th 817, 836 (5th Cir. 2024) (citation omitted). Rather, the Fourth Amendment requires that each distinct search be authorized by its own warrant. *See Marron v. United States*, 275 U.S. 192, 196 (1927) ("The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible."); *Ybarra v. Illinois*, 444 U.S. 85, 92 n.4 (1979) ("'[O]pen-ended' or 'general' warrants are constitutionally prohibited.").

When conduct results in "a significant expansion" of a prior search, it "must be characterized as a separate search." *Walter v. United States*, 447 U.S. 649, 657 (1980). *See also Hicks*, 480 U.S. at 324–25 (moving the stereo equipment to reveal the hidden serial number constituted a "'search' separate and apart" from the search of the house because it "produce[d] a new invasion of respondent's privacy").

The three steps authorized by the geofence warrant amount to three separate and distinct searches, each requiring independent review and approval by a neutral magistrate.

1. A search occurred when officers requested and obtained anonymized Location History data showing every user within the geofence.

The officers conducted their first search when they reviewed anonymized location history of the users located within a 300-meter diameter of the bank within one hour of the robbery. This initial search revealed that 19 users, including Okello Chatrie, were present within the geofence during the specified timeframe. Pet. App. 299a.

The officers' examination of the Step 1 records fits squarely within the original public meaning of "search." The Step 1 request compelled Google to produce private user records revealing the movements of its users within a defined geographic area over a fixed period. That inquiry had one purpose: to discover "evidence of criminal wrongdoing." *Maryland v. King*, 569 U.S. 435, 468 (2013) (Scalia, J., dissenting). When the government invades a constitutionally protected property interest for that purpose—as it did here by

acquiring and viewing Chatrie's private location records—it conducts a search within the meaning of the Fourth Amendment and a warrant is required. *See Jones*, 565 U.S. at 404.

2. New searches occurred when the officers reviewed additional Location History records and identifying information.

After reviewing the first production of records, law enforcement sought additional information for all 19 users identified in Step 1. Pet. App. 299a. Google objected to the breadth of that request, and law enforcement ultimately narrowed its demand to nine devices. *Id.* at 299a–300a. The records produced in response to that narrowed request were markedly different from those obtained at Step 1 in two respects. First, they tracked users' movements over a longer period. Where Step 1 requested Location History for one hour, the Step 2 request covered two hours. Second, and significantly, the Step 2 records were not confined to the geofence. They followed users' movements both inside and outside the geofence, revealing a broader picture of where those individuals had traveled.

When law enforcement examined the Step 2 records, it conducted a search "separate and apart" from its first search. *Hicks*, 480 U.S. at 324. The Step 2 records revealed an entirely new body of information covering a different area over a different period. Their examination was not a continuation or refinement of the first production, but rather "a significant expansion" of the Step 1 search. *Walter*, 447 U.S. at 657. The Step 2 search independently invaded Chatrie's property interest in his digital records and therefore independently required a warrant.

Just as procuring more expansive Location History at Step 2 constituted a new search, Step 3 represents yet another search. By reviewing the records produced at Step 3, law enforcement "exposed" what was "concealed"—they learned the identities of those who had previously been anonymized—and engaged in another search.

B. Courts Must Not Allow a Single Geofence Warrant to Authorize Multiple Searches.

The geofence warrant in this case authorized precisely the sort of exploratory rummaging the Fourth Amendment sought to prohibit. *See Riley*, 573 U.S. at 403. By structuring the warrant around a three-step process that permitted law enforcement to review progressively more sensitive information from Google—without ever returning to a magistrate—the government effectively secured a blank check.

Warrants operate to "assure[] the citizen that the intrusion is authorized by law, and that it is narrowly limited to its objectives and scope." *Skinner v. Ry. Lab. Execs. Ass'n*, 489 U.S. 602, 622 (1989). It is the job of a neutral magistrate—not law enforcement—to determine "whether an intrusion is justified in any given case." *Id.* Authorization to search one thing does not automatically confer authority to search another, no matter how necessary the government believes that search to be. *See Walter,* 447 U.S. at 656–57 ("Consent to search a garage would not implicitly authorize a search of an adjoining house; a warrant to search for a stolen refrigerator would not authorize the opening of desk drawers."); *United States v. Di Re*, 332 U.S. 581, 587 (1948) (officers armed with a warrant to search a residence may not "search all persons found in it").

The Fourth Amendment's protections become illusory if law enforcement officers have the power to define the scope of their own search authority. This Court recognized as much in *Ybarra v. Illinois*. There, officers obtained a warrant to search a bar and its bartender, but then independently decided to search the bar's patrons as well. 444 U.S. at 91–92. The Court rejected the government's contention that the warrant was sufficient to authorize searches of Ybarra and his fellow patrons, emphasizing that "the agents knew nothing in particular about Ybarra" beyond his presence in a public tavern. *Id.* at 91.

The same defect doomed the warrant in *Lo-Ji Sales v. United States*, 442 U.S. 319, 321 (1979). There, police obtained a warrant to search an adult bookstore for specific films, but the warrant also provided that the issuing Town Justice could accompany police during the search so he could "determine independently if any other items at the store" violated the state's obscenity laws. *Id.* This Court held that the search warrant was invalid under the Fourth Amendment because it was too "open-ended," explaining that it cannot be left "entirely to the discretion of the officials conducting the search to decide what items were likely obscene." *Id.* at 325.

The geofence warrant here suffers from the same constitutional deficiencies that doomed the searches in *Ybarra* and *Lo-Ji Sales*. In those cases, officers expanded the scope of the search mid-investigation, effectively determining for themselves what the warrant permitted. Similarly, the geofence warrant outlined three steps the government *may* take but left it entirely up to law enforcement to decide whether to proceed and what additional information to request,

without requiring any return to a magistrate for an independent assessment of whether the new search was justified.

This Court should make clear that each stage of the geofence warrant constituted a distinct search. Each step was a separate investigatory act designed to extract new records from Google's databases. Magistrates and reviewing court must not collapse the entire geofence process as a single search. To do so would grant law enforcement a master key—one warrant authorizing multiple successive intrusions—contrary to the basic structure of the Fourth Amendment.

CONCLUSION

The constitutional principles that resolve this case are not novel. An investigatory act designed to reveal private information is a search. A person's digital records are their property, and that property interest does not evaporate merely because a third party stores the records.

For these reasons and those described by Chatrie, this Court should reverse the judgment below.

Respectfully submitted,

Matthew P. Cavedon
Counsel of Record
Brent Skorup
Laura A. Bondank
CATO INSTITUTE
1000 Mass. Ave., N.W.
Washington, DC 20001
(706) 309-2859
mcavedon@cato.org

Dated: March 2, 2026