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

REPLY BRIEF FOR PETITIONER

GEREMY C. KAMENS
Federal Public Defender
LAURA J. KOENIG
PATRICK L. BRYANT
Assistant Federal Public Defenders
OFFICE OF THE FEDERAL PUBLIC DEFENDER, EASTERN DISTRICT OF VIRGINIA
1650 King Street,
Suite 500
Alexandria, VA 22314

MICHAEL W. PRICE
NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
FOURTH AMENDMENT CENTER
1600 L Street, NW
Washington, DC 20036

ADAM G. UNIKOWSKY
Counsel of Record
LAUREL A. RAYMOND
ANNE S. WARNKE
JENNER & BLOCK LLP
1099 New York Ave., NW
Suite 900
Washington, DC 20001
(202) 639-6000
AUnikowsky@jenner.com

DAVID A. STRAUSS
SARAH M. KONSKY
JENNER & BLOCK SUPREME COURT AND APPELLATE CLINIC AT THE UNIVERSITY OF CHICAGO LAW SCHOOL
1111 E. 60th Street
Chicago, IL 60637

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

INTRODUCTION

When the government directed Google to search petitioner's private account for Location History records, it conducted a Fourth Amendment search. Because the geofence warrant did not comply with the Fourth Amendment, the search was unconstitutional.

The government conducted a search. Location History records are users' property, analogous to emails and documents. These records are stored in users' private Google accounts, and users can review, edit, and delete them. Additionally, users have a reasonable expectation of privacy in their Location History. A person's location can reveal highly sensitive information—particularly when the government gets to pick the time and location. The government's theories as to why Location History is unprotected—many of which would apply equally to emails and documents—would open the door to warrantless rummaging through private information merely because it is in the cloud rather than on a cell phone.

The warrant violated the Fourth Amendment. The warrant directed Google to search tens of millions of accounts to discern devices that might have been within the geofence; caused Google to expose the private location information of 19 people to police merely based on their proximity to the crime; and gave the police complete discretion to winnow that list and conduct additional searches, while casting Google into the role of magistrate. Such a warrant is not issued "upon probable cause … and particularly describing the place to be searched." U.S. Const. amdt. IV.

I. THE GOVERNMENT CONDUCTED A SEARCH.

Under both the property-based approach and the reasonable-expectation-of-privacy approach, the government conducted a search.

A. Users hold a property interest in their Location History.

The government conducted a search because it invaded petitioner's property interest in his Location History. Location History is a form of property, one's digital "papers" and "effects," that is protected by the Fourth Amendment.[1]

1. The Fourth Amendment "assur[es] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *United States v. Jones*, 565 U.S. 400, 406 (2012) (quotation marks omitted). Thus, the government errs in suggesting (Resp. Br. 34) that whether a Fourth Amendment property interest exists is a state-law question requiring a choice-of-law analysis. The question is one of federal constitutional law. The Court has followed this approach in prior property-based Fourth Amendment cases: in *Florida v. Jardines*, 569 U.S. 1 (2013), and *United States v. Jones*, 565 U.S. 400 (2012), the Court

[1] Contrary to the government's contention (Resp. Br. 30), petitioner did not forfeit his property-based argument. Petitioner litigated this issue at length in the district court. *See* 4th Cir. J.A. 38-40, 382-83. Petitioner preserved this issue in the Fourth Circuit for the reasons explained in his certiorari-stage reply brief (at 7-8), which the government ignores.

found Fourth Amendment violations by applying traditional property law principles, not by analyzing contemporary Florida and Maryland law. Likewise, in *Tyler v. Hennepin County*, 598 U.S. 631 (2023), the Court held that property, for Fifth Amendment purposes, turns on "traditional property law principles, plus historical practice and this Court's precedents," not state law. *Id.* at 638 (citations omitted).

To be sure, contemporary state law is "one important source" courts should consider, *id.*, particularly given that Founding-era sources do not specifically address computer data. But the ultimate question is whether Location History qualifies as property under "traditional property law principles." *Id.* (citations omitted).

It does. Google users control their Location History—they may review, edit, and delete it. *See* JA-19 (Google amicus brief)[2]; JA-42, 46 ¶¶ 5, 15 (declaration of Google employee); JA-58 (privacy policy statement that users can "save and manage" location information); Pet. App. 283a (factual finding). And users enjoy the right to exclude—Location History appears only in their private Google accounts. JA-71 (privacy policy). Google does not share it with advertisers. *Infra* at 14.

Numerous state legislatures and courts treat computer data as property. Pet. Br. 16-19; *see* Cato Br. 14 & n.5 (citing 32 state statutes defining property to include

[2] Google's amicus brief in the district court (JA-9-40) was formally entered into evidence based on the live testimony of a Google employee. 4th Cir. J.A. 616.

data). The Court should follow that consensus and hold that computer data is property for Fourth Amendment purposes.

The government contends that Location History is not property because it is purportedly "raw" and hence cannot be "own[ed]." Resp. Br. 32 (citation omitted). But raw data, including location information, has value, *see In re Google Location History Litigation*, 514 F. Supp. 3d 1147, 1158-60 (N.D. Cal. 2021) (finding that plaintiff stated unjust enrichment claim based on retention of Location History), and is regularly bought and sold, including by the government. *See* Alfred Ng, *FBI is Buying Data that Can be Used to Track People, Patel Says*, Politico (Mar. 2026), https://www.politico.com/news/2026/03/18/fbi-buying-data-track-people-patel-00834080. Courts routinely characterize "raw data" as property. *See, e.g.*, *Rodriguez v. ByteDance, Inc.*, No. 23 CV 4953, 2025 WL 672951, at *14 (N.D. Ill. Mar. 3, 2025) (permitting conversion claim to proceed based on alleged theft of data, including location data); *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 635 (N.D. Cal. 2021) (permitting larceny claim to proceed based on alleged theft of personal information). The government offers no basis for its apparent view (Resp. Br. 32) that the Fourth Amendment turns on copyrightability.

The cloud did not exist in 1791, but that should not foreclose Fourth Amendment protection. *See Riley v. California*, 573 U.S. 373, 403 (2014) (digital information is not "any less worthy of the protection for which the Founders fought"). Location History readily qualifies as "papers" and "effects" for Fourth Amendment purposes,

and treating it as property would advance the Fourth Amendment's goal of protecting against the gratuitous inspection of private papers. *See Entick v. Carrington*, 19 How. St. Tr. 1029, 1066 (C.P. 1765) (private papers "will hardly bear an inspection").

The government's theory implies that people lack Fourth Amendment interests even in health information like weight or blood pressure data. That cannot be right. If a person kept a diary reporting where he went every day (or his weight or blood pressure), that would receive Fourth Amendment protection; the result should not change if the information is in the cloud. Just as the Fourth Amendment protects against the use of a heat-detecting device to derive information from within a house even if the police do not physically enter, *see Kyllo v. United States*, 533 U.S. 27 (2001), the Fourth Amendment protects against the digital inspection of private data even if the police do not physically touch it.

No case supports the government's proposed "raw data" doctrine. The government cites a footnote in Justice Thomas's *Carpenter* dissent noting that CSLI might not be "effects." Resp. Br. 32 (quoting *Carpenter v. United States*, 585 U.S. 296, 351 n.8 (2018) (Thomas, J., dissenting)). But that footnote emphasizes that CSLI records are business records—not that the Fourth Amendment does not cover factual records. Justice Thomas later stated that "[b]y now, it is well established that information contained in a computer is 'property'.... Federal and state law routinely define 'property' to include computer data." *Van Buren v. United States*, 593

U.S. 374, 400 (2021) (Thomas, J., dissenting).[3]

2. Google is a bailee. Google's Terms of Use state that Location History is "your location information in your account"—a classic bailment. JA-58; Pet. Br. 21.

The government offers the creative response that "your location information in your account" actually means "location information about you owned by Google." *See* Resp. Br. 35. This framing is inconsistent with how any English speaker would understand these words and Google itself rejects it. Google Br. 3 (Location History constitutes "the user's *personal* records."). The government's example—a tailor's storage of "your measurements"—is inapt: measurements are not stored in customers' private accounts. And the fact that the privacy policy separately clarifies that users own their intellectual property (Resp. Br. 35) is perfectly consistent with users also owning their Location History.

As evidence of Google's ownership, the government points to Google's "deletion" of Location History from its servers. *See id.* (citing Google Br. 2). But in fact, Google moved the data from the cloud to individual devices—

---

[3] The government asserts that "'American law has generally refused to recognize property rights in data.'" Resp. Br. 32 (quoting Steven H. Hazel, *Personal Data as Property*, 70 Syracuse L. Rev. 1055, 1057 (2020)). But the article supports that proposition with only a single Seventh Circuit decision addressing an irrelevant Article III standing issue, Hazel, *supra*, at 1057 & n.4, and then argues that there *should* be property rights in data, *id.* at 1060 & n.24.

confirming that Location History records are not business records. Google Br. 11 (noting migration of Location History data to "on-device storage").

B. Users hold a reasonable expectation of privacy in their Location History.

Petitioner reasonably expected that his Location History would remain private. The fact that this data was stored in a password-protected account establishes not only petitioner's property interest, but also his reasonable expectation of privacy. In arguing against petitioner's property-rights claim, the government cites academic work urging that personal data be protected through privacy torts rather than property law. Resp. Br. 34 (citing Jane R. Bambauer, *How to Get the Property out of Privacy Law*, 133 Yale L.J.F. 1087 (2024)). In practice, courts have protected against intrusions on private data via *both* property law *and* privacy torts, most commonly intrusion on seclusion. *See* Pet. Br. 16-18. That body of tort law—which gives people a means of vindicating privacy rights—underscores their reasonable expectation of privacy.

The sensitivity of Location History reinforces petitioner's reasonable expectation of privacy. Like the CSLI in *Carpenter*, Location History is "detailed, encyclopedic, and effortlessly compiled," goes back years, and "faithfully follow[ed] its owner" everywhere he went. 585 U.S. at 309, 311-12.

The government observes that confidence intervals sometimes have a wide radius. Resp. Br. 7, 24. But Location History is "markedly more *precise*" than the

CSLI in *Carpenter*. Pet. App. 209a. To the extent confidence intervals are sometimes large, this increases the number of accounts swept into a given geofence—hardly a reason to withdraw Fourth Amendment protection. *See* Pet. App. 303a (noting that, in view of confidence intervals, geofence warrant might have swept in people in private residences and a hotel).

The government emphasizes that this case involved two hours of Location History, rather than seven days as in *Carpenter*. Resp. Br. 24. But the relevant time period is not two hours—it is forever. If accessing Location History is not a search, then the government can, without obtaining a warrant, determine precisely where a person was at any time in the past. That violates reasonable expectations of privacy. As the *Carpenter* Court noted, citing Justice Alito's *Jones* concurrence, "[s]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, could not—secretly monitor and catalogue every single movement of an individual's car for a very long period." 585 U.S. at 310 (citation omitted). That is even more true for the movements of the individual himself.

The government insists that a two-hour "window reveals little about the details of petitioner's personal life." Resp. Br. 20. That depends on what the person was doing—a person's presence at a religious ceremony, abortion clinic, or strip club can reveal much. *See Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).

Geofence warrants present serious privacy concerns because they enable the government to draw geofences

around such sensitive locations. *Cf.* Reporters Committee Br. 16-17 (noting that California county used mobile phone data to monitor a church to locate violations of stay-at-home requirements during COVID). The privacy interests at stake go well beyond whether there is a reasonable expectation of privacy in being "parked for two hours behind an office building." Resp. Br. 20.

The geofence warrant in this very case encircled a church. Although the government emphasizes that petitioner robbed a bank rather than engaged in religious worship (Resp. Br. 20), the constitutionality of a warrant turns on whether it *could* disclose that sensitive information, not whether it actually did. *Kyllo*, 533 U.S. at 38-39. And the geofence warrant resulted in millions of people's private information being searched and 18 other people's private information being exposed to the government (including two others who were de-anonymized at Step Three)—to say nothing of the thousands of people whose personal information has been searched and exposed without their knowledge based on geofence warrants that were never unsealed.

This case differs from *United States v. Knotts*, 460 U.S. 276 (1983), on which the government relies. In *Knotts*, the police bugged a chloroform drum with the consent of the container's owner, which then transferred the container to the defendant. *Id.* at 278. The government surveilled the defendant while he traveled on public thoroughfares by following the beeper. *Id.* at 281-82. The beeper revealed no information "that would not have been visible to the naked eye." *Id.* at 285.

The privacy issues here are not comparable. Because the defendant voluntarily accepted the container, *Knotts* did not involve the unconsented invasion of a property interest. *See id.* at 279 n.* (noting that Knotts did not challenge the installation of the beeper). Even under the reasonable-expectation-of-privacy approach, *Knotts* turned on the fact that Knotts was "in an automobile on public thoroughfares." *Id.* at 281. The Court acknowledged the concern that its holding would allow "twenty-four hour surveillance of any citizen," stating that if such practices ever become possible, "there will be time enough then to determine whether different constitutional principles may be applicable." *Id.* at 283-84 (quotation marks omitted). A year later, the Court distinguished *Knotts* in a case where a beeper entered a private home. *United States v. Karo*, 468 U.S. 705, 715 (1984). The Court again distinguished *Knotts* in *Carpenter*, emphasizing that "[u]nlike the bugged container[,]" a cell phone "tracks nearly exactly the movements of its owner." 585 U.S. at 311. As in *Carpenter*, the Court should decline to expand *Knotts*'s limited holding to this dramatically different context.

The Stored Communications Act underscores that petitioner had a reasonable expectation of privacy. The Act requires a warrant when the government obtains the contents of electronic communications like Location History. 18 U.S.C. § 2703(a).[4] The government floats

[4] To the extent the Stored Communication Act permits warrantless searches after 180 days, the Act has been held unconstitutional, *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010), and the

the possibility that Location History might fall within the exception for "communication[s] from a tracking device," Resp. Br. 29 (quoting 18 U.S.C. § 2510(12)(C)), but there is no "tracking device" here distinct from petitioner's cell phone. If the government contends that the cell phone *itself* is a "tracking device," the government's position would allow warrantless searches of any information transmitted by a cell phone—a startling departure from both current practice and public expectation.

Although the Act does not provide a suppression remedy, it confirms that people would reasonably expect that the government will not conduct warrantless searches of private data. As such, the government's concerns about displacing "legislative efforts" (*id.*) are misplaced: Congress has *already* mandated the warrant requirement that petitioner advocates.

C. The third-party doctrine does not apply.

Petitioner did not relinquish his expectation of privacy when he transmitted Location History to Google.

1. The third-party doctrine does not apply because Location History records are personal records, not business records. *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976), both turn on the fact that the materials at issue were business records. *See* Pet. Br. 25-28. It is irrelevant that the records in *Smith* were not "quasi-permanent" (*cf.* Resp. Br.

Department of Justice now seeks warrants even beyond 180 days, H.R. Rep. No. 114-528, at 9 (2016).

27); the salient point was that they belonged to the business. Here, however, Location History belongs to users: they can edit or delete Location History records, and Google itself insists they are *not* business records. *Id.* at 15-16, 26.

Resisting this analysis, the government points to language in the privacy policy stating that Google could make disclosures if it has a "good-faith belief" that disclosure is "reasonably necessary" to comply with "legal process" or for "safety" reasons "as required or permitted by law." Resp. Br. 36; JA-69-70. This language, insists the government, shows either that the third-party doctrine applies (Resp. Br. 26-28) or there was no bailment (*id.* at 35) or no trespass (*id.* at 36), which would imply that no Fourth Amendment search occurred at all.

The government's argument is counterintuitive to say the least. By agreeing to the adhesional privacy policy, users acknowledged that Google could comply with "legal process" such as search warrants—not that the government could access data *without* search warrants. Likewise, Google's statement that it will disclose data for "safety" reasons "as required or permitted by law"—which parallels this Court's holdings that warrants are not needed in cases of safety risk, *see Case v. Montana*, 146 S. Ct. 500 (2026)—does not establish across-the-board consent to give data to police. The government suggests that *Google* would not be liable in trespass if it complied in good faith with a warrant (Resp. Br. 36-37), but that would not forgive *the government's* trespass.

Importantly, these privacy policy provisions apply to *all* data stored on Google's servers, not just Location History. If the Court accepts these arguments, then the Fourth Amendment would not protect email or documents stored on Google's servers. Nor would it protect snail-mail: USPS's Terms of Use similarly state that USPS will comply with "legal processes" and "law enforcement requests."[5] FedEx and UPS even more broadly reserve the right to inspect packages as needed.[6] The Court should reject a holding with such drastic implications.

The government also contends that Google had the "unilateral right to disseminate at least the step-one information," pointing to the provision stating that Google "may share non-personally identifiable information publicly and with its partners—like publishers, advertisers, or rightsholders." Resp. Br. 35; *see* JA-70. Again, because this provision applies to all data stored on Google's servers, this argument would imply that the government could conduct warrantless searches of email and documents. The Court should reject it because the privacy policy's next sentence clarifies what Google has in mind: "we share information publicly to show trends about the general use of our services." JA-70. Sharing

---

[5] *See* U.S. Postal Service Payment & Refund Terms and Conditions, usps.com/terms-conditions/general.htm (last visited Apr. 16, 2026).

[6] *See* UPS Terms and Conditions of Domestic Service at 1 https://www.ups.com/media/en/terms_service_dom_mx.pdf (last visited Apr. 16, 2026); FedEx Terms and Conditions at 155 (2026), https://www.fedex.com/content/dam/fedex/us-united-states/services/Service_Guide_2026.pdf.

aggregate, de-identified data depicting general trends is completely different from acquiescing to law enforcement's demands to search for individual users' data.

Finally, the government points to Google's use of Location History in its advertising business. Resp. Br. 19, 28, 43-44. If Google shared individual users' Location History with advertisers, the government might have a case that the Fourth Amendment does not restrict Google from sharing Location History with law enforcement. In that scenario, law enforcement would be doing what "any private citizen might do." *Jardines*, 569 U.S. at 8 (quotation marks omitted). But Google does not do that. Businesses are never told which devices are nearby, they get no information about individual users, and they cannot ask Google for information about where users were in the past. 4th Cir. J.A. 613, 615; *see* JA-45-46 ("Google has not shared identified LH data with third parties except through legal process"). Advertisers cannot do what the police did here—demand that Google inspect each user's account to assess whether they were at a particular location at a point in time.

To the extent the government suggests that merely letting Google "analyze" data "for patterns" effectuates a waiver of Fourth Amendment rights, even if Google *does not* share the data, the government is incorrect. *See* Resp. Br. 21. Bailments routinely confer limited use rights to the bailee without the bailor relinquishing title. Pet. Br. 21. A Google user does not impliedly consent to government searches merely by allowing Google itself to analyze the data. Companies that collect user data, ranging from AI companies to healthcare companies,

almost invariably analyze that data. If that alone waived Fourth Amendment rights, the Fourth Amendment would no longer mean much.

2. Even if Location History records are business records, the third-party doctrine does not apply under *Carpenter*'s rationale. In *Carpenter*, the Court held that the transmission of CSLI was not a voluntary waiver of privacy protection over location information, even though users could turn their phones off. 585 U.S. at 315. The Court adopted a practical approach to voluntariness, declining to construe people's decision to leave their phones on as implied consent to disclose their movements to the government. *Id.* at 315-16.

A similar practical approach should apply here. When users activate their Android phones, they are told that their phone will not "work correctly" unless multiple features, including Location History, are activated. JA-140. Users are not told the frequency, precision, or duration of the collection of location information and are not told it would be conveyed to law enforcement. Petitioner is not claiming that anyone was "bullied or tricked" into activating Location History. *Cf.* Resp. Br. 25. Rather, petitioner argues that clicking "Yes, I'm In" is not reasonably interpreted as implied consent to the government piercing their private accounts and determining their location at any time without a warrant.

The government touts the fact that only one-third of Google users have Location History activated. Resp. Br. 7, 25. The implication is that people can easily turn it off. But that inference is unsound because as the government recognizes, Resp. Br. 22 n.1, the denominator

includes people who merely use Google without having been offered the opportunity to install Location History. It also includes Google users in foreign countries such as China where collecting Location History is illegal. 4th Cir. J.A. 845, 848. In any event, the Court should reject a rule that would withhold Fourth Amendment protection merely because not everyone has activated a particular feature.

II. THE GEOFENCE IS AN UNCONSTITUTIONAL GENERAL WARRANT.

The warrant authorized the search of millions of people's private Google accounts to identify who was within the geofence. That is a general warrant. If a single warrant cannot justify the search of millions of cell phones, a single warrant cannot justify the search of millions of Google accounts in the cloud. Pet. Br. 32-42.

The government suggests that the Fourth Amendment's particularization requirement is satisfied because the warrant recited "Google." Resp. Br. 39. If this argument were correct, the government could search *everyone's* emails stored by Google based on probable cause that *one* person sent an incriminating email. That cannot be right. The relevant Fourth Amendment unit is a person's account, not "Google." Pet. Br. 37-40.

Zurcher v. Stanford Daily, 436 U.S. 547 (1978), does not support the government. In *Zurcher*, the warrant authorized police to search a newspaper's office for photographs *belonging to the newspaper* containing evidence of a crime. *Id.* at 551. *Zurcher* establishes that a warrant can be issued based on probable cause that a third party possesses relevant evidence, even if the third

party is not implicated in the crime. *Id.* at 554. *Zurcher* does not endorse searching millions of distinct private accounts without individualized probable cause.

The government insists that "any law-enforcement search here was of the information it received—not what Google had to itself examine to provide that information." Resp. Br. 41. But when a private party acts "by compulsion of sovereign authority"—or even with the government's "encouragement, endorsement, and participation"—the private party is treated as "an instrument or agent of the Government," such that "the lawfulness of its acts is controlled by the Fourth Amendment." *Skinner v. Ry. Lab. Execs.' Ass'n*, 489 U.S. 602, 614-16 (1989). That is this case: Google complied with a search warrant. The fact that Google ran the search at the government's behest, as opposed to the government itself running the search, does not cure the Fourth Amendment violation. To the contrary, it makes the geofence warrant akin to the writs of assistance that drew the colonists' ire. Pet. Br. 41-42.

The government attributes the need to search every user's account to "Google's own internal design choices" and speculates that Google could have designed its database differently. Resp. Br. 41-42. But indexing data by account ensures that data will be stored in "a distinct space associated with that user and not with everyone else." Br. of Technologists at 14. That industry standard design structure—which reinforces the reality that each account is akin to a separate virtual storage locker—"is part of the security architecture itself, not a mere business preference about how to sort information." *Id.* at 18. A Google witness testified that because the data was

indexed by account, it was impossible to execute the geofence warrant without searching everyone's account. 4th Cir. J.A. 848-49. The government cannot circumvent the Fourth Amendment by speculating that a general search might not have occurred if Google had designed its system in some different, less secure way. Nor can the government disclaim knowledge of Google's practices (Resp. Br. 42) when the Department of Justice worked with Google to design the three-step geofence warrant process (Pet. App. 286a) and the warrant application touted the officer's "training and experience" regarding Location History. JA-133.

The government claims that it merely ran a "computation" and did not "expose" data of users outside the geofence. Resp. Br. 43-44 (citations omitted). But the fact remains that the government, via Google, peered into private accounts to check whether within-geofence location information was present. In ordinary English, it searched every account for that information. The fact that, for most accounts, the government did not find anything does not change the fact that the accounts were searched: "[A] search is not to be made legal by what it turns up." *United States v. Di Re*, 332 U.S. 581, 595 (1948).

Consider this analogy from petitioner's opening brief (Pet. Br. 35-36): suppose a police officer demanded to search a person's Location History stored locally on his cell phone to check whether he was at a protest a few months earlier. Suppose the officer promised to use a third-party software tool and to leave if the software turned up no "hits." Notwithstanding those assurances, anyone would say this is a search. In this case, the data

was in the cloud—but the often imperceptible distinction between locally-stored data and cloud data should not affect the Fourth Amendment analysis. *Riley*, 573 U.S. at 397.

The government points out that in "searches for papers," "innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." Resp. Br. 45 (quoting *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976)). True but irrelevant. If the government obtains a warrant to search a single safety deposit box and seize a particular paper, it may check all the papers in the box to see whether they meet the description. That does not mean the government can obtain a single warrant to search millions of safety deposit boxes.

Finally, the government asserts that under petitioner's theory, "most search warrants and third-party subpoenas—including, potentially, some CSLI warrants—could be characterized as overbroad general warrants." Resp. Br. 41. This, too, is incorrect. Subpoenas are not warrants: they "do not involve the direct taking of evidence." *Carpenter*, 585 U.S. at 317. A ruling in petitioner's favor would not jeopardize subpoenas, which are subject to a distinct body of law. *See id.* "CSLI warrants" authorize the search of a telecommunication company's business records, not millions of private accounts, and hence do not present the same Fourth Amendment concerns. The government identifies no examples of other law enforcement techniques that would be hindered by a ruling in petitioner's favor.

III. EVEN IF THE GEOFENCE WARRANT WAS NOT A GENERAL WARRANT, THE STEP ONE SEARCH WAS UNCONSTITUTIONAL.

Even accepting the government's premise that a search did not occur until data was exposed to the government, the Step One search was unconstitutional.

1. At Step One, Google disclosed the movements of 19 people within the geofence to the government. Although the government notes that the users were not (yet) identified by name (Resp. Br. 19, 22, 43), their accounts were still searched. As petitioner's opening brief explained, (Pet. Br. 43-45), a search is still a search even when the government does not yet know the identity of the person being searched. Further, the "anonymity" here is illusory because it is often easy to determine a person's identity based on their purportedly "anonymous" movements combined with other publicly available information. Indeed, petitioner's expert determined the likely identity of three purportedly "anonymous" accounts based on two hours of Location History and publicly available information. Pet. App. 305a.

The government's reliance on the users' purported anonymity at Step One rings particularly hollow given the government's own position (Resp. Br. 47) that the probable cause that supported the Step One search provided a sufficient basis, on its own, to de-anonymize the users. The government has also argued in lower courts that it may serve a subpoena for the subscriber information for everyone identified in Step One. *See In re Search of Info. Stored at Premises Controlled by Google*, 481 F. Supp. 3d 730, 733 (N.D. Ill. 2020).

In any event, Google ultimately *did* de-anonymize petitioner based on information gleaned from the Step One search. Thus, even if de-anonymization were relevant, petitioner could still challenge the warrant's constitutionality.

2. The warrant fell short of the Fourth Amendment's requirements for two reasons.

First, the warrant failed to particularly describe the place to be searched. A constitutionally compliant warrant would have identified *particular* accounts to be searched, supported by probable cause that evidence would be found *in those accounts*. Here, however, the warrant identified no particular accounts. Instead, it said that *if*, hypothetically, Google located relevant Location History within an account, *then* there would be probable cause to collect Location History from that account. The warrant was analogous to a warrant that does not identify particular homes but instead says that *if*, hypothetically, contraband is delivered to any home, *then* there would be probable cause to search that home—a type of warrant this Court has already stated is unconstitutional. *United States v. Grubbs*, 547 U.S. 90, 96-97 (2006); *see* Pet. Br. 47-48.

The government's brief does not cite *Grubbs* and instead relies on *Karo*. Resp. Br. 44. But as petitioner explained (Pet. Br. 48-49), in *Karo*, the warrant at issue identified a specific object that could only be in one place at one time—a far cry from this case, where the warrant authorized the search of an indeterminate number of unidentified accounts.

Second, the government lacked probable cause to search everyone within the geofence. The government's case for probable cause was thin—it rested on "footage depicting the perpetrator holding a phone to his ear." Pet. App. 320a. Given the government's emphasis that only one-third of Google users have Location History enabled, it is far from clear how the government was able to show that there was even probable cause that petitioner had Location History installed. Yet based on that meager showing, the government obtained a remarkably broad warrant, covering the private data of *everyone* within the bank, the church, and the church's parking lot. Pet. App. 319a. A person's mere proximity to the crime does not give "probable cause to search that person." *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979).

The government claims that *Ybarra* is inapposite because the "analogy (if any) would be to a warrant for a bar's guest list or security-camera footage, not a bodily frisk of every patron." Resp. Br. 44-45. That analogy is inapt. The bar's guest list and security-camera footage belong to the bar and relate solely to what happened in the bar. By contrast, here, the government pulled 19 people's private information from their separate private accounts and tracked their movements both inside and outside the bank.

The correct analogy is to a warrant to search the *physical* papers of those 19 people. The government lacked probable cause to search their physical papers (*see* Pet. Br. 51), and the result should not change for virtual papers.

The government complains of the "impossibility of further specification." Resp. Br. 44. In effect, the

government claims that because it did not know *which* of the 19 accounts would have incriminating Location History, it had no choice but to review the Location History of all 19 users. But that is precisely the tactic that the Fourth Amendment forbids. The government cannot search 19 people's accounts to *find* the evidence needed to establish probable cause; it requires probable cause to search the accounts *before* the search.

IV. THE STEP TWO AND STEP THREE SEARCHES WERE UNCONSTITUTIONAL.

Even if the Step One search was constitutional, the Steps Two and Three searches were not. The government conducted additional searches at those steps: it obtained additional location information from outside the geofence at Step Two, and the users' identities at Step Three. But the warrant did not identify the subset of accounts that would be searched at those steps with particularity. Nor was there probable cause to conduct those follow-up searches. The information that led the government to focus on those accounts was found *after* the Step One search and hence never presented to the magistrate. *See* Pet. Br. 52-55.

The government insists (Resp. Br. 46) that police officers should have "discretion" and a "warrant's validity does not turn on cabining that discretion to the nth degree," but here the discretion was cabined to the 0th degree. The police had "unfettered discretion," *Steagald v. United States*, 451 U.S. 204, 220 (1981), to select the accounts that were subject to follow-up searches: the warrant identified no criteria for selecting them.

The government responds that "the probable cause that supported investigators' acquisition of Google data at step one did not cease to exist at steps two and three." Resp. Br. 47. But the probable cause in the warrant application addressed only the Step One search. The warrant stated that police would identify the accounts to be searched at Steps Two and Three based on additional information gleaned from the prior searches. JA-136-37. That additional information was not before the magistrate.

The government makes a kind of harmless-error point (Resp. Br. 47): according to the government, the evidence submitted at the outset established probable cause to receive the Step Two and Step Three information of everyone within the geofence, so the government's decision to winnow at Steps Two and Three merely reflected the government's good will.

That is incorrect. The information submitted at the outset, without more, does not establish probable cause to obtain Step Two and Step Three information for every person within the geofence. The geofence warrant covered people who might have exited the church 30 minutes before the robbery without approaching the bank, or stayed in church the whole time. There was not probable cause at the outset to tail the movements of everyone within the geofence for two hours and then deanonymize them.

Moreover, *the magistrate* did not reach that conclusion. The warrant does *not* authorize the collection of Step Two and Step Three information for all persons within the geofence. Instead, the warrant authorized the collection of Step Two and Step Three information

only from those accounts that *law enforcement* found particularly suspicious, subject to Google's review. JA-136-37. But the Fourth Amendment required *the magistrate* to make that follow-up probable-cause determination.[7]

CONCLUSION

The judgment of the Fourth Circuit should be reversed.

Respectfully submitted,

GEREMY C. KAMENS
Federal Public Defender
LAURA J. KOENIG
PATRICK L. BRYANT
Assistant Federal Public Defenders
OFFICE OF THE FEDERAL PUBLIC DEFENDER, EASTERN DISTRICT OF VIRGINIA
1650 King Street,
Suite 500
Alexandria, VA 22314

MICHAEL W. PRICE
NATIONAL ASSOCIATION

ADAM G. UNIKOWSKY
Counsel of Record
LAUREL A. RAYMOND
ANNE S. WARNKE
JENNER & BLOCK LLP
1099 New York Ave., NW
Suite 900
Washington, DC 20001
(202) 639-6000
AUnikowsky@jenner.com

DAVID A. STRAUSS
SARAH M. KONSKY
JENNER & BLOCK
SUPREME COURT AND APPELLATE CLINIC AT THE

[7] The government asks the Court to affirm based on the good-faith exception. Resp. Br. 47-48. But this Court's disposition of the Fourth Amendment question may affect the good-faith analysis. Rather than resolve an issue on which it declined to grant certiorari, the Court should remand.

OF CRIMINAL DEFENSE LAWYERS
FOURTH AMENDMENT CENTER
1600 L Street, NW
Washington, DC 20036

UNIVERSITY OF CHICAGO LAW SCHOOL
1111 E. 60th Street
Chicago, IL 60637