No. 25-112

In the Supreme Court of the United States

OKELLO T. CHATRIE, PETITIONER

v.

UNITED STATES OF AMERICA

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

BRIEF FOR THE UNITED STATES

D. JOHN SAUER
Solicitor General
Counsel of Record
A. TYSEN DUVA
Assistant Attorney General
ERIC J. FEIGIN
Deputy Solicitor General
ZOE A. JACOBY
Assistant to the
Solicitor General
ETHAN A. SACHS
Attorney

Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

QUESTION PRESENTED

Whether the government violated petitioner's Fourth Amendment rights by obtaining—pursuant to a judicial warrant—cellphone location information that petitioner sent to Google LLC.

PARTIES TO THE PROCEEDING

Petitioner (defendant-appellant below) is Okello T. Chatrie.

Respondent (plaintiff-appellee below) is the United States.

TABLE OF CONTENTS

Page

Table of Contents—Continued: Page

TABLE OF AUTHORITIES

Cases:

Cases—Continued: Page

Constitution and statutes:

Statutes—Continued: Page

Miscellaneous:

In the Supreme Court of the United States

No. 25-112

OKELLO T. CHATRIE, PETITIONER

v.

UNITED STATES OF AMERICA

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

BRIEF FOR THE UNITED STATES

OPINIONS BELOW

The opinion of the en banc court of appeals (Pet. App. 1a-142a) is reported at 136 F.4th 100. The prior order of the court of appeals (Pet. App. 143a-144a) is available at 2024 WL 4648102. An earlier panel opinion of the court of appeals (Pet. App. 145a-265a) is reported at 107 F.4th 319. The memorandum opinion of the district court (Pet. App. 264a-344a) is reported at 590 F. Supp. 3d 901.

JURISDICTION

The judgment of the court of appeals was entered on April 30, 2025. The petition for a writ of certiorari was filed on July 28, 2025, and granted on January 16, 2026. This Court's jurisdiction rests on 28 U.S.C. 1254(1).

CONSTITUTIONAL PROVISION INVOLVED

The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and

effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. Amend. IV.

INTRODUCTION

After opting to allow Google LLC to collect, store, and use information about the location of his cellphone, petitioner took that cellphone with him—and used it—when he robbed a credit union at gunpoint. He took no steps to protect his location from disclosure, such as pausing the Location History feature he had enabled or adjusting, deactivating, or forgoing his cellphone during his crime. Investigators were accordingly able to identify him as the robber through a "geofence" warrant, in which a magistrate approved a three-step procedure for law enforcement to receive up to two hours of location information—most of it anonymized—from Google about mobile devices that were archiving locations near the bank at that time. That procedure was fully consistent with the Constitution.

This Court's precedents foreclose a claim of Fourth Amendment protection from the discovery of two hours of public movements, see *United States* v. *Knotts*, 460 U.S. 276 (1983), that someone has chosen to broadcast to a third party, see *Smith* v. *Maryland*, 442 U.S. 735 (1979); *United States* v. *Miller*, 425 U.S. 435 (1976). An individual has no reasonable expectation of privacy in movements that anyone could see, that he has opted to allow a third party to analyze for its own purposes, and that are sufficiently short-term that they reveal little, if anything, about the patterns of his life—particularly when his identity remains anonymous. And the Fourth

Amendment does not recognize property-based interests that are incapable of physical intrusion, especially where neither actual property-law rights, nor ownership, nor even common-law trespass can be shown.

In any event, even for long-term involuntarily collected location data in which an individual *does* have a reasonable expectation of privacy, law enforcement can obtain such information through a warrant. See *Carpenter* v. *United States*, 585 U.S. 296 (2018). Warrants seeking information from third-party custodians that may aid in the identification of suspects or witnesses are a longstanding feature of the Fourth Amendment landscape. See *Zurcher* v. *Stanford Daily*, 436 U.S. 547 (1978). Particularly when (as with a subpoena) the custodian, rather than law enforcement, sifts the requested information out of a broader store, such warrants bear no resemblance to the "unrestrained" government "rummag[ing]" of the colonial period. *Riley* v. *California*, 573 U.S. 373, 403 (2014). That was the case with the warrant here, which was particularized to the information on Google's servers that there was probable cause to believe would identify suspects and witnesses, and which required investigators to try to minimize the scope of the information that they received.

On petitioner's view, however, law enforcement can *never* obtain *any* of the location information that he permitted Google to collect, store, and use—even with a warrant. His path to that counterintuitive result requires a number of novel Fourth Amendment innovations and would push the Court far out ahead of legislatures and common-law courts, where complex issues—such as questions about ownership of personal data, contract law on the Internet, and the proper boundary lines of online privacy—are still being debated and

developed. Petitioner's dramatic expansion of the Fourth Amendment would stifle developments in such evolving areas of law and handicap the investigation of major crimes.

And at all events, petitioner's own suppression motion would be denied based on the good-faith exception to the exclusionary rule no matter what.

STATEMENT

Following a guilty plea in the United States District Court for the Eastern District of Virginia, petitioner was convicted on one count of armed robbery of a credit union, in violation of 18 U.S.C. 2113(a) and (d); and one count of brandishing a firearm during and in relation to a crime of violence, in violation of 18 U.S.C. 924(c)(1)(A)(i) and (ii). Judgment 1. Petitioner was sentenced to 141 months of imprisonment, to be followed by three years of supervised release. Judgment 2-3. A panel of the court of appeals affirmed. Pet. App. 145a-263a. The court granted rehearing en banc, *id.* at 143a-144a, and again affirmed, *id.* at 1a-142a.

1. At approximately 4:50 p.m. on May 20, 2019, petitioner walked into the Call Federal Credit Union in Midlothian, Virginia, while appearing to talk on his cellphone. Pet. App. 265a-266a; C.A. J.A. 1445. Petitioner approached a counter and handed a teller a note that said: "I've been watching you for sometime now. I got your family as hostage and I know where you live, if you or your coworker alert the cops or anyone your family and you are going to be hurt." J.A. 132; see Pet. App. 266a. The note continued: "I got my boys on the lookout out side. The first cop car they see am going to start hurting everyone in sight." *Ibid.*

The note demanded that the teller hand over "all the cash"—"at least 100k"—and "nobody will get hurt."

Pet. App. 266a (citation omitted). After the teller replied that she did not have access to that amount of money, petitioner pulled out a silver and black firearm. *Id.* at 266a-267a. While openly holding the gun, he ordered everyone to the ground and escorted the manager and others to the credit union's safe. *Id.* at 267a. Petitioner forced the manager to open the safe and place $195,000 into a bag. *Ibid.* He then left with the money. *Ibid.*

2. Detective Joshua Hylton responded to the scene of the robbery and began interviewing witnesses and reviewing the credit union's surveillance-camera footage. Pet. App. 291a. Through his initial investigation, Detective Hylton learned that the robber had approached the credit union from the southwest corner of an adjacent church. *Ibid.* And based on footage showing the robber on his cellphone when he entered the credit union, Detective Hylton inferred that the robber might have been "speaking with a coconspirator." *Id.* at 292a (citation omitted). In mid-June, with the robber still at large despite the exhaustion of other leads, Detective Hylton applied to the Chesterfield Circuit Court of Virginia for a "geofence" warrant directed at Google LLC. J.A. 127-137.

a. A geofence warrant is an investigative tool that helps officers identify unknown suspects and witnesses of a crime using mobile-device location information collected by a third-party company. Pet. App. 151a-154a. The warrant is directed at the company and seeks information about devices that appeared within a specified geographic area (the "geofence") during a specified timeframe. *Id.* at 76a (Richardson, J., concurring); C.A. J.A. 929. The warrant is issued only if a judicial officer finds probable cause that evidence of the crime will be

found in the specified time and location window. See Pet. App. 285a.

At the time of the warrant application here, Google collected and stored cellphone location information for users who chose to activate, and enable, an optional Google service called Location History. See Pet. App. 272a-273a. The service allowed Google to generate and present users with a "Timeline" of travels; real-time traffic updates on commutes; and personalized maps and recommendations. J.A. 42; Pet. App. 168a, 270a. For example, Google used Location History to target advertisements to users based on the interests inferred from their travel patterns, and to measure when an ad resulted in a user visiting a store—features that increased Google's ad revenue. Pet. App. 270a-271a; J.A. 42, 45.

The Location History service was turned off by default. Pet. App. 273a. Users who wanted to enable it had to do so through an opt-in screen on an Internet browser, a Google application (like Google Maps), or device settings. See J.A. 44; Pet. App. 149a. A standard opt-in screen would advise the user that Location History "[s]aves where you go with your devices" and that "[t]his data may be saved and used in any Google service where you were signed in." J.A. 146. The opt-in screen also included an expansion arrow, which when clicked would note that "Google regularly obtains location data from your devices * * * even when you aren't using a specific Google service." J.A. 147. To enable Location History, the user had to select "TURN ON" rather than "NO THANKS." J.A. 146.

Even if the user opted into Location History, actual collection and storage of location data from a device required other affirmative steps. As a threshold matter,

the user would have to activate the device-location setting on the user's mobile device. J.A. 43. In addition, the user had to enable another "subsetting" called "'Location Reporting'" for the particular device for which he wanted Google to collect and store Location History information. See J.A. 44. And beyond that, the user had to sign into his Google account on that device. *Ibid.* The user also had the ability, at any time, to request deletion of previously stored location data or to pause the collection of additional data. See Pet. App. 281a-283a.

Only about one-third of active Google accountholders actually opted into the Location History service. Pet. App. 274a. For those who did, information from periods when they allowed location data to be collected, processed, and retained was stored in Google's "Sensorvault" database. *Id.* at 273a; J.A. 44. The accuracy of a mobile device's data, which was collected at intervals of two minutes or longer, depended on its source (*e.g.*, cell sites, WiFi, GPS) and could vary from likely being within a few meters to hundreds of meters of the device's location. See Pet. App. 274a, 302a. For each Location History point, Google's information included a "confidence interval" circle with an estimated 68% likelihood of containing the mobile device. *Id.* at 274a.

b. The warrant application in this case included an affidavit that described the facts of the robbery, including the robber's cellphone use when he entered the credit union and the demand note's reference to accomplices. J.A. 132; Pet. App. 292a, 297a. The application also explained, *inter alia*, that most cellphones are smartphones; that "[n]early every" Android cellphone "has an associated Google account"; and that Google "collects and retains location data" from mobile devices

when a user enables it to do so. J.A. 133; see J.A. 127-137.

The application explained that location-history information can, *inter alia*, "tend to identify potential witnesses and/or suspects," and to "aid investigators in possibly inculpating or exculpating persons of interest." J.A. 133. And the application sought information about devices within 150 meters of a specific latitude and longitude point near the bank within half an hour (4:20 p.m. to 5:20 p.m.) of the robbery. Pet. App. 294a-295a; J.A. 137.

A state magistrate found probable cause to issue the warrant, which authorized the disclosure of information in three steps. Pet. App. 294a-296a. At step one, Google would provide anonymized location information from accountholders reporting device locations in the geofence during the specified time, including "a numerical identifier for the account, the type of account, time stamped location coordinates and the data source that this information came from if available." J.A. 136; see Pet. App. 295a. Steps two and three then required officers, as a prerequisite to receiving any additional information, to "attempt to narrow down the list" of potentially relevant accounts by reviewing the step-one information and comparing it to "the known time and location information that is specific to th[e] crime." J.A. 136, 137.

Specifically, at step two, after undertaking the requisite minimization efforts, law enforcement could request and receive additional anonymized location data for accounts identified as relevant: location information for two hours (one hour before the robbery to one hour after), both inside and outside the geofence. Pet. App. 296a; J.A. 136-137. Finally, at step three, after further efforts to "narrow down the list," officers could request

and receive deanonymized information about a specific requested set of accounts, including usernames and e-mail addresses. J.A. 137; Pet. App. 296a.

c. In this case, at step one, Google provided a chart showing that 19 unique devices had registered locations within the geofence at 209 discrete moments between 4:20 and 5:20 p.m. J.A. 169-175. The chart's entries included latitude and longitude coordinates and the radius of a circle around those coordinates within which Google estimated a 68% likelihood that the device was located. *Ibid.* Although Google's internal design choices required it to query "all Location History data" in its database to obtain that information, Pet. App. 287a (brackets, citation, and emphasis omitted), law enforcement saw only the location updates of 19 accounts from the vicinity of the credit union within half an hour of the robbery.

At step two, Detective Hylton initially asked Google for data regarding all 19 accounts, but Google's reservations about that request led him to ultimately narrow his request to 9 of the 19 accounts. See Pet. App. 299a-300a. Consistent with the process outlined in the warrant, Google provided Detective Hylton with one hour of additional location information for those nine accounts—"30 minutes prior and 30 minutes following the original geofence time frame with no restraints on location"—in the same form as the step-one returns. J.A. 115; see J.A. 114-115, 180-200.

Between steps two and three, investigators ultimately excluded all but three devices. Pet. App. 300a-301a. The first two devices had traveled a path suggesting that they might belong to a driver who dropped off the robber, drove away, and then returned to pick him up. See J.A. 123-126; C.A. J.A. 2014, 2016. The third

device returned results suggesting that it belonged to the robber himself: it appeared within the geofence during the ten minutes before the robbery, then headed away from the geofence toward a residential area. See C.A. J.A. 2008.

At step three, Detective Hylton asked Google to "unmask" each of the three suspicious devices by producing the subscriber information associated with each of them. See J.A. 109. For each of those three devices, Google produced a Google account ID and basic subscriber information like the user's name and e-mail address associated with that ID. See J.A. 206-208. From that subscriber information, investigators learned that the third device—which they believed to be associated with the robber himself—was registered under petitioner's e-mail address, which includes his first and last names. See J.A. 121. As later became clear, petitioner had both chosen to opt into Location History about ten months before the robbery, J.A. 145, and left it enabled when robbing the credit union.

d. Following up on the warrant, officers discovered that petitioner had recently purchased a pistol of the same type used in the robbery. J.A. 121, 145; C.A. J.A. 1445-1446. Upon obtaining and executing federal warrants for residences associated with him, they found two robbery-style demand notes in petitioner's bedroom; nearly $100,000 in U.S. currency, including bills wrapped in bands signed by the victim teller; and a silver and black 9mm semi-automatic pistol. C.A. J.A. 1446. After petitioner was placed under arrest and advised of his *Miranda* rights, he confessed to committing the robbery and to using the 9mm semiautomatic pistol during the robbery. *Ibid.*

3. A federal grand jury in the Eastern District of Virginia returned a two-count indictment against petitioner, charging him with armed credit-union robbery and brandishing a firearm during and in relation to a crime of violence. Indictment 1-3. Petitioner moved to suppress all information that Google had produced pursuant to the geofence warrant, as well as the fruits of that information. C.A. J.A. 25-50. After holding an evidentiary hearing, the district court denied the motion to suppress based on the good-faith exception to the exclusionary rule. Pet. App. 264a-344a. Petitioner entered a conditional guilty plea to both counts, reserving his right to appeal the denial of his motion to suppress. See C.A. J.A. 1428-1443.

A divided panel of the court of appeals affirmed. Pet. App. 145a-187a (majority opinion), 187a-263a (Wynn, J., dissenting). The majority explained that execution of the warrant did not constitute a "search" under the Fourth Amendment, because petitioner "did not have a reasonable expectation of privacy in two hours' worth of Location History data voluntarily exposed to Google." Pet. App. 156a. It observed that the limited amount of information was not "an 'all-encompassing record of [petitioner's] whereabouts.'" *Id.* at 166a (quoting *Carpenter* v. *United States*, 585 U.S. 296, 311 (2018)). And it emphasized that petitioner "voluntarily exposed his location information to Google by opting in to Location History." *Id.* at 168a.

4. After granting rehearing en banc, Pet. App. 143a-144a, the en banc court of appeals affirmed the denial of petitioner's motion to suppress in a single-sentence per curiam opinion. *Id.* at 4a. Fourteen of the 15 judges voted to affirm the district court's decision, with nine expressly finding that the good-faith exception applied.

See *id.* at 5a-22a (Diaz, C.J., concurring); *id.* at 35a (Niemeyer, J., concurring); *id.* at 36a (King, J., concurring); *id.* at 38a n.1 (Wynn, J., concurring in the judgment); *id.* at 97a-99a (Heytens, J., concurring).

SUMMARY OF ARGUMENT

Petitioner affirmatively opted to allow Google to collect, store, and use location information derived from a cellphone that he employed during his armed robbery. Investigators were accordingly able to identify him through a magistrate-issued warrant to Google for short-term location information about mobile devices that registered locations near the robbery around the time it occurred. The investigators did not violate petitioner's Fourth Amendment rights by doing so.

I. As a threshold matter, petitioner lacks a cognizable Fourth Amendment interest in the information that Google provided to law enforcement. The Court has made clear that an individual lacks a reasonable expectation of privacy in information that he "assumed the risk" of sharing with others, *Smith* v. *Maryland*, 442 U.S. 735, 745 (1979), including about his short-term public movements, *United States* v. *Knotts*, 460 U.S. 276, 281-283 (1983). The warrant here sought movement information visible to anyone near petitioner when he robbed the credit union, and the inquiry it specified was closely analogous to what Google itself regularly did with opting-in users' recorded Location History. Anonymized information akin to what investigators received in step one was used by Google to target ads and gauge their effectiveness, and information akin to steps two and three was used to give traffic updates for users' commutes.

Even collapsing all three steps of the warrant, they amounted to two hours of technologically enhanced

location-tracking—which this Court has allowed investigators to obtain even without either voluntary disclosure or a warrant. See *Knotts*, 460 U.S. at 277. Unlike seven days of cell-site location information (CSLI), which can implicate reasonable privacy expectations by showing patterns that reveal the "privacies of life," *Carpenter* v. *United States*, 585 U.S. 296, 311 (2018) (citation omitted), a single journey, or single stop, says little about a person's overall life. And unlike CSLI, which every user must share to make a cellphone functional, Google's Location History here was an optional add-on; enabled only through multiple affirmative acts; temporarily, permanently, and even retroactively undoable; and not even activated by two-thirds of Google accountholders.

Petitioner's primary argument—that he had property rights in the information Google possessed—was forfeited below and lacks analysis by any lower court. And it would be an unwarranted extension of the Fourth Amendment to find a property interest without any physical intrusion, any clear recognition of the information as property, any evident vesting of any property rights in petitioner as opposed to Google, or even any common-law trespass. This Court should not take such leaps in areas of constitutional and property law where legislatures and lower courts are treading cautiously.

II. Even assuming that petitioner's Fourth Amendment rights were implicated, the issuance of and compliance with the warrant ensured that any search was reasonable. See *Carpenter*, 585 U.S. at 319. This Court has long recognized the validity of "third party" warrants for evidence that may identify as-yet-unknown witnesses or suspects. See *Zurcher* v. *Stanford Daily*, 436 U.S. 547, 553-560 (1978). The warrant here was

based on probable cause to believe that Google had information that would help to identify the cellphone-using robber, the accomplices whom his demand note referenced, and people who might have seen them. And it sought particularized information from Google's database in a particularized form.

Indeed, the warrant simply directed Google to locate and turn over the necessary information, such that investigators themselves saw only a minuscule slice of data in Google's database. Even that small slice was further narrowed, as the warrant directed investigators to try to minimize the scope between steps. Contrary to petitioner's suggestion, Google (which raised objections during the process) was no more the government's "agent" than any warrant or subpoena recipient is. And investigators' obligation to minimize the scope of successive steps was a privacy-*protective* minimization feature, not a fatal transformation into a "general warrant" of uncabined discretion.

III. At bottom, petitioner's arguments seem to imply that no geofence warrant, of any sort, could ever be executed. There is no sound reason to embrace such a senseless and harmful result—let alone to reverse a lower-court judgment that rests on the objective good faith of the investigators' efforts here.

ARGUMENT

I. PETITIONER HAD NO FOURTH AMENDMENT INTEREST IN SHORT-TERM INFORMATION ABOUT HIS CELLPHONE'S MOVEMENTS THAT HE ALLOWED GOOGLE LLC TO COLLECT, STORE, AND USE

Although investigators prophylactically secured a warrant in this case, their receipt of short-term location information from Google was not actually a Fourth Amendment "search" that might require one. As one of

the minority of Google accountholders who opted into Location History, petitioner had no reasonable expectation of privacy in any of the limited information disclosed at each step of the warrant's execution. And petitioner's unpreserved claim of a novel property-based interest—now his lead argument—lacks sound footing in any source of law, constitutional or otherwise.

A. Petitioner Had No Reasonable Expectation Of Privacy In The Short-Term Location Information, Which He Voluntarily Authorized Google To Collect

Absent "'physical intrusion of a constitutionally protected area,'" a Fourth Amendment "search" occurs only "when government officers violate a person's 'reasonable expectation of privacy.'" *United States* v. *Jones*, 565 U.S. 400, 406-407 (2012) (citations omitted). The warrant here did not require any "physical intrusion," so this case was resolved below under the reasonable-expectation-of-privacy framework. See Pet. App. 171a n.20. And petitioner had no reasonable expectation of privacy in the limited location information that Google provided, which petitioner had authorized Google to collect, retain, and use for its own purposes.

1. This Court's precedents do not support a reasonable expectation of privacy in voluntarily disclosed short-term public movements

This Court has long recognized that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith* v. *Maryland*, 442 U.S. 735, 743-744 (1979). The Court has held, for example, that an individual lacks a reasonable expectation of privacy in a confession to a trusted confidante, see, *e.g.*, *Lopez* v. *United States*, 373 U.S. 427, 438 (1963); checks and other financial information in

possession of a bank, see *United States* v. *Miller*, 425 U.S. 435, 436-437 (1976); or the phone numbers that he asks the telephone company to call, see *Smith*, 442 U.S. at 744.

The third-party doctrine applies even if the disclosing party subjectively expects the information to stay confidential. For example, the Court has "unanimously rejected" the contention "that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it." *Hoffa* v. *United States*, 385 U.S. 293, 302 (1966). And the Court has held "that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Miller*, 425 U.S. at 443. Bank depositors and telephone dialers alike "assume[ ] the risk" that their transaction and call histories "w[ill] be divulged to police." *Smith*, 442 U.S. at 745; see *Miller*, 425 U.S. at 443.

Although the Court has never questioned the third-party doctrine as a general matter, the Court's decision in *Carpenter* v. *United States*, 585 U.S. 296 (2018), reasoned that the "unique nature" of the privacy interest in seven days of CSLI invariably collected from all active cellphones was so strong that possession by a third party "d[id] not by itself overcome" a "claim to Fourth Amendment protection." *Id.* at 309; see *id.* at 310 n.3. Even before *Carpenter*, a majority of Justices in *Jones* had expressed the view that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." 565 U.S. at 430 (Alito, J.,

concurring in the judgment); see *id.* at 415 (Sotomayor, J., concurring). But in contrast to such longer-term information, this Court has found no reasonable expectation of privacy in short-term information about public movements.

In *United States* v. *Knotts*, 460 U.S. 276 (1983), the Court considered the use of a beeper to track a container of chloroform as it was driven from Minneapolis to Shell Lake, Wisconsin. *Id.* at 277. The Court held that no Fourth Amendment "search" had taken place, because a "person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *Id.* at 281. The Court explained that the same information could have been gathered by "[v]isual surveillance from public places" along the route. *Id.* at 282. And the Court has never retreated from its recognition that such technologically enhanced surveillance—akin to what was possible even "[p]rior to the digital age," *Carpenter*, 585 U.S. at 310—is constitutionally permissible.

Neither *Jones* nor *Carpenter* disturbed *Knotts*'s logic. *Jones*, while acknowledging the holding in *Knotts*, held only that law-enforcement installation of a GPS tracker for 28 days on a car was an impermissible warrantless physical intrusion, 565 U.S. at 403, 409; see *id.* at 430 (Alito, J., concurring in the judgment). And the "narrow" decision in *Carpenter* addressed seven days or more of CSLI records that wireless carriers collected every time a phone was receiving cell service, whether or not the user chose to allow such collection. See 585 U.S. at 310 n.3, 314-316. Recognizing the continuing validity of *Knotts*, see *id.* at 307, *Carpenter* distinguished such monitoring "'for a very long period'"

from surveillance "for a brief stretch." *Id.* at 310 (citation omitted).

2. Google's disclosures in response to the warrant did not violate any reasonable expectation of privacy

The information that Google disclosed to law enforcement here concerned only petitioner's short-term public movements. And he "voluntarily conveyed," *Smith*, 442 U.S. at 744, that information to Google by opting to have Google collect, process, use, and store his movements through the optional Location History service on his phone. He did not have a reasonable expectation of privacy in that information.

a. As a threshold matter, any claim to a reasonable expectation of privacy is especially misplaced with respect to the information that investigators obtained at step one of the warrant: *anonymized* information about the location of petitioner's cellphone (along with 18 others) within 150 meters of the credit union within half an hour of the robbery. See Pet. App. 273a-274a. Although petitioner asserts (Br. 23-24) that step one of the warrant exposed "private information," he fails to explain how he reasonably expected the information that *someone* was near the credit union at the time of the robbery to remain "private."

To the contrary, while at the credit union, petitioner exposed his presence to view by other people, security cameras, and potentially even law enforcement. Those viewers may not have known who he was, but Google did not share that information at step one. Petitioner does not suggest that his identity could be derived solely from his movements within a single hour and 150 meters of the credit union, which was open for business. Even if it could, *Knotts* held that even a *known* suspect who was "travel[ing] over the public streets" was "voluntarily

convey[ing] to anyone who want[s] to look the fact that he was travelling over particular roads in a particular direction" and "the fact of whatever stops he made." 460 U.S. at 281-282. And petitioner is particularly ill-situated to claim a reasonable expectation of privacy because, while he was robbing the bank, he was voluntarily broadcasting his phone's location to Google.

Google for its own purposes collected and used location information in a manner similar to step one of the warrant. Google targeted ads using "radius targeting," which served ads to users based on their proximity to a specified location. C.A. J.A. 614. And it also used Location History to measure "how many users who saw a particular ad actually went to" the advertised stores and then provided advertisers generalized information about the results. *Id.* at 613; see Pet. App. 271a. Even if that information might have been somewhat more abstract than the step-one information here, see C.A. J.A. 615, nothing suggests that petitioner had a right to keep even his *anonymous* information private. Cf. J.A. 70 (privacy policy notifying users that "[w]e may share non-personally identifiable information publicly and with our partners").

b. Petitioner also did not have a reasonable expectation of privacy in the two hours of location information disclosed at steps two and three of the warrant's execution. Although that information was, at step three, deanonymized, it falls squarely within the parameters of *Knotts*. The journey from Minneapolis to Shell Lake at issue there, which involved suspects whose identities were known at the time, took even longer than two hours, as Knotts's coconspirators made—and were permissibly observed to have made—stops at private residences along the way. See J.A. 26-30, *Knotts*, *supra*

(No. 81-1802) (officer testimony about visual and beeper surveillance between 10 a.m. and 4:30 p.m.). Petitioner had no more of a reasonable expectation of privacy in two hours of his public movements than existed in *Knotts*.

Even assuming that the location of a person's cell-phone is his own location, cf. C.A. J.A. 833-834, that short a time window reveals little about the details of petitioner's personal life. A key distinction between the hours in *Knotts* and this case, and the week or four weeks in *Carpenter* and *Jones*, is the latter's much higher likelihood of showing the repeated patterns that reveal "privacies" such as "familial, political, professional, religious, and sexual associations," *Carpenter*, 585 U.S. at 311 (citations omitted); see Pet. App. 165a (panel opinion). A single stop at a doctor's office, for example, does not in itself identify the reason for the visit—or even whether the person is a patient, as opposed to an accompanying companion, pharmaceutical sales representative, or any other person who might once stop in.

Petitioner, for example, parked at a church not to engage in religious worship, but as a staging area to rob a bank. See C.A. J.A. 966. The possibility that the purpose of a stop (or, at step two, the potential identity of the still-anonymous traveler, cf. J.A. 209) might be inferred does not create a reasonable expectation of privacy in the location information itself. A person would not have a reasonable expectation of privacy in the fact that he was parked for two hours behind an office building simply because his law firm's website lists that building's street address as its place of business, even if the additional information raises the likely inference that he was at work during that time. The ability to

draw connections based on further legwork does not give rise to reasonable expectations of privacy in the location information itself.

Any potential privacy concerns were further mitigated by petitioner's sharing of his location with Google during his arrival at, robbery of, and flight from the credit union. This Court's third-party decisions make clear that petitioner "assumed the risk" that any subjective belief in the information's confidentiality would not be controlling. *Smith*, 442 U.S. at 745; *Miller*, 425 U.S. at 443. Those decisions also show that even financial records—which can reveal not only *where* someone was but *why* they were there (*e.g.*, to purchase medical services)—cannot reasonably be expected to remain private in a third party's hands. See *Miller*, 425 U.S. at 443. Nor does petitioner plausibly establish that the nature and permitted uses of Location History are akin to "emails on Google's Gmail service" or "documents on Google drive." Pet. Br. 16 (quoting J.A. 20).

In allowing Google to collect and use his location information here, petitioner permitted Google to analyze it for patterns in ways far more intrusive than would be possible from the limited two-hour window that Google shared with law enforcement. For example, showing an "ad for ski equipment" to a user whose Location History reveals that she "regularly frequents ski resorts," J.A. 45, requires far more analysis than a two-hour time window would allow. The same is true of traffic updates for a commute, J.A. 64—which require Google to determine the existence and purpose of a repeated journey—or other personalized services based on routine activity.

3. Petitioner's contrary arguments are unsound

Petitioner provides no sound basis to declare a reasonable expectation of privacy in any of the information

at issue here—let alone all of it, including anonymized information. Instead, he presses arguments under which even a moment's worth of Location History information, placing a user at a crowded and public place, would—counterintuitively—be constitutionally protected.

a. The reasons why the Court declined to apply its third-party precedents in *Carpenter* are not present here. The Court emphasized there that CSLI—which a cellphone must generate for "[v]irtually any activity"—is "indispensable to participation in modern society"; is collected "without any affirmative act on the part of the user beyond powering up"; and gives users "no way to avoid leaving behind a trail of location data." *Carpenter*, 585 U.S. at 315. Location History information differs in all three respects.

First, Location History is far from "indispensable." Even for those who enjoy Google Android phones or Google apps, opting into Location History is "unnecessary to use a phone or even to use apps like Google Maps." Pet. App. 94a (Richardson, J., concurring); see J.A. 42 (noting that Google Maps does "not require a user to have an account"). The vast majority of the world's population goes about their daily lives without Location History. Even among Google accountholders, only one third—a clear minority—made the choice that petitioner did to enable it. J.A. 145.[1]

---

[1] Even if the denominator of that fraction includes people "who never downloaded a Google app and were thus never presented with the choice" to opt into Location History as petitioner did, Pet. App. 120a-121a (Berner, J., concurring), that simply underscores how many Google accountholders have no need or desire for the services that Location History enables. The "numerous tens of millions" of Location History adopters, *id.* at 270a (citation omitted), comprise a

Second, activating Location History requires the sort of "affirmative act," *Carpenter*, 585 U.S. at 315—indeed, several of them—that activation of CSLI did not. Location History is an optional setting that is turned off by default. See J.A. 42; Pet. App. 278a. To activate the service, petitioner had to take four independent steps: (1) turn on the "device-location setting" on his cellphone; (2) opt into the Location History feature for his Google account settings; (3) enable the Location Reporting feature on his cellphone; and (4) sign into his Google account on a specific phone. J.A. 43-44.

Third, while disabling CSLI required "disconnecting the phone from the network" altogether, *Carpenter*, 585 U.S. at 315, turning off the "trail of location data," *ibid.*, that a user has opted into through Location History required no such dramatic step. As the district court found, petitioner could have asked Google to pause the collection of his Location History—during the robbery or at any other time—through any "app that use[d] Location History," "the device level settings," or by logging into a website. Pet. App. 282a (citations omitted).

While he might have been warned that turning off Location History would "limit" the functionality of certain applications, Pet. App. 282a (brackets and citation omitted), the choice between an uninterrupted record of data and privacy during a robbery was entirely in petitioner's hands. See *id.* at 283a-284a. Even if the user interface for pausing the collection of data was less clear than it could have been, see *ibid.*, petitioner "assumed the risk" of detection, *Smith*, 442 U.S. 744, when he left his Location History timeline intact while the robbery was under investigation.

---

small subset of the absolute number of accountholders, total users of Google products, and global inhabitants.

b. Petitioner's efforts to analogize the information that he allowed Google to collect here to the seven days of CSLI at issue in *Carpenter* are misplaced. Petitioner asserts (Br. 24), for example, that Location History data is at least as precise, or potentially more precise, than CSLI. But it is not clearly any more precise than what a modern-day beeper akin to the one at issue in *Knotts*—or, for that matter, actual visual observation—would allow. That is particularly so because the information is presented in confidence intervals, which may have a wide radius. See Pet. App. 302a.

In any event, for a short public trip that reveals only physical motion, "scientific enhancement of this sort raises no constitutional issues which visual surveillance would not also raise." *Knotts*, 460 U.S. at 285. While Fourth Amendment rights may be infringed by the warrantless employment of "a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion," *Kyllo* v. *United States*, 533 U.S. 27, 40 (2001), petitioner does not claim that anything like that happened to him here.[2]

Petitioner also notes (Br. 24) that here, as in *Carpenter*, law enforcement obtained location information retrospectively, rather than through contemporaneous monitoring of someone's movements. But an individual

[2] To the extent that Google's mobile-device-location confidence intervals suggested someone's potential presence in a private residence, any claim of Fourth Amendment rights would be that person's, not petitioner's. See *United States* v. *Karo*, 468 U.S. 705, 719-721 (1984) (distinguishing which particular individuals had Fourth Amendment rights in interior of a home where beeper was taken). And it is far from obvious that any such claim would succeed, given the potential width of the confidence interval, Google's anonymization, and the opt-in nature of Location History.

who exposes his travel to public view does not acquire a reasonable expectation of privacy simply because he believes that he has managed to make it to his destination unobserved. Were it otherwise, a suspect would have a right of privacy from the observations of not only a beeper but *any* physical observation—by the police or any later-cooperating witness—that he did not happen to notice. It was accordingly "[c]ritical[]" to *Carpenter*'s retrospectivity analysis that CSLI was "continually logged for all of the 400 million devices in the United States," thereby creating a "newfound tracking capacity" that ran "against everyone." 585 U.S. at 312. The same is not true of Location History, which includes only the users who opt in.

c. Attempting to avoid the consequences of that choice, petitioner argues (Br. 28-31) that it was not truly voluntary. He contends, in essence, that he was bullied or tricked into becoming one of the one-third of Google accountholders who enabled Location History, and left in the dark as to how to discontinue it, pause collection, or request deletion of historical information. If accepted, his argument could have widespread implications for the enforceability of online agreements—users could employ a similar rationale to avoid the implication of terms, like arbitration clauses, that they were notified of and opted into. And in this case, the argument is not supported by the record.

Before petitioner could enable Location History, a Google prompt explained that Location History "[s]aves where you go with your devices" and that "[t]his data may be saved and used in any Google service where you were signed in to give you more personalized experiences." J.A. 146. Clicking the expansion arrow on Google's prompt would have further informed

petitioner that to save his information, "Google regularly obtains location data from your devices," "even when you aren't using a specific Google service." J.A. 147. A reasonable user faced with that information would understand that by opting in to the service, he was authorizing Google to track and save his location information. See Pet. App. 185a.

Petitioner complains (Br. 31) that Google's prompts did not explain exactly how frequently Google would collect location information or how precise it would be. But this Court has never suggested—even in the context of bargaining away constitutional rights in a plea agreement—that such detail is necessary to make consent knowing and voluntary. See *United States* v. *Ruiz*, 536 U.S. 622, 629 (2002) (voluntariness of waiver depends on knowing "how it would likely apply in general," regardless of "the specific detailed consequences") (emphases omitted). Indeed, if the agreement had been more detailed, it would provide fuel for the flip-side objection that the prompt was too long to read.

If petitioner, or any other user, wanted more information about Location History, the user could have consulted the privacy policy that Google provided and periodically updated. See J.A. 53-93. The additional information there belies petitioner's assertion (Br. 31) that he "was not told his data would be shared with the government." Google's privacy policy did, in fact, inform users that Google would share personal data outside of Google (such as with the government) if Google believed in good faith that disclosure was "reasonably necessary" to comply with "legal process" or to "[p]rotect" public "safety." J.A. 69-70. Thus, to the extent that it was even necessary, but see *Miller*, 425 U.S. at 443, petitioner had notice that he had signed onto a service that

would create records disclosable to law enforcement during the time that he was robbing the credit union. Furthermore, although Google cannot confirm whether petitioner specifically received additional notifications, shortly before the robbery, Google began periodically reminding users that they had opted in. See J.A. 151-152; C.A. J.A. 772-774.

Petitioner suggests (Br. 29-33) that Google forced users' hands by prompting them to enable Location History "several times," and by stating that Location History was necessary to "get the most from" certain apps and ensure that they "work correctly." As a threshold matter, the experts below could not "say *exactly* which software pathway [petitioner] would have seen when he enabled Location History," so it is unknown whether those particular prompts were actually displayed when petitioner enabled Location History. Pet. App. 277a; see Pet. Br. 29 n.3. In any event, petitioner's involuntariness argument undercuts the validity of online transactions; cannot be squared with the fact that two-thirds of Google accountholders did not enable Location History, J.A. 45; and cannot explain why he was unable to pause collection before committing the robbery.

d. Notwithstanding his own choices, petitioner asserts that he could nonetheless have been confident in the confidentiality of Location History information on the theory that this Court's decisions about third-party disclosures apply only to "business records" that are kept for "'legitimate business purposes.'" Pet. Br. 25 (citation omitted); *id.* at 28. But that claim is at odds with *Smith* v. *Maryland*, which made clear that "the fortuity of whether or not the phone company in fact elects to make a quasi-permanent record" of dialed phone numbers "does not * * * make any constitutional

difference." 442 U.S. at 745. The key point instead was that the defendant "voluntarily conveyed" information to the company that it was "free to record" if it chose to. *Ibid.*; cf. *Couch* v. *United States*, 409 U.S. 322, 327, 335 (1973) (applying voluntary-disclosure principle to business records owned by the defendant, not third-party accountant).

It is the voluntary disclosure itself—not what the recipient does with it or why—that "assume[s] the risk that the information would be divulged to police." *Smith*, 442 U.S. at 743; see *id.* at 745; *Miller*, 425 U.S. at 443. Far from being limited to "legitimate business purposes," the voluntary-disclosure principle has been applied equally to personal interactions that have nothing to do with a company's business. See, *e.g.*, *Hoffa*, 385 U.S. at 301-302. In any event, even if a court were required to evaluate the existence of a "legitimate business purpose," Google clearly had one here: as the district court found, Google used Location History to "support[ ]" its "advertising revenue." Pet. App. 270a-271a.

e. Finally, although petitioner did not raise any statutory claim under the Stored Communications Act (SCA) below, see Pet. App. 128a n.5 (Berner, J., concurring), he argues, in essence, that he would have prevailed had he done so, and that a warrant requirement under a provision of the SCA, 18 U.S.C. 2703(a), should carry over to the Fourth Amendment as well. Section 2703(a) imposes a warrant requirement for obtaining "the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less." 18 U.S.C. 2703(a). Petitioner's reliance on that provision is misplaced on several levels.

To begin with, a true reasonable expectation of privacy would suggest an ongoing—not just 180-day—warrant requirement. Petitioner also does not address whether, in this context, Location History information would fall within Congress's express exclusion of any "communication from a tracking device," defined as "an electronic or mechanical device which permits the tracking of the movement of a person or object," from the definition of "electronic communication." 18 U.S.C. 2510(12)(C), 3117(b). And at all events, Congress's choices in this area reflect, if anything, its view that the proper way to address privacy with respect to evolving online technologies is tailored legislation—not the creation of constitutional rules that would foreclose informed legislative efforts.

B. Petitioner's Unpreserved And Unexamined Property-Based Theory Lacks Foundation

Petitioner provides no basis on which he can avoid the consequences of failing to carry his burden to show a reasonable expectation of privacy. See *Rawlings* v. *Kentucky*, 448 U.S. 98, 104 (1980) (burden on defendant). His new lead theory (Br. 15-22) is one that he failed to preserve in the court of appeals, and which no judge below explored in depth, let alone accepted—namely, that his Fourth Amendment rights were violated by a trespass-like intrusion on his personal property. That theory is not properly presented here; is not grounded in Fourth Amendment doctrine; gets far out ahead of ongoing debates in tort and property law; incorrectly presumes that any property interest would belong to him, rather than Google; and asserts a trespass where none occurred.

1. This Court should not be the first to address petitioner's property theory

At the panel stage, the court of appeals found that petitioner "forfeited his right to raise this issue on appeal" by failing to "advance this claim in the argument section of his opening brief." Pet. App. 171a n.20. In his petition for rehearing en banc, petitioner "request[ed] the opportunity for rebriefing" to address the property-based argument, C.A. Pet. for Reh'g 18-19, but the en banc court did not grant that request. Only one en banc opinion even addressed the argument, rejecting it in a footnote. Pet. App. 95a n.21 (Richardson, J., concurring).

That alone is reason to reject the argument here. Because this Court "is 'a court of review, not of first view,'" it rarely reviews matters that were not properly raised before or passed upon by the court of appeals. *Byrd* v. *United States*, 138 S. Ct. 1518, 1527 (2018) (citation omitted). And it would be particularly inappropriate to do so where adoption of petitioner's theory would require the Court to make pronouncements on evolving areas of property law (a traditional subject of state legislation) that could deter or foreclose further developments.

2. Petitioner's novel property-based theory lacks merit

Nor does petitioner provide a sound basis for his property theory on the merits. To the contrary, that theory is not supported by any current source of law.

a. Petitioner characterizes his claim as grounded in the traditional "common-law trespassory test" that governed before the reasonable-expectation-of-privacy framework adopted in *Katz* v. *United States*, 389 U.S. 347 (1967). Pet. Br. 14 (citation omitted). But only under *Katz*'s privacy framework has this Court ever found

purely electronic information-gathering to constitute a Fourth Amendment search. See, *e.g.*, *Carpenter*, 585 U.S. at 310; *Kyllo*, 533 U.S. at 34 (thermal imaging).

While "physical intrusion" retains independent constitutional significance, *Jones*, 565 U.S. at 404, "[s]ituations involving merely the transmission of electronic signals without trespass," or "physical contact," "remain subject to *Katz* analysis," *id.* at 411 (emphasis omitted). Compare *ibid.* (physical intrusion of GPS device), and *Florida* v. *Jardines*, 569 U.S. 1, 7 (2013) ("unlicensed physical intrusion" of drug-sniffing dog on porch), with *Carpenter*, 585 U.S. at 309-316 (applying *Katz* to CSLI). This case, like *Carpenter*, involves only nonphysical information.

Carpenter, moreover, recognized that the Court has in fact "decoupled violation of a person's Fourth Amendment rights from trespassory violations of his property." 585 U.S. at 304 n.1 (quoting *Kyllo*, 533 U.S. at 32). Even in the physical realm, Fourth Amendment interests have never been treated as coterminous with trespass rights. For example, the Court recognized over a century ago that "the special protection accorded by the Fourth Amendment to the people in their 'persons, houses, papers, and effects' is not extended to the open fields" that someone may own. *Hester* v. *United States*, 265 U.S. 57, 59 (1924) (Holmes, J.). Law enforcement can therefore trespass on such land without committing a constitutional violation. See *id.* at 58.

b. Even assuming the Court were to analyze a purely electronic investigation under a property framework, petitioner provides no sound basis for holding that "private data like Location History" is "property for Fourth Amendment purposes," Br. 19. As a threshold matter, the Fourth Amendment "does not protect possessory

interests in all kinds of property." *Soldal* v. *Cook County*, 506 U.S. 56, 62 n.7 (1992). The Court has explained that the Fourth Amendment "term 'effects' is less inclusive than 'property,'" the term that appeared in Madison's original proposal. *Oliver* v. *United States*, 466 U.S. 170, 176 (1984) (citation omitted). And given the Framers' focus on records containing "'personal or speech-related confidences,'" it is "not obvious" that location records would "satisfy the original meaning of 'papers.'" *Carpenter*, 585 U.S. at 351 n.8 (Thomas, J., dissenting) (quoting Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 Va. L. Rev. 869, 923-924 (1985)).

Regardless, even assuming anything labeled "property" is protected under the Fourth Amendment, "American law has generally refused to recognize property rights in data" as such. Steven H. Hazel, *Personal Data as Property*, 70 Syracuse L. Rev. 1055, 1057 (2020); see Pamela Samuelson, *Privacy as Intellectual Property*, 52 Stan. L. Rev. 1125, 1130-1131 (2000). The fact of a person's name, age, or location at some particular time is not readily understood as something that a person can "own." Nor is "raw data" intellectual property; only an "original" selection, coordination, or arrangement of facts is copyrightable. *Feist Pubs., Inc.* v. *Rural Tel. Serv. Co.*, 499 U.S. 340, 361-362 (1991).

To the extent that petitioner's property argument relies on written terms of service or polices about petitioner's relationship with Google, any *contract* rights those documents might create would not in themselves create *property* rights enforceable under the Fourth Amendment. A nondisclosure agreement between criminal conspirators does not create a property right (or even an enforceable right) against one of them talking to the government. Cf. *Hoffa*, 385 U.S. at 302. By the

same token, without any underlying property right that the Fourth Amendment would otherwise incorporate, there is no property right for any agreement between petitioner and Google to allocate. And petitioner identifies no such underlying property right here.

While petitioner observes (Br. 19) that the Founding Era common law recognized certain intangible interests as property, those interests were tied to land and material things—*e.g.*, "future possessory interests" in real and personal property, and "'incorporeal hereditaments'" like "easements and profits in land." Gregory S. Alexander, *Time and Property in the American Republican Legal Culture*, 66 N.Y.U. L. Rev. 273, 333 (1991) (citation omitted). Petitioner cites (Br. 20) *Entick* v. *Carrington*, 19 How. St. Tr. 1029 (C.P. 1765), in which Lord Camden observed that a warrant for a man's "papers" was broad enough to cover not only "libellous papers" but also "all [his] manuscripts." *Id.* at 1065. But Lord Camden's observation says nothing about whether purely factual information, like where someone was at a particular time, was likewise considered one of his "papers"—or, indeed, his "property" at all.

Even if some States have recently defined "property" to include at least certain forms of computer data, see Pet. Br. 18, petitioner does not identify decisions construing each of those laws to create property rights in records like Location History for the individuals to whom those records may pertain. And to the extent that such decisions exist, there is no reason why a subset of States should have controlling weight on the constitutional analysis.

Efforts to "propertize" personal data have not been uniformly successful. See, *e.g.*, S. 806, 116th Cong., 1st

Sess. (2019) (failed bill that would give individuals ownership rights over data they generate online). As might be expected, the approach has many critics. See, *e.g.*, Cameron F. Kerry & John B. Morris, *Why Data Ownership Is the Wrong Approach to Protecting Privacy*, Brookings (June 26, 2019); Jane R. Bambauer, *How to Get the Property out of Privacy Law*, Yale L.J.F. 1087, 1099 (2024).

This Court should not prematurely constitutionalize that policy debate. And the embrace of particular state laws would generate significant practical problems, including how state courts might interpret them in the future, choice-of-law issues where law-enforcement activities cross state boundaries (as they did here), and reconsideration of Fourth Amendment doctrine if the property-law landscape were to shift.

c. Even accepting the premise that Location History records could be property, petitioner cannot show that they were *his* property, rather than the property of Google, which created, used, and controlled them. See *Minnesota* v. *Carter*, 525 U.S. 83, 92 (1998) (Scalia, J., concurring) (emphasizing Fourth Amendment's use of "their"). When enabled to do so, mobile devices sent updates to Google through a process set up by Google. See Pet. App. 273a. Google then "process[ed]" those updates—not only for storage in Google's database, but also to calculate a "display radius" of a determined size around a given set of coordinates, representing "Google's estimate" of the device location's accuracy. J.A. 25, 44, 51; see Pet. App. 274a. Google then enjoyed the use of the information in its database, relying on it, for example, to measure ad performance, which in turn helped Google increase its ad revenue. See Pet. App. 270a-271a. And Google could destroy the records in its

database—a power that it exercised recently by "delet[ing]" some "Location History data that was previously stored on Google's servers." Google Amicus Br. 2.

Google also had the unilateral right to disseminate at least the step-one information that it provided pursuant to the warrant. Google's privacy policy made clear that it "may share non-personally identifiable information publicly and with its partners—like publishers, advertisers, or rightsholders," without giving accountholders any right to preclude it from doing so. J.A. 70. And the policy made clear that Google could, without consulting the accountholder, also disclose the information in other circumstances, such as to "address * * * technical issues," or to "[p]rotect against harm to the rights, property, or safety of Google, our users, or the public as required or permitted by law." *Ibid.*

Petitioner errs in asserting (Br. 15-21) that he was the owner—and Google simply the bailee—of the information that Google generated, collected, stored, used, and disclosed. He notes (Br. 21) that Google described Location History as "your data" and "your information," but the "your" in that description referred to the *subject*, not the *owner*, of the information. If a tailor makes a note of "your measurements" for his files, the note still belongs to the tailor, not "you." When Google wanted to clarify property rights, it used different and more explicit language: for example, by telling users, "'[y]ou retain ownership of any intellectual property rights that you hold in [certain] content.'" Pet. App. 95a n.21 (quoting C.A. J.A. 2083).

Petitioner also errs in asserting (Br. 15-22) that he, rather than Google, had the meaningful rights to "exclude" others from the information in Google's database and to "destroy" it. The privacy policy did not provide

for user objections if Google decided that a disclosure was appropriate. J.A. 69. And while a user could tell Google to "start[] the process of removing [Location History information] from the product and [Google's] systems," J.A. 46, Google had discretion to "retain data for limited periods when it needs to be kept for legitimate business or legal purposes." J.A. 72. In any event, even an unqualified user right to deletion would not suggest that the Location History information belonged to the user: a customer would not "own" a tailor's record of his measurements even if he could demand that the tailor throw it away.

d. Finally, even assuming petitioner had property rights in the Location History information, and that any intrusion analogous to a "trespass" would implicate the Fourth Amendment, no such trespass occurred. Petitioner states that a "bailee who uses the item in a different way than he's supposed to, or against the bailor's instructions, is liable" for a property tort. Pet. Br. 21 (quoting *Carpenter*, 585 U.S. at 399 (Gorsuch, J., dissenting)). But Google did not use the Location History data in "a different way than [it was] supposed to." *Ibid.*

The privacy policy on which petitioner relies (Br. 21) as a source of the supposed "bailment" provides that Google "will share personal information outside of Google" if Google either independently deems it appropriate to "[p]rotect against harm to the rights, property, or safety of Google, our users, or the public as required or permitted by law," or has "a good-faith belief" that disclosure is "reasonably necessary" to comply with any "legal process, or enforceable governmental request." J.A. 69-70. That is exactly what happened here.

Whether or not the warrant here was actually enforceable, Google could at least in "good faith" believe

it to be, cf. Pet. App. 336a-337a (good-faith-exception finding by district court), or else decide to disclose the information for safety purposes to help catch "armed and dangerous suspect(s) still at large," J.A. 98 (law-enforcement communication to Google). Google's disclosure was thus consistent with the terms of any "bailment" agreement.

Petitioner's identification (Br. 18) of a few state laws creating statutory torts or crimes for "computer trespass" does not support his argument. The examples that he cites are limited to "unauthorized" or "malicious" access of computer data, see, *e.g.* Va. Code Ann. § 18.2-152.4 (2021), which is not what happened here. Indeed, if anything, the existence of such laws suggests that the asserted common-law trespass principles that petitioner would incorporate into the Fourth Amendment benefit from legislative, rather than judicial, adaptation to intangible online information.

II. ANY SEARCH WAS REASONABLE BECAUSE THE GOVERNMENT OBTAINED A PARTICULARIZED WARRANT SUPPORTED BY PROBABLE CAUSE

Even if petitioner's Fourth Amendment rights might otherwise have been infringed at some step of the warrant process, the explicit authorization of a judicial warrant rendered the process reasonable under the Fourth Amendment. As in *Carpenter*, any Fourth Amendment concerns are satisfied by the securing of a warrant (or circumstances that create an exception to the Fourth Amendment's warrant requirement). See 585 U.S. at 316-320. Petitioner's contrary arguments would rewrite the law of warrants, subpoenas, and third-party agency to render it seemingly impossible for judges to authorize the acquisition of valuable evidence in cases like this.

A. The Warrant Authorized A Particularized Search Based On Probable Cause

The Fourth Amendment's Warrant Clause provides for the issuance of warrants, "upon probable cause," that "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. Amend. IV. The probable-cause requirement ensures a judicial determination of a "fair probability that contraband or evidence of crime will be found in a particular place." *Illinois* v. *Gates*, 462 U.S. 213, 238 (1983). The particularity requirement, in turn, guards against "general, exploratory rummaging in a person's belongings," and prevents "the seizure of one thing under a warrant describing another." *Andresen* v. *Maryland*, 427 U.S. 463, 480 (1976) (citations omitted).

This Court has made clear that the Warrant Clause permits the issuance of search warrants that seek evidence held by a third party that is potentially helpful to law enforcement in the investigation of a crime, even if there are no specific suspects. See *Zurcher* v. *Stanford Daily*, 436 U.S. 547, 553-560 (1978). Not only is there no need for "probable cause to believe that the third party is implicated in the crime," but "'a search warrant may be issued on a complaint which does not identify any particular person as the likely offender.'" *Id.* at 554, 556 n.6 (citation omitted). When there is probable cause that a search "will aid in a particular apprehension or conviction," *Messerschmidt* v. *Millender*, 565 U.S. 535, 552 n.7 (2012) (citation and emphasis omitted), "[t]he critical element in a reasonable search is" simply "reasonable cause to believe that the specific 'things' to be searched for and seized are located" in the targeted place, *Zurcher*, 436 U.S. at 556 (citation omitted).

The warrant here satisfied those requirements. The application provided a "fair probability," *Gates*, 462 U.S. at 238, that Google would have location information about people who were within 150 meters of the credit union around the time that it was robbed. See J.A. 132-133. The application explained, *inter alia*, that most American adults own smartphones, that Google could collect and store location information from those smartphones when Location History was enabled, and that the credit-union robber was apparently on a cellphone when he walked in. J.A. 132-133. The application also provided a fair probability that the information would "aid" in the "apprehension or conviction" of the robber, *Messerschmidt*, 565 U.S. at 552 n.7, given the robber's observed use of the cellphone, the frequency with which cellphones generally are used to coordinate criminal activity, the demand note's reference to "boys on the lookout out side," and the additional potential to identify witnesses in the area who might have seen the robber or his accomplices. J.A. 131-132.

The warrant also "particularly describ[ed] the place to be searched" and "things to be seized," U.S. Const. Amend. IV. It stated that evidence "may be found within computer servers maintained or controlled by Google, Inc. or Google Payment Corp.," "stored at premises controlled by Google, Inc." J.A. 130; see J.A. 129. And it described the "material sought" in three detailed steps: (1) at step one, "anonymized information" with specified attributes (*e.g.*, numerical account identifier and time-stamped location information) for each mobile-device location update within the given time and distance from the credit union; (2) at step two, anonymized information in a similar form for any location updates for the two hours of the robbery for a law-

enforcement-minimized subset of the anonymous devices from step one; and (3) specific "identifying account information[]" (*e.g.*, "user name and subscriber information") for devices that remained relevant even after further law-enforcement minimization efforts. J.A. 131-132.

If investigators needed a warrant even at step one, it is difficult to see what more they could possibly have said or done to obtain it. The geofence radius was intentionally chosen to exclude heavily trafficked areas less likely to provide useful witnesses, like a busy road, popular businesses, and hotels. C.A. J.A. 940-941, 1988. And the magistrate's familiarity with local conditions would keep the expected information within reasonable bounds; had the investigators sought a warrant likely to produce information well beyond what the circumstances supported, the magistrate could have narrowed or denied it. Particularly given the "deferential" standard of review for warrants, *Massachusetts* v. *Upton*, 466 U.S. 727, 733 (1984) (per curiam), the probable cause and particularization were sufficient for law enforcement to obtain a warrant here.

B. The Warrant Was Valid At Step One

Petitioner nonetheless would invalidate the warrant from start to finish, on theories that would preclude law enforcement from ever obtaining even anonymized information about potential suspects and witnesses near the scene of a crime. Petitioner principally argues (Br. 32-41) that a warrant like this is inherently an unconstitutional "general warrant," because at step one, Google had "to search *every* user's account—millions in total"—to find responsive information. That argument is misconceived.

1. Just as in *Carpenter*, where a search occurred "when the Government *accessed* CSLI from the wireless carriers," 585 U.S. at 313 (emphasis added), any law-enforcement search here was of the information it received—not what Google had to itself examine to provide that information. See *id.* at 316 ("[T]he *acquisition* of Carpenter's CSLI was a search.") (emphasis added). In contrast to "the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity," *Riley* v. *California*, 573 U.S. 373, 403 (2014), law enforcement here did not have free rein to rummage through Google's database.

Thus, as in *Carpenter*, a "warrant supported by probable cause" to search particular records—there, seven days of CSLI; here, the anonymized step-one information—was sufficient for "acquiring such records." 585 U.S. at 316. Were it otherwise, most search warrants and third-party subpoenas—including, potentially, some CSLI warrants—could be characterized as overbroad general warrants, because they would authorize some third-party recipient to "search" a broader set of its own files to find responsive documents. See Pet. App. 127a (Berner, J., concurring). That has not been the law. See, *e.g.*, *Oklahoma Press Publ'g Co.* v. *Walling*, 327 U.S. 186, 202-214 (1946) (distinguishing subpoena from "actual search and seizure").

Moreover, the reason that Google had to query "across *all* [Location History] data" to respond to the geofence warrant, J.A. 50, is because of Google's own internal design choices about how it organized its database. If Google had indexed the information by location, it could have retrieved the information responsive to the

warrant more efficiently. But as even petitioner appears to acknowledge (Br. 40-41), the constitutional analysis cannot turn on the technical details of Google's private decisions about its specific data structure. Cf. *Smith*, 442 U.S. at 745 (explaining that phone company's storage practices did not "make any constitutional difference").

Carpenter did not suggest that the validity of a CSLI warrant hinged on how the wireless provider organizes the data. See 585 U.S. at 313-320. And such a requirement would make little sense. At the time a subpoena or warrant is sought (or even thereafter), law enforcement may not even know how a third party organizes what it has. In this case, even after factfinding, the precise details of Google's internal organization of its information remain unclear. Officers requesting search warrants, magistrates evaluating those requests, and courts assessing their sufficiency should not have to wade into those complicated technical issues to make seemingly arbitrary distinctions, far removed from normal experience.[3]

2. Petitioner argues that Google was acting as "an instrument or agent of the Government" when it scanned its databases for responsive data. Pet. Br. 33 (quoting *Skinner* v. *Railway Labor Execs.' Ass'n*, 489 U.S. 602, 614 (1989)). But the single case that he cites involved bodily searches required by statute and regulation, and even then, it recognized that agency issues "necessarily

[3] A design choice might make a difference if it were to render the recipient of a geofence warrant incapable of complying with it. The government's understanding is that Google's recent decision to eliminate a centralized database altogether, and store Location History information on mobile devices themselves, is such a change. See Br. in Opp. 18.

turn[] on the degree of the Government's participation in the private party's activities." *Skinner*, 489 U.S. at 614. The subject of a subpoena or other judicial order, however, is far from the government's "agent"—it may, in fact, assert Fourth and Fifth Amendment rights of its own. See 2 Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 4.13, at 1051 (6th ed. 2020) (LaFave).

Akin to a subpoena, the warrant here provided directions only as to *what* Google would provide, not *how* it might do so. And as in *Carpenter*, the particularity and probable cause requirements of the Warrant Clause would come into play only because of "what" the government would seize and search, not "how" a third party might provide it. See 585 U.S. at 316. Google's step-one returns revealed nothing about any accounts other than the 19 (anonymized) ones with locational updates from inside the geofence at the relevant time. The government learned nothing about other accounts—how many there were, to whom they corresponded, whether they even had Location History enabled at that time, or whether they had paused it or requested deletion after the fact.

Nor is it even clear how much (if anything) Google itself even learned about other users when it "r[a]n a computation" to match data in its database to the parameters of the warrant. J.A. 50. "When a filter scans through data" in that manner, "blindly check[ing] for a match," "the filter does not 'see' the data in a Fourth Amendment sense." Orin S. Kerr, *Data Scanning and the Fourth Amendment*, 67 B.C. L. Rev. 431, 459 (2026). And any information that might have been exposed was information that Google itself could already access and

use for its own advertising purposes. See Pet. App. 271a.

Google's disclosure thus did not "expose[ ] to view" anything that was otherwise "concealed." *Arizona* v. *Hicks*, 480 U.S. 321, 325 (1987); cf. 4 LaFave § 8.6(a), at 322 (a "bailee" can generally consent to a government search of the portions of bailed property that the bailee "could be expected to make use of" under the bailment). At all events, to the extent that the interests of other accountholders were implicated, their "Fourth Amendment rights," if any, "may not be vicariously asserted" by petitioner. *Rakas* v. *Illinois*, 439 U.S. 128, 133-134 (1978) (citation omitted).

3. Because the warrant was agnostic as to Google's methods, petitioner's suggestion that investigators needed to do the impossible—"identify a *particular* account" to be searched before even step one, Br. 38—is misplaced. Indeed, the Warrant Clause generally does not require such specificity even in more analog contexts. In *United States* v. *Karo*, 468 U.S. 705 (1984), for example, this Court explained that the government could obtain a valid warrant to track the location of a beeper—even inside "private premises"—notwithstanding that the government could not know in advance where the beeper would end up, let alone whose (if anyone's) private premises they might be. *Id.* at 718. As *Karo* illustrates, when there is probable cause for a search, the impossibility of further specification does not present an insurmountable hurdle to the issuance of a lawful warrant.

Petitioner's efforts (Br. 49-51) to create a similarly impossible hurdle through the probable-cause requirement are likewise mistaken. Petitioner principally relies on *Ybarra* v. *Illinois*, 444 U.S. 85 (1979), which held

that probable cause that a bartender was dealing drugs out of a bar could not authorize a bodily frisk of every bar patron based on the patrons' mere "propinquity to others independently suspected of criminal activity." *Id.* at 90-91. The warrant here, however, did not purport to authorize a bodily search of suspects based on suspicion that they were involved in a crime. It sought evidence from a third party that could identify suspects and witnesses of a crime—a commonplace step in criminal investigation. See, *e.g.*, *Zurcher*, 436 U.S. at 551 (valid warrant for photographic evidence potentially showing identity of suspects). 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. See *Carpenter*, 585 U.S. at 316 ("We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras."); *City of Los Angeles* v. *Patel*, 576 U.S. 409, 423 (2015) (discussing administrative warrants for hotel registries).

Even "[i]n searches for papers," conducted by law enforcement itself, "it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." *Andresen*, 427 U.S. at 482 n.11. The warrant-authorized "'seizure' of telephone conversations" may likewise overhear other conversations. *Ibid.* But the prospect of incidentally encountering other documents while looking for certain evidence does not transform a warrant for that evidence into general warrant, or otherwise render the search "unreasonable," U.S. Const. Amend. IV. Cf. *Illinois* v. *Lidster*, 540 U.S. 419 (2004) (upholding constitutionality of stopping all vehicles to ask for information about hit-and-

run at same location a week earlier). And as the Court has recognized, they can be appropriately addressed by conducting searches "in a manner that minimizes unwarranted intrusions upon privacy"—not by foreclosing them altogether. *Andresen*, 427 U.S. at 482 n.11.

C. The Warrant Was Valid At Steps Two And Three

The warrant-authorized procedure here included explicit minimization measures. Only anonymized information was returned at step one; the investigators were required to "attempt to narrow down the list" of potentially relevant accounts between steps one and two (which likewise revealed only anonymized data); and then to do so again between steps two and three. J.A. 130-131. Petitioner, however, would turn that salutary feature of the warrant into a bug, on the theory that the minimization measures gave law enforcement too much discretion in the narrowing of the limited information that it was authorized to obtain. See Pet. Br. 52-55. That theory is misconceived.

As a general matter, warrants inherently leave officers some "room to make a judgment as to what particular documents or things are subject to seizure under the warrant which he is executing." 2 LaFave § 4.6(a), at 750-751 (citation omitted). A warrant's validity does not turn on cabining that discretion to the nth degree. A federal wiretap warrant, for example, must specify that the wiretap be "conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter." 18 U.S.C. 2518(5). But given the practical realities, the validity of the warrant-based search turns on the reasonableness of law enforcement's minimization steps under the circumstances—not the absence of any discretion as to

how to minimize. See *Scott* v. *United States*, 436 U.S. 128, 139-143 (1978).

Here, the probable cause that supported investigators' acquisition of Google data at step one did not cease to exist at steps two and three. The magistrate could reasonably find that the facts supported the acquisition of two hours of identifiable location information from accounts satisfying the stated geofencing criteria. And the warrant described with particularity exactly what that information would look like. See J.A. 130-131. Requiring law enforcement to repeatedly make efforts to narrow the scope of the information to be disclosed—with Google able to, as it did, object to the reasonableness of the government's efforts, see Pet. App. 299a-300a—was a protective measure, not a constitutional flaw. Much less is it one that would preclude any form of geofence warrant, completely foreclosing a valuable "tool[]" to catch "modern-day criminal[s]" like petitioner, who chose to use a cellphone on which he was sharing his location as an instrument of his crime. *Id.* at 26a-28a (Wilkinson, J. concurring).

III. IN ALL EVENTS, THE DECISION BELOW SHOULD BE AFFIRMED

Even if this Court finds that petitioner's Fourth Amendment rights were violated, the appropriate disposition is to affirm, rather than to reverse as petitioner urges (Br. 55). The district court determined—correctly—that regardless of whether the government violated the Fourth Amendment, suppression is unwarranted under the good-faith exception to the exclusionary rule. Pet. App. 344a. The en banc court of appeals affirmed the denial of petitioner's suppression motion, *id.* at 4a, with a majority of judges expressly finding that the good-faith exception applies. See *id.* at 5a-22a (Diaz,

C.J., concurring); *id.* at 35a (Niemeyer, J., concurring); *id.* at 36a (King, J., concurring); *id.* at 38a n.1 (Wynn, J., concurring in the judgment); *id.* at 97a-99a (Heytens, J., concurring).

The application of the good-faith exception is "an issue separate from the question whether the Fourth Amendment rights of the party seeking to invoke the rule were violated." *United States* v. *Leon*, 468 U.S. 897, 906 (1984) (citation omitted). Petitioner asked (Pet. 34-37) this Court to grant review on that separate issue, but the Court declined to do so. See 2026 WL 120676 (Jan. 16, 2026). Accordingly, the Court's decision in this case will not disturb the independent determination that suppression is unwarranted.

CONCLUSION

The judgment of the court of appeals should be affirmed.

Respectfully submitted.

D. JOHN SAUER
Solicitor General
A. TYSEN DUVA
Assistant Attorney General
ERIC J. FEIGIN
Deputy Solicitor General
ZOE A. JACOBY
Assistant to the Solicitor General
ETHAN A. SACHS
Attorney

MARCH 2026