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

PETITIONER'S OPENING BRIEF

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

QUESTION PRESENTED

This case concerns the constitutionality of geofence warrants. For cell phone users to use certain services, their cell phones must continuously transmit their exact locations to their service providers. A geofence warrant allows law enforcement to obtain, from the service provider, the identities of users who were in the vicinity of a particular location at a particular time.

In this case, law enforcement obtained, and served on Google, a geofence warrant seeking anonymized location data for every device within 150 meters of the location of a bank robbery within one hour of the robbery. After Google returned an initial list, law enforcement sought—without seeking an additional warrant—information about the movements of certain devices for a longer, two-hour period, and Google complied with that request as well. Then—again without seeking an additional warrant—law enforcement requested de-anonymized subscriber information for three devices. One of those devices belonged to petitioner Okello Chatrie. Based on the evidence derived from the geofence warrant, petitioner was convicted of armed robbery.

The Court granted certiorari limited to the following question:

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

RELATED PROCEEDINGS

This case arises from and is related to the following proceedings in the United States District Court for the Eastern District of Virginia and the United States Court of Appeals for the Fourth Circuit:

- *United States v. Chatrie*, 590 F. Supp. 3d 901 (E.D. Va. 2022).

- *United States v. Chatrie*, 107 F.4th 319 (4th Cir. 2024) (panel opinion).

- *United States v. Chatrie*, 2024 WL 4648102 (4th Cir. 2024) (granting rehearing en banc).

- *United States v. Chatrie*, 136 F.4th 100 (4th Cir. 2025) (en banc opinion).

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

CONSTITUTIONAL PROVISIONS AND STATUTES

OTHER AUTHORITIES

INTRODUCTION

This case concerns a novel law enforcement technique known as a geofence warrant. Geofence warrants leverage tech companies' practice of collecting granular information about their users' locations. The government draws a "geofence"—a virtual "fence" around a geographic location—and obtains a warrant directing the tech company to identify users who were within that geofence at a particular time.

The geofence warrant in this case was directed to Google. Millions of Americans have activated a Google service known as Location History, which records the location of the user's device approximately every two minutes. A user's Location History, like a user's email and photographs, is stored in the user's own account and can be reviewed, edited, and deleted by the user.

After an investigation of a bank robbery ran cold, the police served a geofence warrant on Google. The warrant directed Google to search every user's private Location History—millions of users in all—in order to locate every device that was within 150 meters of the bank during a time period starting 30 minutes before the robbery and ending 30 minutes afterwards.

The warrant recited a three-step procedure. At Step One, Google would give police detailed location information for every device within the geofence during the one-hour stretch, but would not provide the users' names. At Step Two, the police would identify a subset of users and seek location information for those users over an additional hour and without geographic restriction; Google would return that information, again

without providing any names. Finally, at Step Three, the police would send another narrowed list of users, and Google would reveal their identities. The police and Google followed that three-step process, leading to the identification and conviction of petitioner Okello Chatrie.

The search of petitioner violated the Fourth Amendment. The technology may be novel, but the constitutional problem it presents is not. The Fourth Amendment was born of the Founders' revulsion for general warrants and writs of assistance—instruments that allowed the government to search first and develop suspicions later. A geofence warrant operates on precisely that principle. To find the few people near a crime scene, the government compels a search of every account with Location History enabled—millions of people, all over the country, whose private digital papers must be searched so that the government can identify who was where and when. The potential for abuse is breathtaking: the government need only draw a geofence around a church, a political rally, or a gun shop, and it can compel a search of every user's records to learn who was there. The Fourth Amendment was adopted to ensure that the government could never wield such power.

The Court should reach the following conclusions:

1. A "search" of petitioner occurred. The government accessed private location information in petitioner's Google account, resulting in an infringement of both petitioner's property rights and his reasonable expectation of privacy.

2. The geofence warrant was an unconstitutional general warrant. The warrant compelled Google to conduct a fishing expedition through millions of Google accounts, without any basis for believing that any one of them would contain incriminating evidence. The government's contrary theory—that no search occurs until Google actually *finds* relevant evidence in an account—ignores the principle that a search is a search, even if nothing is found.

3. Even if a search occurs only when relevant information is found, the warrant was still unconstitutional. The Fourth Amendment requires a warrant to identify a *particular* account, supported by probable cause that incriminating evidence exists *in that account*. The warrant in this case—which authorized the government to obtain the private data of an unspecified number of as-yet-unknown individuals who merely happened to be in the vicinity of the robbery, followed by a winnowing process over which police had complete discretion—departed so dramatically from the Fourth Amendment's requirements that it can hardly be called a warrant at all.

OPINIONS BELOW

The Fourth Circuit's en banc opinion is reported at 136 F.4th 100 (4th Cir. 2025). Pet. App. 1a. The Fourth Circuit's panel opinion is reported at 107 F.4th 319 (4th Cir. 2024). Pet. App. 145a. The district court's opinion is reported at 590 F. Supp. 3d 901 (E.D. Va. 2022). Pet. App. 264a.

JURISDICTIONAL STATEMENT

The Fourth Circuit issued its decision on April 30, 2025. This Court has jurisdiction under 28 U.S.C. § 1254(1).

RELEVANT CONSTITUTIONAL PROVISION

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."

STATEMENT OF THE CASE

A. Google's "Location History" Feature

The geofence warrant in this case relied on a Google feature called "Location History." Every two minutes on average, Location History draws on GPS information, Bluetooth beacons, cell site location information ("CSLI"), IP address information, and nearby Wi-Fi networks to record a device's location. Pet. App. 271a. Location History can determine a person's location to within three meters and can determine a person's elevation within a building. Pet. App. 272a, 274a. As the district court found, Location History is "the most sweeping, granular, and comprehensive tool—to a significant degree—when it comes to collecting and storing location data." Pet. App. 270a.

Google prompts users to enable Location History multiple times across multiple apps, starting from when a user first sets up a Google account. Pet. App. 273a. If

a user does not enable Location History immediately upon account setup, Google will prompt him to do so when he sets up an app with "Location History-powered features," like Google Maps, Google Photos, and Google Assistant. Pet App. 279a. Once a user enables Location History through one app, it is enabled across all Google devices, and it remains active even if he deletes the original app. Pet. App. 273a. Google collects and stores Location History at all times, regardless of whether the user is actively using his phone. Pet. App. 103a-104a. A user who enables Location History may review, edit, or delete his data. Pet. App. 281a, 283a; JA-19.

Over 500 million Google users have Location History enabled. Pet. App. 6a.[1] When the warrant in this case was executed, Google stored users' Location History in their accounts in a repository known as the "Sensorvault," where each data point is associated with a unique device ID. Pet. App. 272a.

In 2023, Google announced a new data-storage policy under which Location History is stored on users' devices, rather than in the Sensorvault. Pet. 10-11; BIO 18. Google has not publicly announced whether the new policy has been fully implemented.

---

[1] Below, Google characterized the number of users with Location History enabled as "roughly one-third of active Google users," which meant "numerous tens of millions." JA-45. At the panel stage, Judge Wynn noted that Google has "1.5 billion users worldwide," implying "500 million" Location History users. Pet. App. 228a; *see* Pet. App. 127a (citing case estimating 592 million users).

B. Geofence Warrants

Geofence warrants seek to leverage technology companies' practice of storing users' data in "the cloud." "[C]ompanies such as Apple, Lyft, Snapchat, and Uber have all received geofence warrants, but Google is the most common recipient and the only one known to respond." Pet. App. 5a n.1 (quotation marks and citation omitted).

When law enforcement serves a geofence warrant on Google, it identifies a geographic area—the geofence—which is typically a circle with a specified radius. Pet. App. 285a. Then it identifies a span of time, and requests Location History data for all users within that area during that time. *Id.*

The government worked with Google to create a three-step process for responding to such warrants. Pet. App. 286a. First, law enforcement obtains a warrant compelling Google to disclose a "de-identified" list of all Google users whose Location History indicates they were in the geofence during the applicable time interval. *Id.* After being served with the warrant, Google searches every user's Location History and picks out the users whose stored Location History indicates their location was within the geofence. Pet. App. 287a-288a. Google then compiles a list for law enforcement including, for each user, the stored latitude/longitude coordinates, timestamps, confidence intervals, and sources of information. *Id.* At this step, each user's information is connected to a "de-identified" device number. Pet. App. 286a-287a.

Second, the government reviews the list of de-identified data. If needed, it may then ask Google for additional Location History information for the users identified in Step One, both over a longer time period and outside the geofence. Pet. App. 289a-290a. Typically, Google requires the government to narrow its request to a subset of accounts from the original geofence. Pet. App. 290a.

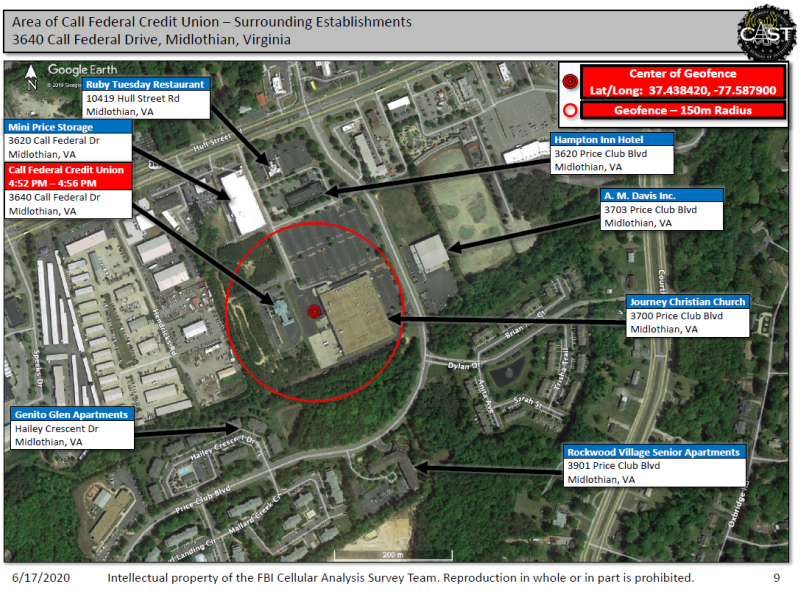
Third, after reviewing the additional data received at Step Two, the government asks Google to provide the names and account identifiers—including email addresses and phone numbers—associated with particular devices it analyzed at Step Two. Pet. App. 290a-291a.

C. Factual Background

On May 20, 2019, a man robbed the Call Federal Credit Union in Midlothian, Virginia and left on foot. Pet. App. 265a-267a. Detective Hylton of the local police responded to the scene, interviewed witnesses, and reviewed surveillance video. Pet. App. 291a. Over the next few weeks, his investigation stalled. Pet. App. 292a.

Then on June 14, 2019, Detective Hylton applied for a geofence warrant. Pet. App. 293a. In the warrant application's accompanying affidavit, Detective Hylton said the robber appeared to be using a cell phone in surveillance footage, and that "when people act in concert with one another to commit a crime, they frequently utilize cellular telephones." Pet. App. 296a. A Virginia magistrate signed the warrant. Pet. App. 294a.

The warrant authorized a geofence with a 300-meter diameter—longer than three football fields—drawn



over the site of the robbery, encompassing both the bank and a nearby church. Pet. App. 294a; JA-158.

The warrant followed Google's three-step procedure. At Step One, the warrant called for de-identified information for all user accounts inside the geofence from 4:20 to 5:20 pm. Pet. App. 295a; JA-136. The warrant stated that law enforcement would "review" that information and "attempt to narrow down the list" before returning to Google and seeking non-geographically limited location information for an additional 30 minutes on either side of the original hour— *i.e.*, from 3:50 to 5:50 pm. Pet. App. 296a; JA-136. The warrant then stated that law enforcement would again "attempt to narrow down the list" and return to Google for Step Three, at which point the accounts would be linked to identifiable users. Pet. App. 295a-296a; JA-137.

After Detective Hylton sent the warrant to Google, Google executed Step One and provided him with "anonymized" data for 19 users found within the geofence. Pet. App. 299a; JA-99, 160, 164-175.

Detective Hylton then requested Step Two and Step Three data for all 19 users, but Google refused that request. Pet. App. 299a-300a; JA-100-107. In response, Detective Hylton narrowed his request and sought Step Two data—*i.e.*, an extra hour of location data, unbounded by the geofence—for nine users, which Google provided. Pet. App. 300a; JA-176-200. Detective Hylton did not explain to Google why he chose these nine accounts, nor did he consult the state magistrate. Pet. App. 300a; JA-106-107.

Finally, Detective Hylton requested that Google de-anonymize three users, again without explaining why or consulting a magistrate. Pet. App. 300a-301a; JA-109-110. Google provided the information. Pet. App. 300a; JA-111, 201-208. One of those de-anonymized users was petitioner. Pet. App. 106a.

D. Proceedings Below

Petitioner was indicted on robbery and firearms charges. Pet. App. 306a. He moved to suppress the fruits of the geofence warrant. The district court conducted extensive fact-finding, relying on, among other things, an amicus brief by Google, four declarations by Google employees, and in-person testimony from Google employees. Pet. App. 306a-308a. The district court concluded that the warrant violated the Fourth Amendment's particularity and probable cause requirements. Pet. App. 312a-313a. Nonetheless, the district court

declined to suppress the evidence through application of the good-faith exception to the exclusionary rule. *See* Pet. App. 336a-344a.

Petitioner entered a conditional guilty plea, reserving his right to appeal the denial of his motion to suppress. Pet. App. 80a.

A divided Fourth Circuit panel affirmed. The majority held that no search occurred because petitioner voluntarily exposed his information to Google. Pet. App. 148a. Dissenting, Judge Wynn concluded that the government violated petitioner's reasonable expectation of privacy. Pet. App. 187a.

The Fourth Circuit reheard the case *en banc* and affirmed the district court's judgment in a one-sentence per curiam opinion without reasoning. Pet. App. 4a.

The court divided 7-7 on whether a Fourth Amendment search had occurred, with one judge declining to reach the issue. Seven judges concluded that no Fourth Amendment search occurred because petitioner lacked a "reasonable expectation of privacy in two hours' worth of Location History data voluntarily exposed to Google," Pet. App. 80a-81a (Richardson, J.), with three judges within that group filing separate concurrences. Pet. App. 23a-30a (Wilkinson, J.); Pet. App. 31a-35a (Niemeyer, J.); Pet. App. 36a (King, J.). Seven judges concluded that a Fourth Amendment search *had* occurred. They reasoned that the government had "invaded [petitioner's] reasonable expectation of privacy" in accessing his data, an expectation that the third-party doctrine was "wholly inadequate" to defeat. Pet. App. 37a, 60a, 69a (Wynn, J.); *see* Pet. App. 111a-122a (Berner, J.).

Chief Judge Diaz declined to decide whether a search had occurred, instead voting to affirm based on the good-faith exception. Pet. App. 5a-22a.

Of the seven judges who found a Fourth Amendment search, five concluded that the government's warrant application was not supported by probable cause, with two not opining on the issue. Pet. App. 122a-126a (Berner, J.). However, only Judge Gregory would have suppressed the evidence. Pet. App. 130a-142a (Gregory, J.). The other six indicated that suppression was unwarranted under the good-faith exception. Pet. App. 38a n.1 (Wynn, J.); Pet. App. 97a-99a (Heytens, J.).

SUMMARY OF THE ARGUMENT

I. The government conducted a Fourth Amendment search for two reasons: it invaded petitioner's property interest and it infringed on petitioner's reasonable expectation of privacy.

Petitioner had a property interest in his Location History data. Location History is user-generated content that is stored in a user's Google account. The user can review, edit, export, or delete it at will. Courts and legislatures have recognized that users have a property interest in private data like Location History. Although the data was on Google's servers, Google's status as bailee did not strip petitioner of his property interest.

Additionally, petitioner had a reasonable expectation of privacy in his Location History. In *Carpenter v. United States*, 585 U.S. 296 (2018), this Court held that cell phone users have a reasonable expectation of privacy in their cell-site location data. *Carpenter*'s reasoning applies equally to Location History: just as in

Carpenter, accessing Location History allows the government to determine a person's historical location with remarkable precision.

The third-party doctrine does not apply to Location History. Prior cases have held that a person lacks a reasonable expectation of privacy in a third party's business records, but Google has acknowledged that Location History is not a business record. Even if it was, activating Location History should not be construed as consent to Google sharing that information with the government.

II. The geofence warrant was an unconstitutional general warrant.

The government directed Google to search *everyone's* Location History—millions of people in all—to determine whether they had been within the geofence at the relevant time.

The warrant's assertion that the police would search "Google" was insufficiently particularized. Just as the Fourth Amendment requires warrants to identify a particular apartment in an apartment complex or a particular package in a warehouse, the Fourth Amendment requires warrants to identify a particular Google account. The Fourth Amendment does not permit a warrant that allows the police to rummage through *all* Google accounts merely based on probable cause that incriminating evidence is *somewhere*. By permitting such a search, the geofence warrant was a general warrant—exactly what the Fourth Amendment was designed to prevent.

III. Even if a search did not occur until the government received the Step One results from Google, that search was still unconstitutional.

At Step One of the geofence warrant, the government retrieved location information of 19 users who were within the geofence within one hour of the crime. Therefore, it conducted Fourth Amendment searches of those 19 users. The fact that this location information was purportedly anonymized does not change the fact that those users were searched.

To justify the search or seizure of data in a Google account, the warrant must identify a *particular* account, based on probable cause that *the particular account* will have relevant evidence. That did not happen here. The warrant's statement that the government would search and seize data from an unspecified set of accounts that contained location data within the geofence did not satisfy the Fourth Amendment's particularity requirement. Moreover, there was no probable cause to search the accounts of everyone who merely happened to be in the vicinity of the crime.

IV. At Steps Two and Three, the government retrieved additional private information and hence conducted additional searches. Those searches were unconstitutional.

The warrant stated that the police would review information retrieved at Step One and use it to gather additional information at Step Two, and then do the same at Step Three. However, the police had complete discretion to decide which accounts to search at Steps Two and Three. The warrant did not identify any accounts with

particularity or provide any details to identify them. And there was no probable cause to justify those additional searches. Although Google reviewed the government's Step Two and Step Three requests, Google is not a judge and has no authority to approve warrants.

ARGUMENT

I. ACCESSING LOCATION HISTORY IS A FOURTH AMENDMENT "SEARCH."

The Fourth Amendment protects against "unreasonable searches and seizures." The first question in this case is whether the government conducted a Fourth Amendment "search."

Historically, the concept of a Fourth Amendment search was "tied to common-law trespass." *United States v. Jones*, 565 U.S. 400, 405 (2012). In *Katz v. United States*, 389 U.S. 347 (1967), however, this Court concluded that attaching an eavesdropping device to a public telephone booth constituted a search, emphasizing that "the Fourth Amendment protects people, not places." *Id.* at 351. Concurring, Justice Harlan concluded that a search occurs when the government infringes on a "reasonable expectation of privacy," a formulation later cases have applied. *Id.* at 360 (Harlan, J., concurring); *see Carpenter*, 585 U.S. at 304-05.

"[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test." *Jones*, 565 U.S. at 409. Thus, a Fourth Amendment search occurs when the government infringes on *either* a property interest, *or* a reasonable expectation of privacy.

Here, both criteria for a search are independently satisfied. Users have both a property interest and a reasonable expectation of privacy in their Location History.

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

Location History is private data stored in private accounts on Google's servers. The Court should hold that such data is a form of property, one's digital "papers" and "effects," that deserves Fourth Amendment protection.

Location History has the key attributes of "property" as traditionally understood: the right to use, enjoy, dispose, and exclude.

"Property consists of the free use, enjoyment, and disposal of a person's acquisitions without control or diminution save by the law of the land." *Buchanan v. Warley*, 245 U.S. 60, 74 (1917) (citing 1 William Blackstone, *Commentaries on the Laws of England* 127 (Cooley's Ed.)). Google users may freely use, enjoy, and dispose of Location History. They may "review, edit, or delete" Location History information "from Google's servers at will." JA-19; *see* JA-72 ("You can export a copy of your information or delete it from your Google Account at any time.").

Google users also may exclude others from their Location History—"one of the most treasured rights of property ownership." *Cedar Point Nursery v. Hassid*, 594 U.S. 139, 149 (2021) (quotation marks omitted). Location History is in a user's password-protected personal account, and Google has a strict privacy policy that bars Google from sharing user data with others. JA-71

(Google protects against "unauthorized access, alteration, disclosure, or destruction of the information we hold.").[2]

As Google explained, Location History is analogous to "emails on Google's Gmail service" and "documents on Google Drive." JA-20. It is "controlled by the user, and Google stores that information in accordance with the user's decisions (*e.g.*, to opt in or out, or to save, edit, or delete the information), including to enhance the user's experience when using other Google products and services." *Id.*

Given the many property-like attributes of private electronic data like Location History, courts and legislatures alike have recognized it as a form of property.

Courts have consistently held that those who improperly access private data may be civilly liable. Many courts have relied on traditional property torts like conversion and trespass to chattels. *See e.g. Skapinetz v. CoesterVMS.com, Inc.*, No. CV PX-17-1098, 2018 WL 805393, at *4 (D. Md. Feb. 9, 2018) (recognizing both conversion and trespass to chattels claims for unauthorized access to Google email accounts and collecting like cases); *Physicians Interactive v. Lathian Sys. Inc.*, No. CA 03-1193-A, 2003 WL 23018270, at *9 (E.D. Va. Dec. 5, 2003) (unauthorized website access intermeddled with "personal property in the rightful possession of the [p]laintiff" and unauthorized viewing of that information

[2] Throughout this brief, we describe Google's policies as they existed when petitioner activated Location History. Pet. App. 276a (petitioner activated Location History on July 9, 2018); JA-53 (privacy policy as of that date).

served "as a *prima facie* basis for a claim for trespass on chattels"); *Microsoft Corp. v. John Does 1-8*, No. 1:14-cv-811, 2015 WL 4937441, at *11 (E.D. Va. Aug. 17, 2015) (unauthorized access to computer systems "may form the basis for claims of trespass to chattels and conversion"); *Kremen v. Cohen*, 337 F.3d 1024, 1030, 1033 (9th Cir. 2003) (conversion of website domain names); *Integrated Direct Mktg., LLC v. May*, 495 S.W.3d 73, 76 (Ark. 2016) ("intangible property, such as electronic data…can be converted"); *Budsgunshop.com, LLC v. Sec. Safe Outlet, Inc.*, No. 5:10-CV-00390-KSF, 2012 WL 1899851, at *9, *18 (E.D. Ky. May 23, 2012) (conversion of website and "all data and electronic information stored within"); *Thyroff v. Nationwide Mut. Ins. Co.*, 864 N.E.2d 1272, 1278 (N.Y. 2007) (electronic data is indistinguishable from printed documents for purposes of conversion); *Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 697–98 (D. Md. 2011) (trespass to chattels for redirect command that directed viewers away from plaintiff's website).

Other courts have relied on privacy torts, most commonly intrusion on seclusion. *See, e.g.*, *In re Google Location History Litig.*, 514 F. Supp. 3d 1147, 1155 (N.D. Cal. 2021) (unauthorized collection of location data); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 603 (9th Cir. 2020) (unauthorized collection of personal data); *New Mexico ex rel. Balderas v. Tiny Lab Prods.*, 457 F. Supp. 3d 1103, 1126-27 (D.N.M. 2020) (unauthorized tracking of online behavior); *McDonald v. Kiloo ApS*, 385 F. Supp. 3d 1022, 1034-35 (N.D. Cal. 2019) (same); *see also Agency for Health Care Admin. v. Associated Indus. of Fla., Inc.*, 678 So. 2d 1239, 1252 & n.20

(Fla. 1996) (one who "physically *or* electronically intrud[es] into [another's] private quarters" can be held liable for "invasion of privacy").

State legislatures, too, have treated computer data as a form of property for purposes of criminal and civil trespass laws. In Virginia, the Virginia Computer Crimes Act defines "[p]roperty" to include "computer data[] … within a computer network." Va. Code Ann. § 18.2-152.2. Virginia criminalizes "computer trespass" (which includes making, with "malicious intent," an "unauthorized copy"), *id.* § 18.2-152.4, and permits a civil cause of action for those injured by those violations, *id.* § 18.2-152.12. Other states have similar schemes. *See, e.g.*, Conn. Gen. Stat. §§ 53-451, 53-452 (defining "property" to include "computer data[] … within a computer network" and imposing criminal and civil liability); Tex. Penal Code §§ 33.01(16), 33.02, Tex. Civ. Prac. & Rem. Code § 143.001 (similar); Ga. Code Ann. §§ 16-9-92(13); 16-9-93(c), (g) (defining "property" as including "data," and imposing criminal and civil liability for unauthorized viewing of "personal data relating to any other person"); Del. Code Ann. tit. 11, §§ 935, 941 (criminalizing "misuse" of "computer system information," and creating civil cause of action while defining "property" to include "computer … data"); Mass. Gen. Laws ch. 266 § 30(2) ("property" includes "electronically … stored data" under criminal law); N.Y. Penal Law § 156.00 ("'Computer data' is property" under criminal law).

Congress has also protected private data like Location History. The Stored Communications Act imposes criminal and civil liability on those who obtain unauthorized "access to a wire or electronic communication while

it is in electronic storage," 18 U.S.C. §§ 2701(a), 2707, and a warrant is needed to obtain the "contents of a wire or electronic communication that is in electronic storage." 18 U.S.C. § 2703(a), (b)(1)(A); JA-27-28, 27 n.10. As Google explained below, Location History constitutes the "contents" of an "electronic communication[]"—"the locations and travels recorded therein are fundamentally the contents of the journal, capable of being reviewed, edited, and deleted by the user." JA-28-29; *see* 18 U.S.C. § 2510(8). Indeed, law enforcement obtained a warrant in this case—albeit a constitutionally invalid one.

Given the property-like attributes of private data like Location History, the Court should hold that it is property for Fourth Amendment purposes. At common law, intangible property was a form of property. *See* 2 William Blackstone, *Commentaries on the Laws of England* chs. 2–3 (1766) (recognizing "incorporeal hereditaments" as property); Gregory S. Alexander, *Time and Property in the American Republican Legal Culture*, 66 N.Y.U. L. Rev. 273, 333 (May 1991) ("[I]ntangible interests were hardly unknown to the eighteenth-century common law of property."). In the Takings context, the Court has held that intangible interests are a form of constitutionally-protected property. *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1003 (1984). That reasoning should extend to the Fourth Amendment. *Carpenter*, 585 U.S. at 402 (Gorsuch, J., dissenting) ("[S]tate-created rights are sufficient to make something someone's property for constitutional purposes").

Further, the terms "papers" and "effects" are capacious enough to encompass private data like Location

History. In *Entick v. Carrington*, Lord Camden noted that the term "papers" is "general" and had been executed in previous warrants "in its utmost latitude." 19 How. St. Tr. 1029, 1065 (C.P. 1765); *Jones*, 565 U.S. at 405 (describing *Entick* as "the true and ultimate expression of constitutional law" (quotation marks omitted)).

"Effects" had an even broader meaning at the Founding and referred to anything a person had "of value." Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 Mich. L. Rev. 547, 708 n.462 (1999); *see also* Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 Yale L.J. 946, 985 (2016) ("'effects' was synonymous with personal property: possessions other than buildings and land").

Google stores Location History and uses it to support Google Maps, as well as its advertising business. Advertisers never obtain Location History; instead, they advertise through Google, which uses its own de-identified, "aggregate models" to target advertisements and improve Google Maps. Pet. App. 64a, 271a-272a. But the fact that Google stores and makes limited use of Location History data does not imply that users forfeit Fourth Amendment protection. *See Carpenter*, 585 U.S. at 399 (Gorsuch, J., dissenting) ("[T]he fact that a third party has access to or possession of your papers and effects does not necessarily eliminate your interest in them."); *Chapman v. United States*, 365 U.S. 610, 617-18 (1961) (warrantless search of tenant's apartment unconstitutional even when landlord consents).

Google is a bailee with limited rights to use the data, and the bailment does not undermine users' Fourth

Amendment rights. "[A] bailment is a delivery of a thing in trust for some special object or purpose, and upon a contract, expressed or implied, to conform to the object or purpose of the trust." Joseph Story, Commentaries on the Law of Bailments § 2, p. 2 (1832). Bailments often permit the bailee to make limited use of the property—indeed, in some cases, that use "is of the essence of the contract." *Id.* But "[a] bailee who uses the item in a different way than he's supposed to, or against the bailor's instructions, is liable for conversion." *Carpenter*, 585 U.S. at 399 (Gorsuch, J., dissenting); *see* 8 C.J.S., Bailments Westlaw (database updated Dec. 2025) § 43. Here, Google's privacy policy refers to Location History as "your location information in your account," JA-58; *see* JA-53 ("you're trusting us with your information"), while also authorizing Google to use it for certain narrow purposes, JA-61-63. When a user activates Location History, a pop-up window similarly characterizes Location History as "your data." JA-142. This language creates a bailment. *Sturm v. Boker*, 150 U.S. 312, 326, 329 (1893) (when contract "'consigned'" goods to third party, but "the title to the property" was "not changed," bailment was created).

Property in a bailee's hands is protected under the Fourth Amendment. For example, giving a sealed envelope to the mail carrier does not withdraw Fourth Amendment protection. *See Ex parte Jackson*, 96 U.S. 727, 733 (1877) (Fourth Amendment extends to "papers, thus closed against inspection, wherever they may be."). No one would think they lose Fourth Amendment protection over email because it is stored on a third party's servers. *See United States v. Warshak*, 631 F.3d 266, 286

(6th Cir. 2010). The same is true for Location History, which is simply another type of private data stored by Google.

This analysis establishes that, even under the *Carpenter* dissenters' approach, accessing Location History is a search. In *Carpenter*, Justice Thomas concluded that accessing CSLI was not a search because Carpenter "did not create the records, he does not maintain them, he cannot control them, and he cannot destroy them," and "[n]either the terms of his contracts nor any provision of law makes the records his." 585 U.S. at 342 (Thomas, J., dissenting); *accord id.* at 329 (Kennedy, J., dissenting) ("The defendants could make no argument that the records were their own papers or effects."). Here, by contrast, petitioner maintains, controls, and can destroy the records, and the terms of his contracts and provisions of law make the records his.

Likewise, Justice Alito found Carpenter had not "entrusted papers ... to the safekeeping of another," and the case did "not involve a bailment." *Id.* at 383 n.6 (Alito, J., dissenting). Here again, by contrast, Google is a bailee.

Finally, Justice Gorsuch's dissent suggested that a property-based approach might be meritorious but concluded that Carpenter had waived that argument. *Id.* at 406 (Gorsuch, J., dissenting). Here, petitioner has preserved the argument that Location History belongs to him. *See* Pet. Reply 8.

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

Additionally, users have a reasonable expectation of privacy in Location History. In *Carpenter*, this Court

held that users have a reasonable expectation of privacy in their CSLI. 585 U.S. at 310-11. The Court's reasoning in *Carpenter* applies with equal force to this case.

As *Carpenter* explained, CSLI is "detailed, encyclopedic, and effortlessly compiled." *Id.* at 309. Google Location History is more detailed and more encyclopedic than CSLI: it can pinpoint a user's location within three meters, every two minutes, down to elevation within a building. Pet. App. 104a, 271a-274a. In *Carpenter*, a full day of data points resulted in 101 data points. 585 U.S. at 302. Here, Google collected and turned over 76 data points on average, per person, from just two hours. Pet. App. 209a.

Carpenter emphasized the "retrospective quality" of CSLI, and that it is retained by wireless carriers for "up to five years." 585 U.S. at 312. At the relevant time, Location History was retained forever unless the user deleted it or enabled an auto-delete function. Pet. App. 283a-284a.

Carpenter noted that CSLI implicates privacy because "a cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." 585 U.S. at 311. So too here. The government is free to draw a geofence encompassing any of these types of locales. In this case, Step One of the geofence covered a church, while Step Two had no boundaries and showed users' trips to private residences, a school, and a hospital. *See* Pet. App. 54a; JA-158, 209 (Three Paths Video).

In *Carpenter*, the Court emphasized that CSLI

searches are "easy, cheap, and efficient compared to traditional investigative tools." *Carpenter*, 585 U.S. at 311. So too with Location History. When the government serves a geofence warrant, it merely asks Google to click a few buttons. *See* JA-97-113, 164-208.

Although geofence warrants do not tail a particular person's movements for a long period, they nonetheless present serious privacy concerns. When using geofence warrants, the government does not need days of data to reveal highly private information: it can *target* sensitive locations like "the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring). And once the government draws the geofence around the abortion clinic or union meeting, it obtains *everyone's* private information who was at those locations—not just the information of a suspect.

Indeed, users have a stronger expectation of privacy in Location History than they do in CSLI. The CSLI at issue in *Carpenter* was subject to limited federal privacy protections, but not subject to any requirement that law enforcement obtain a warrant before accessing it. *See* 47 U.S.C. § 222(c), (h)(1)(A); *Carpenter*, 585 U.S. at 359-60 (Thomas, J., dissenting). By contrast, as noted above, *supra* at 18-19, Congress *does* require a warrant before accessing Location History. The fact that Congress *itself* imposed a warrant requirement demonstrates that the "expectation of privacy is one that society is prepared to recognize as reasonable." *Carpenter*, 585 U.S.

at 304 (majority opinion) (quotation marks omitted).

C. The third-party doctrine does not apply.

In *United States v. Miller*, 425 U.S. 435, 442-43 (1976), and *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979), this Court recognized the third-party doctrine, under which a person relinquishes a reasonable expectation of privacy over certain information when he voluntarily discloses it to a third party. Here, the third-party doctrine does not apply for two reasons. First, the doctrine applies only to business records, and Location History is not a business record. Second, even if Location History were a business record, *Carpenter* establishes that the doctrine does not apply.

1. The third-party doctrine does not apply because Location History is not a business record.

In *Miller*, this Court held that a bank's customer lacked a reasonable expectation of privacy over canceled checks, deposit slips, and monthly statements. 425 U.S. at 442. The Court explained that the documents were "business records of the banks" that were "exposed to their employees in the ordinary course of business." *Id.* at 440, 442. It emphasized that "[t]he checks are not confidential communications but negotiable instruments to be used in commercial transactions." *Id.* at 442. In *Smith*, the Court similarly held that a person lacked a reasonable expectation of privacy over telephone numbers transmitted to the telephone company, explaining that the company used the numbers for "a variety of legitimate business purposes." 442 U.S. at 743. Hence, the

Court held, "it is too much to believe that telephone subscribers ... harbor any general expectation that the numbers they dial will remain secret." *Id.*

In *Carpenter*, the government urged this Court to extend *Miller* and *Smith* to CSLI, reasoning that "cell-site records are fair game because they are 'business records' created and maintained by the wireless carriers." 585 U.S. at 313. This Court declined that request. The Court did not take issue with the government's premise that cell-site records were business records, but nonetheless declined to apply the third-party doctrine given the privacy implications of accessing CSLI. *Id.* at 314. The dissenters, by contrast, would have extended *Smith* and *Miller* to CSLI, reasoning that "[c]ell-site records … are no different from the many other kinds of business records the Government has a lawful right to obtain by compulsory process." *Id.* at 322 (Kennedy, J., dissenting).

Under the approach of all nine members of the *Carpenter* Court, *Miller* and *Smith* do not extend to this case. Unlike in *Miller*, *Smith*, and *Carpenter*, Location History is *not* a business record.

In Google's words: "Google's 'Location History' is not a business record, but a journal of a user's location and travels that is created, edited, and stored by and for the benefit of Google users who have opted into the service." JA-15 (formatting modified). *Miller* and *Smith* reason that people have no expectation of privacy in how businesses will use their own business records; that reasoning does not apply when the business itself states that the data is *not* its business record.

Of note, Google's privacy policy states that information will be shared with the government to meet any applicable "legal process" or "enforceable government request." JA-70. That statement suggests that Google will share information only pursuant to a legally valid warrant—not that Google retains the unilateral discretion to treat Location History as a business record and voluntarily share Location History with the government.

Indeed, as noted above, *supra* at 5, Google has recently changed the way Location History is stored; it is now stored on the user's device rather than in the Sensorvault. Most users never noticed this change. Yet presumably the government would agree that the third-party doctrine does not apply and it needs a warrant to search a cell phone. It is difficult to understand why that opaque engineering change should make a Fourth Amendment difference. *Miller* and *Smith* invoke the expectations of a reasonable person. *Miller*, 425 U.S. at 442; *Smith*, 442 U.S. at 743. Here, reasonable persons would have no idea that their expectations had any reason to change.

In *Riley v. California*, 573 U.S. 373 (2014), the Court made a similar point. The government argued that, under the search-incident-to-arrest doctrine, it should be able to conduct warrantless searches of arrestees' cell phones, but conceded that "the search incident to arrest exception may not be stretched to cover a search of files accessed remotely—that is, a search of files stored in the cloud." *Id.* at 397. The Court rejected this proposed dichotomy between on-device and off-device data, concluding that if a warrant is needed to search files in the cloud,

a warrant should be needed to search files on a cell phone. As the Court explained, "[c]ell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference." *Id.* This case mirrors *Riley*. Cell phone users may not know if their Location History is stored on their cell phone or in the cloud. If a warrant is needed to search the former, it should be needed to search the latter.

2. Alternatively, the third-party doctrine does not apply under *Carpenter*'s rationale.

Even if Location History were a business record, the third-party doctrine would not apply. In *Carpenter*, the Court declined to apply the third-party doctrine to CSLI, concluding that there is a "world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today." 585 U.S. at 314. The Court's reasoning applies equally to this case.

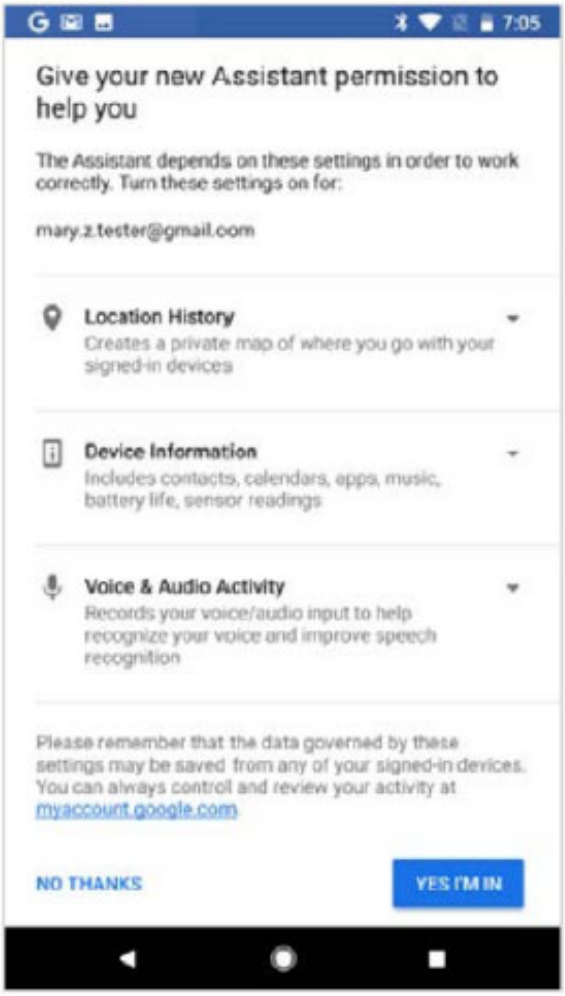
First, *Carpenter* emphasized that the privacy interests implicated by CSLI are greater than the privacy interests implicated by phone numbers and cancelled checks. 585 U.S. at 314-15. As discussed above, *supra* at 23, the Location History in this case is even more revealing than the CSLI in *Carpenter*, and certainly more revealing than the information in *Miller* or *Smith*.

Second, *Carpenter* held that sharing CSLI is not "voluntary"—even though a person is free to leave his cell phone at home or turn it off. 585 U.S. at 315. The Court

reasoned that in view of the ubiquitous nature of cell phones, the mere use of a cell phone cannot be construed as consent to disclose location data to the government. *See id.* Thus, *Carpenter* endorses a practical approach to voluntariness, focusing not on the theoretical ability to avoid data collection, but the practicalities of everyday life. Under that approach, turning over Location History is not voluntary.

Petitioner used an Android phone. During the relevant period, Android phone users[3] were prompted to enable Location History several times, beginning at set-up. Pet. App. 278a-279a. This is the screen people saw when they activated core phone capabilities:

[3] There was some uncertainty below on the precise software pathway petitioner used to activate his phone, and the district court reached no firm conclusion. Pet. App. 276a-277a.



JA-140. Users were thus told that unless they accepted multiple different services, including Location History, their device would not "work correctly." Further, even non-Android users who install Google apps—such as Google Maps—are constantly prompted to click "yes." Pet. App. 278a-281a; Fourth Circuit JA 1934-39 (noting

that users are told that Location History is required to "get the most from" Google Maps and are shown similar messages for other marquee Google functionalities). Users could activate Location History using the app, but could not delete it using the app; they instead had to visit myactivity.google.com. Pet. App. 283a.

Clicking "yes" should not be construed as consent to hand Location History to the government. A user clicking "yes" would have no idea that Google would collect information that would even make a geofence warrant *possible*. As the district court noted, petitioner was not told "how frequently Google would record [petitioner's] location" or "how precise Location History can be." Pet. App. 332a. Nor was he told that "Location History would automatically and precisely track his location even when he wasn't using his phone," across "all devices on which [he was] logged into," "even when [he had] deleted the respective Google app." Pet. App. 67a, 226a. And he certainly was not told his data would be shared with the government.

Indeed, in *Carpenter*, a person who wanted to keep his location private could simply decline to place or receive calls: "no call, no data." Pet. App. 208a. Here, the person would have to go to a web interface and request deletion of data he may not know was being collected. *See* Pet. App. 283a. In short, if handing CSLI to telecommunication companies does not trigger the third-party doctrine, handing Location History to Google should not either.

II. THE SEARCH VIOLATED THE FOURTH AMENDMENT BECAUSE THE WARRANT WAS AN UNCONSTITUTIONAL GENERAL WARRANT.

Because accessing Location History is a search, the government was required to obtain a warrant. "Although the ultimate measure of the constitutionality of a governmental search is 'reasonableness,'" this Court's "cases establish that warrantless searches are typically unreasonable where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing." *Carpenter*, 585 U.S. at 316 (quotation marks omitted).

Further, the government was required to obtain a *constitutionally valid* warrant. "[T]he presumptive rule against warrantless searches applies with equal force to searches whose only defect is a lack of particularity in the warrant." *Groh v. Ramirez*, 540 U.S. 551, 559 (2004). "[A] search conducted pursuant to a warrant that fails to conform to the particularity requirement of the Fourth Amendment is unconstitutional." *Id.* (citation omitted).

To determine whether the warrant in this case was constitutionally valid, the Court must drill down on precisely *what* was searched. As explained below, the warrant authorized the government to search *every* user's account—millions in total. Because the warrant did not identify the "place to be searched" with particularity but instead authorized the search of millions of distinct "places," it was an unconstitutional general warrant.

A. The warrant authorized the government to search every account.

At Step One, Google, at the government's behest, searched every user's Location History to check whether the device was within the geofence. The Court should hold that (1) the *government* conducted a Fourth Amendment search and (2) that search was of *every* user's Location History.

First, the search was attributable to the government. "Although the Fourth Amendment does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative, the Amendment protects against such intrusions if the private party acted as an instrument or agent of the Government." *Skinner v. Ry. Lab. Execs.' Ass'n*, 489 U.S. 602, 614 (1989). When the search is the product of "the Government's encouragement, endorsement, and participation," it is attributable to the government for Fourth Amendment purposes. *Id.* at 615–16.

That was the case here. Although a Google employee was responsible for inputting the relevant search terms and collecting the outputs, Google did not do so on its own or for any independent business purpose. Rather, the government encouraged, endorsed, and participated in that search: it served a search warrant on Google and compelled Google's compliance. Google was not acting on its "own initiative," but as the government's agent. *Id.* at 614.

Second, when Google obeyed the geofence warrant, it had "no way to identify which of its users were present in the area of interest without searching the LH

information stored by every [LH] user[.]" JA-27; *see* Pet. App. 287a (Google searched "*all* [Location History] data"). When Google checked every account for Location History responsive to the warrant, it conducted a Fourth Amendment search of every account. The government's contrary argument—that there is no search until within-geofence data is exposed to the government—is wrong.

Begin with the property-based approach. In *Jones*, this Court held that when the government puts a GPS device on the underside of a privately-owned car "for the purpose of obtaining information," it conducts a Fourth Amendment "search." 565 U.S. at 404-05. Attaching a tiny device to a vehicle's underside is a miniscule property-rights infringement that causes no quantifiable damage—but that did not matter. Drawing upon the seminal *Entick* case, the Court explained: "He is a trespasser, though he does no damage at all, if he will tread upon his neighbour's ground, he must justify it by law." *Id.* at 405 (quoting *Entick*, 95 Eng. Rep. 810). The Court elaborated that "[t]respass alone does not qualify, but there must be conjoined with that what was present here: an attempt to find something or to obtain information." *Id.* at 408 n.5.

Under that standard, the government, via Google, searched every account. As explained above, a core aspect of a user's property right is the right to exclude others from accessing their Google account. *Supra* at 15-16. The government violated that right by inspecting each user's account to check whether there was data within it responsive to the warrant. It did so in "an attempt to find something or to obtain information." *Jones*, 565

U.S. at 408 n.5. Therefore, even if the property-rights violation went unnoticed, the government conducted a search.

The same is true under the reasonable-expectations-of-privacy approach: if a person holds a reasonable expectation of privacy in data, then intruding into that data for purposes of extracting information violates that reasonable expectation. In *Kyllo v. United States*, 533 U.S. 27 (2001), this Court held that the use of a "thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within the home" constituted a search. *Id.* at 29. Likewise, in *Arizona v. Hicks*, 480 U.S. 321 (1987), this Court held that moving stereo equipment constituted a search, reasoning that a "search is a search, even if it happens to disclose nothing but the bottom of a turntable." *Id.* at 325. Both *Kyllo* and *Hicks* were reasonable-expectation-of-privacy cases, and they reach the same conclusion as *Jones*: if information is private, invading that privacy is a search.

True, unlike in *Hicks*, the police did not personally lay eyes on users' Location History. Instead, it delegated that task to Google's software tool. But a software-assisted search is still a search. If, for example, the government used Google's AI tool to read someone's emails and report suspicious activity, anyone would call that a search, even though the AI tool is software and even if the AI tool found nothing. The same is true here.

Or consider the following example. Today, unlike in 2019, Location History is stored locally on people's cell phones. Suppose a police officer demanded to search a person's Location History on his cell phone as to

whether he was at a particular location at a particular time—say, a political protest. Suppose the officer offered the assurance that he would use software to conduct the search, and if the software reported that the person was not at the protest, the officer would leave. Most people would rather obviously view this demand as an infringement on their reasonable expectation of privacy.

If that is a search, then the government searched each account here, too. After all, like in that hypothetical, the government used software to check whether each person was at a particular location at a particular time. Of course, unlike in that hypothetical, the government made its request directly to Google and did not notify users. But the fact that people were not told that their accounts were searched does not change the fact that their accounts were, in fact, searched.

Accentuating the privacy concerns here, Google was receiving as many as 180 geofence warrants per week. Note, *Geofence Warrants and the Fourth Amendment*, 134 Harv. L. Rev. 2508, 2510 (2021). One would suspect most people would think the government infringed on their reasonable expectation of privacy if they learned that, thousands of times per year, officials were rummaging through their personal data and checking whether they were at a particular location at a particular time.

The government's contrary view—that a search occurs only when Google *finds* responsive information and sends it to the government—is untenable. "[A] search is not to be made legal by what it turns up. In law it is good or bad when it starts and does not change character from

its success." *United States v. Di Re*, 332 U.S. 581, 595 (1948). Whether the government searched a particular user's account should not turn on whether information responsive to the warrant was found.

Indeed, in *Entick*, the search was unlawful even though officers "did not find what they searched for." 19 How. St. Tr. at 1038 (counsel for plaintiff). Consistent with *Entick*, the Fourth Amendment bans *both* unreasonable "searches" *and* unreasonable "seizures"—thus protecting against unreasonable searches, even if nothing is seized. Here, the government may have *seized* data from only 19 accounts, but it *searched* every user's account.

B. The Fourth Amendment required the warrant to identify *a particular account*, based on probable cause that evidence would be found *in that account*.

The Fourth Amendment requires a warrant "particularly describ[ing] the place to be searched, and the persons or things to be seized." U.S. Const. amdt. IV. The Fourth Amendment also requires that the warrant be issued "upon probable cause." *Id.* To satisfy that requirement, there must be probable cause that evidence will be found *in the place described with particularity*. *See Illinois v. Gates*, 462 U.S. 213, 238 (1983) (Fourth Amendment requires probable cause "that contraband or evidence of a crime will be found in a particular place").

Here, the warrant described the place to be searched as "Google LLC," JA-134, based on probable cause that evidence would be found "within computer servers

maintained or controlled by Google." JA-130. Those statements do not satisfy the Fourth Amendment's particularity and probable cause requirements. Instead, the warrant was required to identify a *particular* account, and establish probable cause that evidence would be found *in that account*. It could not authorize the search of millions of accounts in the hopes that incriminating location data would be found somewhere.

That conclusion follows from well-settled principles governing searches of physical property. For example, to authorize the search of an apartment within a larger apartment building, the warrant must identify the *particular apartment* and establish probable cause that evidence is in *that apartment*. A warrant that identifies an entire apartment building as the "place to be searched," based on probable cause that contraband exists *somewhere* in the building, violates the Fourth Amendment. *See* 2 Wayne R. LaFave, Search and Seizure § 4.5(b) (6th ed. 2020) ("[T]he probable cause requirement would be substantially diluted if a search of several living units could be authorized upon a showing that some one of the units within the description, not further identifiable, probably contained the items sought."); *Maryland v. Garrison*, 480 U.S. 79, 88 n.13 (1987) (upholding warrant when police made a factual error as to the number of dwellings in a building, but "expressly distinguish[ing] the facts of this case from a situation in which the police know there are two apartments on a certain floor of a building, and have probable cause to believe that drugs are being sold out of that floor, but do not know in which of the two apartments the illegal transactions are taking place").

Likewise, to obtain a warrant to open a mailed package, the government must identify *the particular package* and establish probable cause that evidence will be found *in that package*. If a warehouse contains a thousand packages, the government cannot declare the warehouse to be the "place to be searched" and hence obtain a warrant permitting it to open every single package based on probable cause that *at least one* package has contraband. *See Ex parte Jackson*, 96 U.S. at 733 (opening mail requires "like warrant … as is required when papers are subjected to search in one's own household"). For instance, in *United States v. Van Leeuwen*, 397 U.S. 249 (1970), this Court approved of a procedure in which two packages could be detained until warrants could be obtained showing probable cause that *each of those two individual packages* had contraband. *Id.* at 252-53 (when "probable cause existed for believing that the California package was part of an illicit project," "[a] warrant could have been obtained that day for the one package," and warrant was obtainable for second package only *after* "it was learned that the second package was also probably part of an illicit project").

These principles resolve how the Fourth Amendment applies here. Just as a warrant authorizing a search of a package requires the package to be identified with particularity based on probable cause that contraband is in that package, the search of a Google account requires the account to be identified with particularity based on probable cause that evidence is in that account. The government cannot declare "Google" as the "place to be searched," JA-127, 134, and obtain a warrant to

search millions of accounts on the theory that there is probative evidence in at least one of them.

Indeed, if this warrant's reference to "Google" satisfies the Fourth Amendment, absurd consequences would follow. Suppose the government obtained probable cause that *someone's* Gmail account contained an incriminating communication. Under the government's theory, the government could obtain a single warrant identifying "Google" as the "place" to be searched and then search *everyone's* Gmail accounts for the incriminating communication. That cannot be right.

Berger v. New York, 388 U.S. 41 (1967), bolsters that conclusion in the context of electronic recording devices. This Court held that identifying a particular person in the warrant is not enough to satisfy the particularity requirement: the warrant must also identify a specific communication. *Id.* at 59. It follows *a fortiori* that a warrant that does not identify a particular account, but instead authorizes inspection of millions of people's private data, cannot be particularized.

Consistent with *Berger*, the Stored Communication Act states that a warrant will not issue unless the government shows that "the contents of a wire or electronic communication"—*i.e.*, *one particular* communication—are "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). It does not permit the government to obtain one warrant to search millions of accounts.

Return to an example above. Today, Location History is stored locally on cell phones. Suppose the government wanted to search everyone's Location History.

It seems obvious the government could not obtain a single warrant authorizing a search of every Google user's cell phone in America. The result should not change because, at the relevant time, Google stored information on its own server. Just as in *Riley*, the government could not evade the warrant requirement because data was on a cell phone rather than a server, *see* 573 U.S. at 397, so too, here, the government cannot evade the warrant requirement because data is on a server rather than a cell phone.

C. The geofence warrant was an unconstitutional general warrant.

The geofence warrant violated the Fourth Amendment's particularity requirement. Rather than identify a specific account with particularity, it unconstitutionally authorized the search of millions of separate accounts and the seizure of incriminating location data in *whomever's* account it might be found.

The warrant also violated the probable cause requirement. There was not probable cause that evidence would be found in any particular account—which is why Google had to search all of them.

These are not mere technical defects. The flaws in this warrant go to the heart of the Fourth Amendment. The Fourth Amendment "was the founding generation's response 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*, 573 U.S. at 403.

Writs of assistance—a particularly loathed type of general warrant—provide a close analogy. "Vivid in the memory of the newly independent Americans were those general warrants known as writs of assistance under which officers of the Crown had so bedeviled the colonists." *Stanford v. Texas*, 379 U.S. 476, 481 (1965). "[W]rits of assistance ... noted only the object of the search—any uncustomed goods—and thus left customs officials completely free to search any place where they believed such goods might be." *Steagald v. United States*, 451 U.S. 204, 220 (1981). They were called "writs of assistance" because they "commanded 'all officers and subjects of the Crown to assist in their execution.'" *United States v. New York Tel. Co.*, 434 U.S. 159, 180 n.3 (1977) (Stevens, J., dissenting in part) (citation omitted). Writs of assistance were so reviled that they "helped spark the Revolution itself." *Carpenter*, 585 U.S. at 303-04.

The technology has changed, but the principle has not. The geofence warrant was the modern edition of a writ of assistance: it commandeered Google to execute a general warrant noting "only the object of the search" and leaving police "completely free to search any place"—here, any user account—"where they believed" the evidence might be. *Steagald*, 451 U.S. at 220. Such warrants are anathema to the Fourth Amendment.

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

At Step One, Google returned the location information of 19 users, including petitioner, who were within the geofence. Even if, as the government claims,

digitally inspecting millions of people's accounts was not a Fourth Amendment "search," the government, at a minimum, conducted a Fourth Amendment "search" of those 19 users. That search was unconstitutional.

A. At Step One, the government searched the 19 users' accounts.

At Step One, Google, at the government's behest, copied the private data of those 19 users and transmitted it to the government, which then examined it to check for incriminating movements. In petitioner's view, the correct Fourth Amendment analysis requires finding that the government *searched* every account and *seized* data from those 19 users. But, at a minimum, the government searched those 19 users.[4]

Under the property-based approach, the government's collection and analysis of private data readily satisfies the requirement of an intrusion on property interests. *Supra* at 16-17 (citing case law characterizing the collection of private data as conversion or trespass). Under the reasonable-expectation-of-privacy approach, the exposure of private information to the government is a search. *See Kyllo*, 533 U.S. at 37-38.

To be sure, the Location History data was provided in conjunction with anonymous account numbers rather

[4] In petitioner's view, at Step One, the government conducted searches *and* seizures of the 19 users. Likewise, at Steps Two and Three, the government conducted additional searches of users *and* seizures of their data. In this brief, petitioner focuses on the searches.

than names. But that anonymity is both irrelevant to the Fourth Amendment and illusory.

First, anonymity is irrelevant. Whether the government has conducted a search does not turn on whether the government knows who was searched. In many of this Court's Fourth Amendment cases, the government conducted a search without knowing the identity of who was searched; that did not alter the Fourth Amendment analysis. In *Riley*'s companion case, for example, the police arrested the defendant (Wurie), searched his cell phone, and did not determine his identity until after the search, yet the Court still held that the defendant was searched. 573 U.S. at 380; *see also, e.g.*, *Bond v. United States*, 529 U.S. 334 (2000) (impromptu search of bus passenger's bag). That has to be right: If an officer enters a house and rifles through the drawers, then he surely conducts a search regardless of whether he knows who lives in the house. This case—where the government rifled through the Location History of 19 people to check for incriminating movements—is no different.

Second, anonymity is illusory because it will often be easy to infer a person's identity based on a snapshot of his movements. Here, for example, after Step Two—when the government obtained two hours' worth of purportedly anonymized location information for nine people—petitioner's expert witness showed how three of those people's identities could be discerned by combining the information on their movements with public information like tax records and social media postings. Pet. App. 305a.

Of course, whether people's identities can be inferred from their movements will vary from case to case. But

whether an action is a search should not turn on an *ex post* assessment of whether individuals' identities can be determined from the provided data. Officers and magistrates need to know whether a search is occurring *before* the search. *See Kyllo*, 533 U.S. at 39 (rejecting approach under which officers "would be unable to know in advance" whether their search would be constitutional). Rather than forcing magistrates to make speculative judgments about whether location information will allow the government to infer a person's identity, the Court should hold that whenever the government collects Location History, it conducts a search.

B. The warrant was unconstitutional because it did not identify particular accounts based on probable cause that evidence would be in those accounts.

Even if only the 19 accounts (as opposed to millions of accounts) were searched, the warrant was still unconstitutional.

The warrant recites:

> For each type of Google account that is associated with a device that was inside the [geofence], during the time frame listed above, Google will provide "anonymized information" regarding the Accounts that are associated with a device that was inside the described geographical area during the time frame described above.

JA-136. That statement does not satisfy the Fourth Amendment's requirement of a warrant "particularly describing the place to be searched."

The Fourth Amendment's particularity requirement is satisfied when "the description is such that the officer with a search warrant can, with reasonable effort ascertain and identify the place intended." *Steele v. United States*, 267 U.S. 498, 503 (1925). Thus, here, the Fourth Amendment requires the officer to be able, "with reasonable effort," to "ascertain and identify" from the warrant the *particular accounts to be searched*. *Id.* For example, a warrant that specified "Okello Chatrie's account" would be particularized. The government need not know the person's name: "the account belonging to JohnDoe123@gmail.com" would suffice. But the warrant must point to a particular account.

Here, though, the warrant's description of the accounts to be searched—essentially, "whoever's accounts contain data within the geofence"—provided insufficient information for the officer to know whose accounts to search. Instead, the officer gleaned this information only *after* Google searched the Sensorvault and located accounts containing data within the geofence. Under the Fourth Amendment, however, the *warrant itself* must contain a particularized description of the places to be searched; identifying those places cannot turn on information not available to the magistrate.

This principle implements the very "point of the Fourth Amendment"—to require a prior finding of probable cause that particular evidence will be found in a particular place "by a neutral and detached magistrate instead of … by the officer engaged in the often competitive enterprise of ferreting out crime." *Johnson v. United States*, 333 U.S. 10, 13-14 (1948). This "separation of functions" is foundational to the Fourth

Amendment, *Gerstein v. Pugh*, 420 U.S. 103, 117-18 (1975), and central to the common-law principles that inform its meaning. "It is not fit that the receiving or judging of the information should be left to the discretion of the officer. The magistrate ought to judge; and should give certain directions to the officer." *United States v. U.S. Dist. Ct. for E. Dist. of Mich.*, 407 U.S. 297, 316 (1972) (quoting *Leach v. Three of the King's Messengers*, 19 How. St. Tr. 1001, 1027 (1765)).

Due to this flaw in the warrant, there was also a violation of the Fourth Amendment's probable cause requirement. To satisfy that requirement, there must be probable cause that "evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238. That requirement cannot be satisfied when, as here, the warrant does not identify a particular place. At most, the warrant establishes probable cause that there is relevant evidence *in some user's account in the Sensorvault.* JA-132-33, 136 (describing evidence that relevant evidence exists at Google as a whole). But there was no probable cause that any *particular* account contained relevant evidence.

United States v. Grubbs, 547 U.S. 90 (2006), confirms this analysis. In *Grubbs*, this Court addressed so-called "anticipatory warrants"—that is, warrants that "subject their execution to some condition precedent other than the mere passage of time—a so-called 'triggering condition.'" *Id.* at 94. The Court held that, to satisfy the Fourth Amendment, there must be "probable cause to believe the triggering condition *will occur*." *Id.* at 96-97. Otherwise, "an anticipatory warrant could be issued for every house in the country, authorizing search and seizure *if* contraband should be delivered—though for any

single location there is no likelihood that contraband will be delivered." *Id.* at 96.

The geofence warrant is just like that latter warrant—the one the *Grubbs* Court believed self-evidently unconstitutional. To borrow *Grubbs*' language, the warrant issued for every account in the country, authorizing search *if* relevant Location History should be found—though for any single account there was no likelihood that relevant Location History would be found. Just as a warrant authorizing a search at "wherever the contraband is delivered" violates the Fourth Amendment, so too does a warrant authorizing a search at "wherever the within-geofence location information is found."

United States v. Karo, 468 U.S. 705 (1984), is not to the contrary. In *Karo*, this Court held that the police violated the Fourth Amendment when, without obtaining a warrant, it placed a beeper in a container of chemicals that was later delivered to a buyer's home. The Court explained that "the monitoring of a beeper in a private residence … violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence." *Id.* at 714. In dicta, the Court emphasized that a warrant could have been obtained. The Court rejected the government's argument that "it would be impossible to describe the 'place' to be searched, because the location of the place is precisely what is sought to be discovered through the search," holding that "it will still be possible to describe the object into which the beeper is to be placed, the circumstances that led agents to wish to install the beeper, and the length of time for which beeper surveillance is requested." *Id.* at 718. The Court held that "this

information will suffice to permit issuance of a warrant authorizing beeper installation and surveillance." *Id.*

Thus, in the hypothetical warrant postulated in *Karo*, a specific object is identified with particularity—the "object into which the beeper is to be placed." *Id.* Here, by contrast, the warrant identifies no particularized object akin to the specific container in *Karo*.

Moreover, in *Karo*, the container—and hence the beeper—could only be in one place at any given time, obviating any concern that the warrant would authorize a government dragnet. Here, unlike in *Karo*, the warrant authorized the search of an indeterminate number of people who were in the vicinity of the robbery. In short, *Karo*'s dictum should not apply to this distinct fact pattern.

C. The warrant was unconstitutional because there was no probable cause that every user in the geofence had relevant evidence.

Even if the warrant's reference to the "Accounts that are associated with a device that was inside the described geographical area during the time frame described above," JA-136, was sufficiently particularized, the geofence warrant would still violate the Fourth Amendment. The warrant application did not establish, and could not have established, probable cause to search every Location History user "inside the described geographical area during the time frame described above." *Id.*

What happened here was not like reviewing surveillance video or interviewing all witnesses in the vicinity

of the crime. Instead, the government *searched* all Location History users in the vicinity of the crime.

To satisfy the Fourth Amendment, a warrant must identify each place to be searched with particularity and establish probable cause that evidence will exist in each of those places. *See Gates*, 462 U.S. at 238 (probable cause requires "a fair probability that contraband or evidence of a crime will be found in a particular place"). Here, assuming that the warrant's indirect reference to the 19 accounts searched at Step One was sufficiently particularized, the government would have to show probable cause that evidence would appear in each of those accounts.

Probable cause was absent. There was not a "fair probability" that "contraband or evidence of a crime" would be found in a person's account merely because he was *near* a robbery. The "mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979). Here, the warrant impermissibly authorized the collection of people's private data *solely* because of their "mere propinquity," in time and space, to the robbery.

The lack of probable cause here is particularly clear given the geofence's size. As the district court emphasized, "it is difficult to overstate the breadth of this warrant, particularly in light of the narrowness of the Government's probable cause showing." Pet. App. 319a. Based solely on the fact that the perpetrator was holding a cell phone, "law enforcement simply drew a circle with a 150- meter radius that encompassed the Bank, the entirety of the Church, and the Church's parking lot." *Id.*

And, given the radius of Google's "confidence intervals" (*i.e.*, the margin of error), the warrant might have reported the locations of someone dining in a nearby restaurant, staying in a nearby hotel, or living in his own home at a nearby apartment complex or senior living facility. Pet. App. 319a-320a. "[F]ootage depicting the perpetrator holding a phone to his ear" could not justify such a "sweeping warrant." Pet. App. 320a.

In an age when cell phones are ubiquitous, it is inconceivable that, merely based on petitioner's apparent use of his device, the government could have obtained warrants to search the physical papers or effects of every person who was near the bank, regardless of whether they were in church or walking on the street. The result should not change merely because the government searched their digital papers instead.

IV. THE STEP TWO AND STEP THREE SEARCHES VIOLATED THE FOURTH AMENDMENT.

Even if the Step One search complied with the Fourth Amendment, the Steps Two and Three searches did not.

A. The government conducted searches at Steps Two and Three.

At Step Two, the government sought and obtained additional information: for 9 of the 19 individuals, it obtained an extra hour's worth of location information, including information outside the geofence. Pet. App. 300a; JA-106-108. At Step Three, the government obtained yet more information: the identity of three suspects. JA-110-111, 206-208.

When the government undertakes a "new invasion of … privacy" and obtains additional private information, it conducts a fresh Fourth Amendment search. *Hicks*, 480 U.S. at 324-25. Here, when the officer obtained additional private information at Step Two and yet more at Step Three, he conducted Fourth Amendment searches.[5]

B. The warrant was defective and could not authorize the Step Two and Three searches.

Because the government did not obtain additional warrants at Steps Two and Three, the *original* warrant was required to satisfy the particularity and probable cause requirements with respect to the *subsequent* searches. It did not.

1. The warrant was not particularized.

First, the warrant did not identify the nine accounts subject to the additional Step Two search, or the three accounts subject to the additional Step Three search, with particularity. Nor did it even identify the process to identify those accounts with particularity.

The warrant application merely explained the three-step process and stated that, at the second step, the

---

[5] Even if, as the government contends, "searches" occur only when data is de-anonymized, searches occurred here at Step Two (when user information could be de-anonymized based on publicly-available information) and Step Three (when users were explicitly de-anonymized by Google). *See* Pet. App. 121a (Berner, J.) (reaching this conclusion).

government might find some additional unspecified set of accounts and might deem it useful to obtain additional location information. JA-130-131. But it gave the government unfettered discretion to identify the subset of accounts at Step Two for which additional information would be sought.

As the district court elaborated, the warrant "contains no language objectively identifying *which* accounts for which officers would obtain further identifying information," no "objective guardrails by which officers could *determine* which accounts would be subject to further scrutiny," and no limit on "the *number* of devices for which agents could obtain identifying information." Pet. App. 328a. Indeed, initially, at Step Two, the government sought more detailed information on all 19 accounts; it obtained 9 only because Google pushed back. Pet. App. 299a-300a, 329a. Even then the detective "did not specify to Google why he was choosing these particular users." Pet. App. 329a.

The same is true for Step Three. The warrant stated that the government might seek to unmask an unspecified number of users based on information obtained from the first two steps. JA-137. The warrant identified no criteria for making this determination.

As such, it was impossible, based on the warrant, to "ascertain and identify" the accounts that were searched at Steps Two and Three. *Steele*, 267 U.S. at 503. Because the warrant gave the officer complete discretion in deciding who to search, it was not particularized. *See* Pet. App. 329a-330a (reaching the same conclusion); *Steagald*, 451 U.S. at 220 (Fourth Amendment prohibits warrants that "leave[] to the unfettered discretion of the

police the decision as to which particular homes should be searched").

2. The warrant was not supported by probable cause.

The government's initial warrant application also did not establish probable cause to search the nine accounts at Step Two or the three accounts at Step Three.

The government identified the nine accounts in Step Two based on information received in Step One. And it identified the three accounts in Step Three based on the information it received in Step Two. But the government did not present the Step One or Step Two information to the state magistrate, because it obtained the warrant *before* Step One. Thus, as Judge Berner observed, "When the detective applied for the geofence warrant, it would have been impossible for him to describe the facts that would ultimately support his decision to conduct a Fourth Amendment search targeting nine particular individuals." Pet. App. 122a.

The government could have attempted to obtain a supplemental warrant, but it never did. The officer "sought judicial authorization only once—prior to the first request to Google." Pet. App. 126a. "Because the detective could not explain why he would eventually search the Location History data of certain, then-unknown users in Google's dataset, he failed to show probable cause to conduct the second and third requests." *Id.*

Effectively, the government transformed Google into the magistrate. "Google, not a magistrate, was the sole entity that could confine the scope of the ultimate search." *Id.* At Steps Two and Three, Google did ask

that the detective narrow his initial request. Pet. App. 299a-300a. But a warrant must be issued by an *actual* magistrate. *Grubbs*, 547 U.S. at 99 ("The Constitution protects property owners ... by interposing, *ex ante*, the deliberate, impartial judgment of a judicial officer between the citizen and the police[.]" (quotation marks and ellipses omitted)). "Probable cause determinations cannot be delegated to private entities." Pet. App. 126a.

Because the government conducted searches at Step Two and Step Three—and because the geofence warrant, to the extent it authorized those searches, was unconstitutional—those searches violated the Fourth Amendment.

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

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

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

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