No. 25-112

IN THE

Supreme Court of the United States

OKELLO T. CHATRIE,

Petitioner,

v.

UNITED STATES,

Respondent.

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

BRIEF OF TECHNOLOGISTS AS *AMICI CURIAE* IN SUPPORT OF NEITHER PARTY

CHRISTOPHER T. BAVITZ
Counsel of Record
MASON A. KORTZ
MICHAEL ROSENBLOOM
CYBERLAW CLINIC
HARVARD LAW SCHOOL
1557 Massachusetts Avenue
Cambridge, MA 02138
(617) 384-9125
cbavitz@law.harvard.edu

RICHARD SALGADO
1746 Fordham Way
Mountain View, CA 94040

JONATHAN MAYER
PRINCETON UNIVERSITY
307 Sherrerd Hall
Princeton, NJ 08540

Counsel for Amici Curiae

March 9, 2026

120958

COUNSEL PRESS

(800) 274-3321 • (800) 359-6859

TABLE OF CONTENTS

Table of Contents

TABLE OF CITED AUTHORITIES

Page

CASES

Page

Cited Authorities

Page

CONSTITUTIONAL PROVISIONS

STATUTES

Page

LEGISLATIVE HISTORY

OTHER AUTHORITIES

Page

INTEREST OF *AMICI CURIAE*[1]

Amici curiae are technical experts in the design and implementation of online services, cybersecurity, and data privacy. *Amici* aim to assist the Court in identifying a framework for resolving this case and foreseeable similar cases in a manner consistent with how technology is designed, implemented, and used.

Steven M. Bellovin is the Percy K. and Vida L. Hudson Professor Emeritus of Computer Science at Columbia University.

Joseph Bonneau is an Associate Professor of Computer Science at the Courant Institute, New York University.

Vint Cerf is an Internet pioneer and co-designer of the TCP/IP protocols and the architecture of the Internet, and is widely known as one of the "Fathers of the Internet."

Shaanan Cohney is the Deputy Head of School, Computing and Information Systems, at the University of Melbourne.

Zakir Durumeric is an Assistant Professor of Computer Science at Stanford University.

---

1. Pursuant to Supreme Court Rule 37, counsel for *amici curiae* represent that no counsel for a party authored this brief in whole or in part and that no parties or their counsel, nor any other person or entity other than *amici* and their counsel, made monetary contributions intended to fund the preparation or submission of this brief.

Laura Edelson is an Assistant Professor of Computer Science at Northeastern University.

David Evans is the Olsen Bicentennial Professor of Engineering and a Professor of Computer Science at the University of Virginia.

Stephanie Forrest is a computer scientist with over 30 years of experience in cybersecurity.

Grant Ho is an Assistant Professor of Computer Science at the University of Chicago.

Tadayoshi Kohno is a Professor and the McDevitt Chair in Computer Science, Ethics, and Society in the Department of Computer Science and the Center for Digital Ethics at Georgetown University.

Frank Li is an Assistant Professor in the School of Cybersecurity and Privacy at the Georgia Institute of Technology.

Jonathan Mayer is an Associate Professor of Computer Science and Public Affairs at Princeton University.

Alan Mislove is a Professor and the Senior Associate Dean for Academic Affairs at the Khoury College of Computer Sciences at Northeastern University.

Arvind Narayanan is a Professor of Computer Science at Princeton University and the Director of its Center for Information Technology Policy.

Bruce Schneier is a Fellow and Lecturer at the Harvard Kennedy School and the Munk School at the University of Toronto.

Eugene H. Spafford is a Distinguished Professor of Computer Science at Purdue University.

Alexander C. Stamos is the Chief Product Officer of Corridor Security Inc. and a Lecturer in Computer Science at Stanford University.

SUMMARY OF ARGUMENT

This case involves location data, but it is not about location data. This case involves data centers and servers, but it is not about those either. It is about the information we keep in our online accounts. And it is about the circumstances, if any, under which the government may inspect that data across millions of accounts. *Amici* submit this brief to provide the Court with independent technical analysis that explains why the "account," from a technical perspective, is the correct logical unit searched pursuant to the warrant.

The concept of an "account" is foundational to the design, implementation, and use of computer systems. For over half a century, it has been the primary way multi-user systems segregate and manage virtual, private spaces for data storage and processing. Today, many people

have accounts with a broad range of services, using them to store everything from personal communications to passwords. The idea of a personal account has become so familiar that it has found its way into statutes, common law decisions, and even this Court's precedents.

In today's hyperscale environments, accounts are more relevant than ever. Data and processes are no longer bound to distinct physical architecture, yet they remain in many cases bound to user identity through accounts. The same concepts of stable identifiers, access controls, and permissions that defined multi-user mainframes in the 1960s are still in use by globe-spanning services today. For this reason, analyzing searches in terms of the accounts involved, separate from the physical infrastructure involved or the type of data retrieved, is appropriate from a technical point of view.

Treating the account as the analytically relevant unit for a search draws a clear line between searches of provider-held business records, as seen in *Carpenter*, and searches of user-held account data, as seen here. When the government compels a service provider like Google to retrieve information that is logically stored in accounts, it necessarily commands the provider to cross the digital boundary of each account searched. This act, the compelled intrusion into the account, provides a relevant moment for Fourth Amendment analysis. Through the application of established Fourth Amendment principles, this Court can decide whether that intrusion amounts to a search in the constitutional sense.

Acknowledging that an account is a "unit of search" would promote administrability, predictability, and

cohesion in this area of law. An account-centric approach would ground Fourth Amendment analysis in over half a century of stable computing architecture. It would also avoid factual rabbit holes, accord with scientific research on the difficulty of discerning data sensitivity, provide meaningful guidance to lower courts and legislatures, and provide valuable clarity for a broad category of fact patterns while reserving the disposition of related doctrinal tussles for future cases.

ARGUMENT

On June 14, 2019, as part of an investigation into the robbery of a federal credit union, law enforcement obtained a so-called geofence warrant from a state magistrate judge. JA 127-28. The search warrant commanded Google to assist the government by looking through its "computer servers" for data reflecting the location of mobile devices. *Id.* at 129-31. Where the data suggested a device was in the area of the credit union around the time it was robbed, the warrant directed Google to disclose information about the Google account associated with that device.

Google had only one way to execute the warrant as commanded. It had to "search across all [Location History] data," JA 50, all of which was stored in non-public Google accounts, *id.* at 42-45. Google did so. *Id.* at 49-50.

How should courts reason about law enforcement surveillance, effectuated through an online service, under the Fourth Amendment? The warrant's text, which reflects a position advanced by some participants in this case, obscures more than it illuminates. An online service's "computer servers" can be located in dozens of

data centers across the globe. *E.g.*, *Locations of Google Data Centers*, GOOGLE[2] (identifying 29 U.S. locations with Google data centers and 50 locations globally). As we explain below, a user's data can be spread across many servers and storage devices, and it may reside in multiple data centers in different states or even different countries. There is no readily discernible physical location for the relevant bits that the government seeks and that the online service stores. And even if the government could physically seize all the servers and devices that possibly stored the data that it sought, it would assuredly lack the technical capacity to analyze them.

Rather than identifying discrete physical computers, warrants like this one compel online services to make sense of their massive and complex technical infrastructure through abstractions. One of the most common and long-standing abstractions in data storage is the concept of a user account, a virtual space identified with a specific user and bounded by access controls. Our argument in this brief is simple: for Fourth Amendment purposes, the Court should make sense of online service architecture just as the services and their users do.

From a technical perspective, the government's conduct in this case involved accessing Google accounts and analyzing the Location History data within them. This is a simple proposition, but it has profound consequences. Treating these accounts as cognizable "units of search" under the Fourth Amendment would obviate the need for fact-intensive line drawing about technical details, avoid constitutionalizing the three-step

2. https://datacenters.google/locations/

process, and leave distinct doctrinal puzzles for future cases. Accordingly, *amici* respectfully urge this Court to assess whether there was a search within the meaning of the Fourth Amendment and whether the warrant satisfied constitutional requirements from an account-based perspective.

I. As a technical matter, the government, through Google, searched user accounts when executing the warrant.

Since the 1960s, computer systems have relied on the notion of "accounts": separate means of accessing and using systems, allocated to users and protected by access controls and permissions, with distinct virtual spaces for storing and processing data. The underlying implementations of "accounts" have changed significantly over time, from early time-shared mainframes with punch-card readers up to modern "hyperscaler" services that run complex generative artificial intelligence models. But the logical abstraction of an "account" has remained a foundation of system design.

Today, the concept of an online account is a familiar part of our world. In the context of this case, it is the appropriate unit of Fourth Amendment analysis, scoping the virtual places or areas that the government could (and did) search.[3] In modern online services, user content is stored, segregated, and accessed through account-defined spaces enforced by identity, permissions, and privileged

3. Except where explicitly noted, *amici* use "search" in the technical, rather than constitutional, sense.

access controls.[4] Alternate abstractions, urged by others in this case, do not match how the technology works or the way it appears to ordinary users. Describing the place to be searched in terms of Google's "computer servers" obscures the architecture that matters. Likewise, characterizing the information as "business records" and Google as a "custodian of records" is contrary to how systems are structured and how users interact with services like Location History. An account, on the other hand, is both technically and socially cognizable as a discrete unit for Fourth Amendment analysis.

A. The "account" is a well-established concept in the history of computing that is technically, socially, and legally cognizable.

Accounts have existed since the early years of digital computing. In the time-sharing era, beginning in the 1960s, multiple users accessed the same central mainframe computer through separate terminals, often simultaneously. *See*, *e.g.*, IEEE Computer Society, *Compatible Time-Sharing System (1961-1973)* (2011).[5] That

4. This brief is focused on providing technical analysis, and *amici* do not take a position on which doctrinal basis is appropriate for recognizing "accounts" as Fourth Amendment units. The Court could recognize access to an account as a trespass onto property (as in *Jardines*), a trespass consisting of interference with property (as in *Jones*), government conduct that implicates privacy statutes (as members of the Court suggested in *Carpenter*), or an invasion of a reasonable expectation of privacy (as in *Katz*).

5. https://multicians.org/thvv/compatible-time-sharing-system.pdf

environment, and the subsequent adoption of workstation networking in the decades following, depended on a reliable way to identify each user, authenticate access, allocate resources, and maintain separation among files, processes, and permissions. *See, e.g.*, C. Marceau, *Multics System-Programmers Manual*, Section BQ.4.00 (1967)[6] (describing procedures for identifying and providing access to users). The account provided that structure. It gave shared computing a logical architecture and it established discrete, access-controlled user spaces.

Over time, computing expanded beyond government, educational, and business settings to the home. As operating systems for these relatively low-power consumer machines matured, account provisioning became a basic operating-system function in consumer systems. *See Evolving the Windows User Model – A Look to the Past*, Microsoft Security Community Blog (Jan. 23, 2025).[7] User-specific logins, profiles, settings, and permissions came to define the scope of each user's workspace and authority, while elevated privileges remained reserved for the administrator account. These account structures persist today in current operating systems for desktop and laptop computers, smartphones and tablets, and even televisions and cars.

Cloud computing extended this long-standing design principle across distributed infrastructure. As storage

6. https://multicians.org/mspm/bq-4-00.670526.user-id-databases.pdf

7. https://techcommunity.microsoft.com/blog/microsoft-security-blog/evolving-the-windows-user-model-%E2%80%93-a-look-to-the-past/4369642

and processing moved off the local device and into feature-rich and powerful systems operated by service providers, the account continued to define the user's digital space. *See*, *e.g.*, *Change From a Local Account to a Microsoft Account in Windows*, Microsoft Support.[8] It links data to a particular user, governs access to that data, and allows the provider to store, retrieve, process, and secure user information across large-scale systems. Across mainframes, personal computers, and cloud platforms, the account has remained the enduring unit by which computing systems associate digital resources with particular users and preserve separation, control, and continuity in ordinary use.

Accounts are a familiar enough concept that they have made their way into legal doctrine. This Court has repeatedly spoken of online accounts in straightforward terms, treating their nature as self-evident in light of common experience. *See*, *e.g.*, *Murthy v. Missouri*, 603 U.S. 43, 58-62 (2024) (examining standing implications of restrictions on accounts); *Lindke v. Freed*, 601 U.S. 187, 201-04 (2024) (referring to user control of account in resolving state action question); *City of Ontario v. Quon*, 560 U.S. 746, 752 (2010) (using privacy interest in personal email account as a baseline comparator for intrusiveness of search). Other courts have recognized accounts, and their contents, as the object of both property and privacy rights. *See*, *e.g.*, *JLM Couture, Inc. v. Gutman*, 91 F.4th 91, 102 (2d Cir. 2024) (analyzing social media account as discrete unit of property interest); *Lazette v. Kulmatycki*,

8. https://support.microsoft.com/en-us/windows/change-from-a-local-account-to-a-microsoft-account-in-windows-395203bf-9f1b-eb24-b042-5b8dae6c1d20

949 F. Supp. 2d 748, 760-61 (N.D. Ohio 2013) (holding that unwanted access to email account could support common law claim for invasion of privacy); *Ajemian v. Yahoo!, Inc.*, 84 N.E.3d 766, 773 (Mass. 2017) (treating decedent's email account as common law property of estate).

Federal statutes that protect the privacy of systems and data also implicitly recognize the concept of an account. The Electronic Communications Privacy Act of 1986 (ECPA) presupposes both a scope of "authorization" for access to stored communications and of the possibility of access "exceed[ing] authorization," that is, access beyond the scope of one's own account. 18 U.S.C. § 2701; S. Rep. No. 99-541, at 36 (1986) ("For example, a computer mail facility authorizes a subscriber to access information in their portion of the facilities storage. Accessing the storage of other subscribers without specific authorization to do so would be a violation of this provision."); H.R. Rep. No. 99-647, at 63 (1986) (describing how ECPA protects email when it is "accessible specifically" by a user). Similarly, the primary federal computer crime law, the Computer Fraud and Abuse Act of 1986 (CFAA), deals with authorized and unauthorized access to computer systems. 18 U.S.C. § 1030. The CFAA recognizes that there are spaces in a computer system where a person does and does not have authorized access to enter, based on whether there is a "gate" that restricts access. *Van Buren v. United States*, 593 U.S. 374, 390-91 (2021). Accounts, protected by access controls, are the technical implementation of those legally recognized gates.

Accounts appear textually in statutory law as well. Indeed, several surveillance laws treat accounts as

personal identifiers. The USA FREEDOM Act, Pub. L. 114-23, § 104, 129 Stat. 268, 274 (2015), treats an "account" as a "specific selection term." This makes an account a legally cognizable personal identifier, comparable to a person's name or address, that the government can use to seek data under the (now sunsetted) Section 215 of the USA PATRIOT Act, Pub. L. 107-56, § 215, 115 Stat. 272, 287 (2001), or the pen register and trap and trace authority of the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1842. The legislative history behind a 2001 amendment to the Wiretap Act noted that "an Internet user account" is a type of "facility" that can be targeted for surveillance. H.R. Rep. No. 107-236, at 52-53 (2001). The CLOUD Act's executive-agreement framework likewise requires that qualifying foreign orders use a target identifier such as an "account." 18 U.S.C. § 2523(b)(4)(D)(ii).

B. Accounts are the relevant unit of personal access in modern hyperscale systems.

While the warrant in this case called for a search of Google's "computer servers," the only way Google could carry out that search was to examine information stored within user accounts. To understand why the warrant's execution required an account-by-account search, it helps to understand what an "account" is in modern cloud systems and how that user-facing construct relates to the underlying storage and processing infrastructure.

Hyperscale services like those Google provides operate through distributed infrastructure that is constantly changing. Achieving modern security,

reliability, maintenance, and speed requires flexibility. Accordingly, data and processing are spread across many servers, in different racks, different data centers, and often different regions and continents, so that capacity can expand or contract with demand, traffic can shift when network connections, power, or other hardware fail, and service can continue without interruption during maintenance. That same distribution also serves security and performance goals. Sharding – the technique of distributing data structures across a shared infrastructure – helps avoid computation, network, or storage bottlenecks, compartmentalizes data, limits damage when something goes wrong, and makes unauthorized access or corruption less able to affect the whole system. Local caching places frequently-needed data closer to the user to reduce latency.

In these complex hyperscale environments, online services do not manually organize or manage bits of stored data. Instead, they work through abstractions, using code, protocols, and algorithms to handle massive and complex logical data.

An account is an access-controlled user space scoped by the provider's identity and access control systems. The common ingredients are familiar even if provider-specific terminology differs: a recognized user, a method of authentication, a set of permissions that defines what that user may do, and system rules that determine whether a requested action is allowed. In some cases, service providers provision accounts directly to end users. In other cases, they provide cloud infrastructure to businesses and other organizations that themselves have

users.[9] Either way, to the individual user, the "account" is the relevant unit of personal space.

What turns those design elements into an actual security boundary is the account's stable identifier. That identifier is the reference point that allows the system to distinguish one account from another and to keep those accounts separate as the service operates at scale. To the user, this is why signing in consistently returns the same account, with the same stored information, as a distinct space associated with that user and not with everyone else.

---

9. The technical analysis that *amici* offer in this section is for an online service that maintains its own underlying technical infrastructure, as that was Google's practice for the systems relevant to this case. It is increasingly common for online services to build on top of other online services, such as "infrastructure as a service" (IaaS) virtual hardware providers or "platform as a service" (PaaS) database providers. These approaches allow smaller online services to benefit from hyperscale performance. Google, for example, offers Google Cloud IaaS and PaaS services to other online services. If an online service is a "tenant" of Google Cloud (i.e., built on top of Google Cloud services), it usually maintains its own user identifiers, authentication methods, and access controls. From the user's perspective, and from a technical design perspective, the user still has a logical "account" that is a virtual space. *See Identity Platform Multi-tenancy*, GOOGLE (Feb. 27, 2026), https://docs.cloud.google.com/identity-platform/docs/multi-tenancy. Thus, the account is still the relevant unit for Fourth Amendment analysis, and data in the account is not a "business record" of either the tenant or the underlying service provider. The ubiquity of user identity management offerings from IaaS and PaaS providers, such as Amazon Web Services, Microsoft Azure, and Google Cloud, reinforces how foundational user accounts are to modern online services.

The account boundary is then enforced through access-control machinery. After authentication, the provider's service layer evaluates whether the identified user may perform the requested action on the requested resource under the policies in force. That is how privilege separation is implemented in practice. Ordinary users receive access to the resources and functions associated with their own accounts. More privileged identities, such as administrators or support personnel acting on the provider's behalf, may be granted broader roles, but only through separately defined permissions. To the user, this appears as the ordinary expectation that only the account holder may take actions on the contents of the account unless someone acting through specially conferred privileges overrides that default.

C. Alternative abstractions based on physical infrastructure or categories of data are inaccurate and unnecessary.

The warrant in this case described the place of the search as Google's "computer servers" and the items to be seized as various categories of location- and account-related data. From a technical perspective, this description is both misleading and irrelevant. As a matter of how online services are designed, implemented, and used, the places to be searched are users' Google accounts and the items to be seized are the Location History information stored inside those accounts.

First, the warrant's reference to Google's "computer servers" identifies a technically irrelevant object. In a hyperscale environment, there is rarely a stable and prespecified collection of hardware that supports an online

service. Even if storage and processing functions are described using physical-world terms like "platform," and assigned names that sound tangible, like "sensorvault," those functions are actually logical constructs across shifting infrastructure. Such functions may be distributed, replicated, rebalanced, and reconstituted across regions as the system operates, and the same physical servers and storage may support many different functions at once.

It is similarly an error to conceptualize these account-bound data structures as a database table or a spreadsheet saved to a file on a hard drive. That model suggests a static, human-legible body of information sitting in one place. Hyperscale systems do not work that way. What is casually described as a "database" is a logical construct implemented across distributed storage layers, sharding, replication, caching, and failover mechanisms designed to preserve reliability, reduce latency, and maintain continuity of service when hardware fails or is taken offline for maintenance. Those dynamic features do not dissolve the account boundary. The account identifier remains the reference point that keeps one user's data distinct from another's and tells the system what information may be retrieved under what permissions. The underlying infrastructure may shift constantly, but the operative unit of access remains the account-defined user space.

At the same time, it is unnecessary, and ultimately distracting, to focus on the type of information stored in the account. Affixing labels such as "metadata" or "location data" to information does not, in the abstract, tell us what data structure is appropriate. To determine that, one must know the context in which the provider holds that information. Location information illustrates

the point nicely. In one context, as with carrier-maintained cell-site location information (CSLI), location information may take the form of provider-generated transactional records created incidentally to furnishing the service. *See Carpenter v. United States*, 585 U.S. 296, 301-03 (2018). But in Google's Location History service, location information is generated by users with their own devices and stored within non-public user accounts. *See* JA 43 (explaining that the Location History functionality requires both an active device and a Google account). It may be the exact same data, but it is considered a corporate record in one context and content in another. *See In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125, 137 (3d Cir. 2015) (explaining that "there is no general answer to the question of whether locational information is content").

The same is true elsewhere in cloud systems. If a customer uses a cloud provider's infrastructure to run its own email system, records generated within that customer's service, including access logs, may be content from the perspective of the underlying infrastructure provider. Context matters. To put it in more analogue terms, the address on the outside of an envelope is routing information. *See* WAYNE R. LAFAVE, ET AL., 2 CRIM. PROC. § 4.4(d) (3d ed.). The same address written in the body of the letter inside is content. *Id.* The label depends on function, placement, and the role the provider is playing. The context of information, whether it be location information or anything else, is essential to consider when making assertions about rights of the user. *See* Steven M. Bellovin et al., *It's Too Complicated: How the Internet Upends* Katz, Smith*, and Electronic Surveillance Law*, 30 HARV. J.L. & TECH. 1, 61 (2016) ("The content/non-content

distinction changes depending on where in the system you ask the question – or from which entity law enforcement seeks to compel the information.").

In summary, framing the compelled act as a search of "computer servers" or "databases" obscures what Google was actually required to do. Moreover, context-free assertions about the content of the accounts, like "individuals generally have no reasonable expectation of privacy in their movements through public spaces," do not make sense when applied to data held in cloud architecture. The analysis accordingly must proceed at the level of the account, not the equipment or the data.

D. Searching data in a system with accounts requires crossing the boundary into each account.

As illustrated above, indexing by account identifier is not discretionary bookkeeping. It is one of the basic ways a provider keeps one user's space separate from another's. It is what makes user-specific isolation possible at scale. The identifier ties requests, permissions, and stored data to the correct user space, allowing the system to retrieve the right information while excluding everyone else's. In that sense, account-binding is part of the security architecture itself, not a mere business preference about how to sort information. There is an important implication of this architecture: when a provider is required to look for evidence or contraband stored in an account, the provider is forced to exercise extraordinary privileged access to breach the boundaries and examine the content within.[10]

10. *Amici* do not take the position that if information is not bound to a user account, it cannot receive Fourth Amendment

From a systems engineering perspective, provider-generated records and subscriber-stored content are distinct categories of information, and through account implementation that distinction is built into the service architecture itself. The data structures used to maintain provider-generated records, such as billing information, communications routing data, and access logs, are subject to different design constraints because those records serve different functions. They are generated by the provider as an incident of operating the service and document the functioning of the system, the delivery of the service, and the provider's own administrative processes. The architecture accordingly treats them as provider-side operational records.

Subscriber content stored within an account is different. That material is housed within a user-specific, non-public account space that the system maintains for the subscriber. The code, protocols, and access controls that create the account structure reflect that distinction. They preserve a persistent user space for subscriber-held material, rather than treating that material as part of the provider's own system-wide recordkeeping. Characterizing user accounts as a business decision is no different from saying that the Hyatt made a business decision to offer separate hotel rooms rather than having guests sleep in the lobby together. A modern online service

---

protections. *Carpenter* illustrates that the Fourth Amendment can apply to provider-created and provider-held information held outside an account. *Amici* merely note that the Court need not reach that question here, because the provider stored the information within non-public user accounts, and that account-binding matters because it identifies the boundary the provider was required to cross to conduct the search.

cannot function without accounts separated by access controls, just like a hotel cannot function without rooms separated by walls.

That distinction is why Google's role with respect to Location History data in a Google account is not best described as that of a custodian of records holding its own corporate business records. With respect to Google account contents, Google is acting as a host and processor of customer-controlled material. While Google maintains the storage, processing, and access-controlled environment within which the account exists, the purpose of the account is to give the subscriber a non-public, persistent space in which information may be kept, accessed, and processed over time. Content stored in that account is not created "as an incident of providing the service" in the same way as the provider's own billing entries, routing logs, or authentication records.

That distinction is also why, when the government compelled Google to produce the requested information, it necessarily ordered Google to search through individual subscriber accounts.[11] This is, as a technical matter, fundamentally different from ordering Google to produce

11. The search in this case was limited to Location History information, which is stored in user accounts, and no other repository of location data. JA 49-50 ("[N]o [location] information other than [Location History] is stored and searchable in association with specific user accounts at a level of precision sufficient to be searched and produced in response to a geofence warrant."); JA 46-47 (explaining that Location History search "does not search or draw on [Web & App Activity] data in any way"); JA 47-48 (explaining that Google Location Accuracy "is not stored with user identifiers").

its own business records. Producing provider-generated logs involves retrieving records the provider created for its own operational purposes. Searching account contents requires the provider to enter user-bounded spaces and examine material stored within them. The fact that the provider has the technical means to do so does not make it the custodian of records for that content, any more than the fact that hotel staff can enter a room makes the hotel the custodian of the guest's luggage. *See* Part II.C. The provider's technical access exists because it built and operates the system. But using that access to examine account contents requires the provider to invoke heightened privileges sufficient to cross the account walls the system itself ordinarily enforces. In that respect, the compelled search is not the routine production of the provider's own business records, but the forced use of privileged access to enter protected account spaces and inspect subscriber-held content inside.

II. By grounding the ruling on the account nature of the intrusion, the Court can avoid unnecessary factual or doctrinal analysis.

Treating each account as a distinct place to be searched maintains technical fidelity and is judicially administrable. Once a court determines that the government compelled access to a non-public account, it can conclude, based solely on that, whether a search occurred. Under this approach, courts need not wrestle with hard factual questions about voluntariness, draw lines based on the sensitivity of data, or make sweeping characterizations about electronic searches generally. Moreover, the concept of individually controlled spaces within a larger infrastructure maps directly onto long-standing rules regarding multi-unit

physical properties. Thus, the account-oriented approach gives lower courts a rule that is administrable, precise, and familiar.

A. The Court can avoid several difficult, fact-bound questions.

Focusing on the moment of compelled intrusion into a user account obviates a host of difficult questions that have troubled lower courts. Using this approach, courts do not have to determine whether the data constitutes a "business record" and, if so, whether the individual's disclosure of data was "voluntary." Similarly, courts do not need to engage in a lengthy analysis of the sensitivity, precision, and amount of geolocation information at issue, as this Court had to in *Carpenter*, 585 U.S. at 310-13. Once a court establishes government-compelled entry into a non-public account, the analysis need not travel further down these thorny paths.

i. The Court does not need to address whether information in an account was voluntarily disclosed.

Using the account-based approach outlined above, the Court need not engage in a protracted inquiry into whether Location History subscribers in general, or the defendant in particular, voluntarily disclosed location data to Google. That is simply not a relevant question for an account-intrusion case. If an account enjoys Fourth Amendment protection, so do the contents of the account – regardless of how particular items arrived. By treating the government's compelled entry into an account as the relevant Fourth Amendment event, the Court can avoid

extended debates over voluntariness. *See United States v. Jones*, 565 U.S. 400, 418 (2012) (Sotomayor, J., concurring) (noting that Court could avoid "difficult questions" of voluntariness where a "physical intrusion . . . supplies a narrower basis for decision").

In *Carpenter*, this Court necessarily had to engage with the question of voluntariness. *See* 585 U.S. at 315-16. This was the required approach for a case that involved provider-created, provider-held location information stored outside of an account structure. However, the Court was frank that its decision was grounded in "the unique nature of cell phone location information." *Id.* at 315. This in turn required an in-depth analysis of both the pervasive nature of cell phones and the control, or lack thereof, that wireless subscribers have over the disclosure of CSLI. *See id.* (citing *Riley v. California*, 573 U.S. 373, 385 (2014)). Any discussion of voluntariness in the present case would require an equally fact-intensive and technical inquiry about smartphone location sensors and settings, the Location History feature's design and implementation, and Google's privacy representations and practices.

This Court could choose to conduct such an inquiry which, beyond its factual and technical complexity, should consider the evolving scientific understanding of consent in online privacy.[12]

---

12. *See generally* Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509 (2015) (summarizing dozens of behavioral studies on online privacy, which demonstrate that online privacy behaviors and choices are often explainable by lack of knowledge or understanding, default settings, user interface designs, and other contextual factors.

Or, this Court could rest its decision on the account-based nature of the search. For the reasons stated in Part I.D, *amici* submit that, in a case about account-based information, the latter is more appropriate. The lower court record in this case exemplifies the difficulty and ambiguity of a "voluntariness" inquiry, and it demonstrates how an account-based framework would be much easier to apply. *See United States v. Chatrie*, 590 F. Supp. 3d 901, 935 (E.D. Va. 2022), *aff'd*, 107 F.4th 319 (4th Cir. 2024), *aff'd on reh'g en banc*, 136 F.4th 100 (4th Cir. 2025) (explaining that "the Court simply cannot determine whether Chatrie 'voluntarily' agreed to disclose his Location History data based on this murky, indeterminate record").

ii. The Court does not need to conduct a *Carpenter*-style inquiry into the amount, precision, or sensitivity of information in an account.

The account-intrusion approach also obviates the need for the Court to undertake a freestanding inquiry into the sensitivity of the geolocation information involved. This approach does not require the Court to decide how precise the data was, how much time is enough to become constitutionally significant, or what exactly counts as "location data." Those are line-drawing problems that follow when the analysis turns on the revelatory power of the information itself.[13]

13. Assessing the sensitivity of data may benefit from technical analysis. The account-based approach that *amici* recommend would avoid the need for courts to extrapolate from technical analysis that may be highly nuanced, incomplete, or inconclusive, and it mitigates the risk that courts may arrive at conclusions unsupported by technical analysis. *Compare Chatrie*, 107 F. 4th at 324-25 (describing the Location History data produced by Google as "anonymized") *with* Yves-Alexandre

Such problems disappear with the account-based approach that *amici* recommend.

In *Carpenter*, the Court devoted significant discussion and debate to examining the amount, precision, and sensitivity of the collected CSLI. The Court, over several pages, concluded that the amount of data that law enforcement could access over the course of "127 days" was sufficient to constitute a Fourth Amendment violation. 585 U.S. at 312-313. The sensitivity of the data also was a significant topic of debate. *Compare id.* at 311-13 (describing CSLI as an "intimate window into a person's life") *with id.* at 336 (Kennedy, J., dissenting) (characterizing CSLI as less revealing than bank or phone records).

Many post-*Carpenter* cases involving non-content location tracking technologies similarly devoted substantial attention to the precision and amount of data involved. *See, e.g.*, *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 341-46 (4th Cir. 2021) (holding 45 days of aerial surveillance data likely violated Fourth Amendment); *United States v. Hood*, 920 F.3d 87, 91-92 (1st Cir. 2019) (declining to extend *Carpenter* to Internet Protocol (IP) addresses, in part because IP addresses do not reveal location); *United States v. Hasbajrami*, 945 F.3d 641, 671-72 (2d Cir. 2019) (distinguishing, for Fourth Amendment purposes, between targeted interception of emails and querying a "vast" email database). Indeed, lower courts in both the case at hand and its Fifth Circuit equivalent

---

de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3 Sci. Rep., no. 1376, 2013, at 2 (analyzing an "anonymized mobile phone dataset" and concluding that "mobility datasets are likely to be re-identifiable using information only on a few outside locations").

were largely concerned with how long and how precisely the Location History data at issue described Chatrie's movements. *See Chatrie*, 590 F. Supp. 3d at 908-09 (considering accuracy of Location History data); *Chatrie*, 107 F.4th at 330 (considering duration of information obtained by the government); *United States v. Smith*, 110 F.4th 817, 823-24 (5th Cir. 2024) (emphasizing both volume and quality of Location History data).

There is no need for such analysis when it comes to Location History and other data stored in user accounts. The relevant Fourth Amendment moment occurs at the point of government entry into an account to obtain information, just as there is a Fourth Amendment search when the government opens a letter or email to examine its contents, regardless of what is inside. *See United States v. Jacobsen*, 466 U.S. 109, 114 (1984); *Ex parte Jackson*, 96 U.S. 727, 733 (1877); *United States v. Warshak*, 631 F.3d 266, 285 (6th Cir. 2010); *United States v. Maher*, 120 F.4th 297, 307 (2d Cir. 2024). Courts in such cases do not need to examine the nature of the content, the sensitivity of the words written, or the number of pages in the envelope; it is protected by virtue of being within a sealed envelope. *Ex parte Jackson*, 96 U.S. at 733. Data in a non-public user account should be treated the same way: if the account is a constitutionally protected space, then the content is also protected by virtue of its placement therein.

iii. The Court does not need to address the constitutionality of other data searches.

The account framework likewise allows the Court to leave for another day questions about information stored outside an account context. The Court in *Carpenter* made

clear that users may retain Fourth Amendment protection in information a provider receives and processes even when that information is not stored within a user account. *See* 585 U.S. at 313-14. By using an account-focused framework, the Court can avoid deciding when to apply *Carpenter* to other forms of data, location or otherwise, stored outside a discrete user account.[14] Likewise, it need not determine the scope of constitutional protection for metadata, that is, information about servicing an account rather than inside an account. Just as *Kyllo v. United States* did not rule on the constitutionality of thermal imaging outside the home, 533 U.S. 27, 34-35 (2001), and *Florida v. Jardines* did not address the use of drug-sniffing dogs in other contexts, 569 U.S. 1, 10-11 (2013), the approach suggested here would avoid ruling broader than is necessary. This restraint fits with the Court's policy "to avoid unnecessary decisions of constitutional issues." *Mills v. Rogers*, 457 U.S. 291, 305 (1982).

B. The Court can avoid constitutionalizing Google's three-step process.

Acknowledging the technical reality of the account, the analysis can also proceed without reference to the three-step search policy that generated so much confusion in the lower courts. Instead, the analysis turns on the

14. In *Carpenter* the Court expressly declined to address whether government collection of CSLI in real time or as a "tower dump" would constitute a Fourth Amendment search. 585 U.S. at 316. Applying an account-centric approach would assist the Court in resolving this case similarly, without addressing the constitutional status of tower dumps or other CSLI investigative techniques, at least as cellular network technology is currently implemented.

nature of accounts themselves as non-public spaces within a larger infrastructure. This approach is entirely consistent with this Court's focus in other cases on the fact of an intrusion into a constitutionally protected interest.

Google followed a three-step compliance procedure as required in the warrant. *Chatrie*, 107 F.4th at 324. This process led to considerable disagreement on how to define the constitutional significance of those steps. In finding a search occurred, the district court treated the constitutionally significant event as the disclosure of "location information for *all* Google account owners who entered the geofence over the span of an hour." *Chatrie*, 590 F. Supp. 3d at 929 (emphasis in original). The panel majority disagreed, instead considering Chatrie's interest in "two hours' worth of [his] Location History data." *Chatrie*, 107 F.4th at 325. On rehearing, Judge Niemeyer focused on the geographic area, *Chatrie*, 136 F.4th at 113, Judge Wynn took issue with the "unbounded data requested by police at Step 2," *id.* at 122, and Judge Berner argued that only non-anonymous Location History information implicates the Fourth Amendment, *id.* at 144. Each of these characterizations led to different constitutional analyses.

This Court could, of course, resolve this confusion by adopting one of the myriad approaches articulated in the lower court opinions. However, this would elevate the three-step procedure into a source of Fourth Amendment doctrine. The three-step process reflects an attempt to minimize disclosure of data from user accounts. It is a court-sanctioned strategy for executing a warrant, not a cure for possible constitutional deficiencies. Data minimization procedures, however laudable, are not a

substitute for constitutional limits. *See Riley*, 573 U.S. at 398 ("[T]he Founders did not fight a revolution to gain the right to government agency [data minimization] protocols."). An account-centric view avoids this problem by focusing on a single Fourth Amendment event: the moment Google was compelled to enter a user account and examine its contents.

This approach, which focuses on the nature of the intrusion over the method of the search, finds support in this Court's jurisprudence. In *Kyllo*, the Court held that thermal imaging of a home constituted a search. 533 U.S. at 34-35. This result was not based on the technical nature of the search, *see id.* at 35-36 (declining to distinguish between "through-the-wall" and "off-the-wall" surveillance), or the sensitivity of the information obtained, *see id.* at 37-39 (declining to impose an "intimate details" requirement before finding a search occurred). Rather, it was grounded in the existence of an "intrusion into a constitutionally protected area." *Id.* at 34 (quoting *Silverman v. United States*, 365 U.S. 505, 512 (1961)). Similarly, in *Jardines* the Court held that the use of a drug-sniffing dog on the defendant's front porch was a search. 569 U.S. at 11-12. The constitutionally significant event was not the deployment of the dog or even the detection of the odor of marijuana; it was the intrusion into the curtilage of the home. *Id.* at 6-7. Grounding this case in the intrusion into an account would not require the creation of new Fourth Amendment doctrine.

C. The account-centered approach is analogous to searches of multi-unit properties such as hotels.

As described in Part I, user accounts have been part of everyday life for decades. As such, it is entirely possible to assess the constitutional interests in an account without reference to physical-world analogues. At the same time, *amici* recognize that analogies can be useful, especially when they have withstood the test of time. *See Computer Privacy, Hearings Before the Subcomm. on Admin. Prac. and Proc. of the Comm. on the Judiciary*, 90th Cong. 120 (1967) (statement of Dr. Emmanuel R. Piore, Vice President and Chief Scientist, IBM) (analogizing password-controlled account access to apartment lock and key). Accordingly, *amici* offer one such analogy: individual units in a multi-unit property, specifically hotels.[15]

Under this analogy, the system infrastructure is the hotel and the provider is the innkeeper. The account is the hotel room and the account holder is the guest. The stable account identifier is the room number that ties a particular space to that guest. The protocols and permissions that define and confine ordinary access are the walls of the

15. Another analogy consistent with the account-centric perspective is accounts-as-safe deposit boxes. *See*, *e.g.*, *United States v. Hill*, 705 F. Supp. 3d 811, 824-827 (E.D. Mich. 2023) (discussing application of the Fourth Amendment to safe deposit boxes). The account is the box, the account holder is the box owner, the account identifier is the box number, and the account access controls are the reinforced walls and door of the box. The bank assigns boxes and issues keys, and it may retain a key for its own access in exceptional circumstances, but the box owner decides what material to place inside.

room. The verification and credentialing processes are the closed door and the key that controls entry. The account access logs are the hotel registry and related business records. Finally, the contents of the account are the items brought by the guest or supplied by the hotel.

Analogizing to a hotel provides insights. As an initial matter, it confirms that distinct subdivisions of a common infrastructure are amenable to Fourth Amendment analysis. *See Hoffa v. United States*, 385 U.S. 293, 301 (1966) ("A hotel room can clearly be the object of Fourth Amendment protection as much as a home or an office."); *United States v. Nerber*, 222 F.3d 597, 600 n.2 (9th Cir. 2000) ("For Fourth Amendment purposes, a hotel room is treated essentially the same, if not exactly the same, as a home."). For the reasons described in Part I, an account is a logically distinct subdivision of computing infrastructure. The Court should apply established Fourth Amendment doctrine to determine whether it is the kind of subdivision in which a user has a Fourth Amendment interest.

Should the Court decide that accounts are protected under the Fourth Amendment, the hotel analogy provides a framework for further analysis. For example, it would suggest that a service provider's occasional entry into an account for its own purposes does not eliminate the user's privacy interest. *See Stoner v. California*, 376 U.S. 483, 489 (1964) (upholding Fourth Amendment rights in a rented hotel room despite permission for hotel employees to enter the room). It would also provide a starting point, if not a conclusion, for determining whether a search was reasonable. In *United States v. Winsor*, 816 F.2d 1394, 1395-96 (9th Cir. 1987), *rev'd on other grounds*, 846 F.2d

1569 (9th Cir. 1988), the court looked to several factors to determine whether a warrantless search of multiple hotel rooms was reasonable: the number of rooms searched, the likelihood of finding the suspect with the first door-knock, whether complying with the search was voluntary, the intrusiveness of the search, the threat of violence and the cost of delay, and whether the officers had probable cause to enter the room after finding the suspect inside. *Id*. at 1397-1400. Other courts have considered the constitutionality of multi-unit warrants. Compare *Jacobs v. City of Chicago*, 215 F.3d 758, 767 (7th Cir. 2000) (holding that "probable cause to search one apartment in a multi-unit building does not support a warrant authorizing a search of the entire building") with *United States v. Gilman*, 684 F.2d 616, 618 (9th Cir. 1982) (approving of whole-building warrants where officers are unaware that a building is a multi-unit structure, officers have probable cause to search each unit, or the target of the search has access to the entire structure).

CONCLUSION

For the reasons stated above, *amici* respectfully urge the Court to apply an account-based framework to the case at hand. Doing so aligns with the technical reality and user experience in modern computing systems and provides several substantial benefits to this Court and others that will inevitably face similar cases.

Respectfully submitted,

Christopher T. Bavitz
Counsel of Record
Mason A. Kortz
Michael Rosenbloom
Cyberlaw Clinic
Harvard Law School
1557 Massachusetts Avenue
Cambridge, MA 02138
(617) 384-9125
cbavitz@law.harvard.edu

Richard Salgado
1746 Fordham Way
Mountain View, CA 94040

Jonathan Mayer
Princeton University
307 Sherrerd Hall
Princeton, NJ 08540

March 9, 2026

Counsel for Amici Curiae