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 FOR NETCHOICE
AS AMICUS CURIAE SUPPORTING PETITIONER

PAUL TASKE
NETCHOICE
1401 K Street, N.W.
Suite 502
Washington, DC 20025
(202) 845-8817

ROBERT A. VAN KIRK
AMY MASON SAHARIA
CHARLES L. MCCLOUD
Counsel of Record
ATTICUS W. DEPROSPO
BRETT V. RIES
WILLIAMS & CONNOLLY LLP
680 Maine Avenue, S.W.
Washington, DC 20024
(202) 434-5000
lmccloud@wc.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases:

Constitution and Statute:

Other Authorities:

INTEREST OF *AMICUS CURIAE*[*]

Amicus NetChoice is a national trade association of leading e-commerce and online businesses. NetChoice members share the goals of promoting free expression and free enterprise online while ensuring their users' data is secure. NetChoice members also provide a diverse array of online services that depend on users trusting that their location data is secure when provided, including the Google Location History service at issue in this case. A list of NetChoice's members is included in Appendix A to this brief.

NetChoice has a significant interest in securing constitutional safeguards for users' location data because its members provide various online marketplaces and services that rely on users' trust to foster innovation and economic growth. NetChoice also believes that safeguarding fundamental property and privacy rights for users' location data is essential to facilitating a trustworthy Internet. Although individuals entrust NetChoice's members with their data, that should not mean that users automatically lose their Fourth Amendment privacy interests in that data. Stripping users' data of Fourth Amendment protections will chill free expression and free enterprise. A clear rule acknowledging the privacy interest in user data will also provide critical guidance to NetChoice's members in determining how they may respond, if at all, to government requests for user data.

---

[*] Pursuant to Rule 37.6, amicus affirms that no counsel for a party authored this brief in whole or in part and that no person other than amicus or their counsel have made any monetary contributions intended to fund the preparation or submission of this brief.

INTRODUCTION AND SUMMARY OF ARGUMENT

We live in a digital age. Emails and texts have replaced snail mail. Sentimental photographs once stored in shoeboxes and photo albums are now stored in the cloud. Sudden thoughts are jotted in a notes app, not on a notepad. Videos are recorded on Snapchat and TikTok instead of a camcorder. Documents once stuffed in a filing cabinet are now saved on Google Drive. Financial information historically tracked on a ledger is monitored with the JPMorganChase app. Millions of times each day, individuals are sharing and storing personal information online with NetChoice members.

Cell phones have been a key driver of these profound changes. For the nine in ten Americans who own a smartphone, Pet.App.64a, their phones and the services they provide have become such a "pervasive and insistent part of daily life" that they might be considered "an important feature of human anatomy," *Riley v. California*, 573 U.S. 373, 385 (2014). These hand-held devices allow individuals to "keep on their person a digital record of nearly every aspect of their lives." *Id.* at 395 (citation omitted). And quite a precise one. With user permission, Google can use Location History data to track user movements on average every two minutes, and in certain circumstances, down to a three-meter radius, or even across floors of a building. Pet.App.271a-272a, 274a. That history data can be used to generate a "detailed, encyclopedic, and effortlessly compiled" "comprehensive dossier of [one's] physical movements." *Carpenter v. United States*, 585 U.S. 296, 297, 315 (2018).

In the government's hands, this digital treasure trove of sensitive information can lead to exactly the kind of "arbitrary exercises of police power" that the Founders aimed to prevent. *United States v. Jones*, 565 U.S. 400,

416 (2012) (Sotomayor, J., concurring). For example, one state supreme court has already ruled that the government can execute reverse keyword warrants, which require online service providers to identify users who have done a particular search within a particular period, without running afoul of the Fourth Amendment, despite the breadth and depth of information such searches can reveal. Pet. 22. And, if individuals knew Big Brother was always watching, it would "chill[] associational and expressive freedoms." *Jones*, 565 U.S. at 416. "Only the few" who do not participate in the digital age could escape this "tireless and absolute surveillance." *Carpenter*, 585 U.S. at 312.

Fortunately, the Fourth Amendment is not silent about this "seismic shift[] in digital technology." *Id.* at 313. This Court has long been tasked with "ensur[ing] that the 'progress of science' does not erode Fourth Amendment protections." *Id.* at 320 (citation omitted). Otherwise, individuals are left "at the mercy of advancing technology." *Kyllo v. United States*, 533 U.S. 27, 35-36 (2001). Put simply, "a new balancing of law enforcement and privacy interests" is needed in light of this evolving digital landscape. *Riley*, 573 U.S. at 407 (Alito, J., concurring).

This Court need not look far for a solution. The answer is "already reflect[ed]" in this Court's property-based approach to the Fourth Amendment. *Carpenter*, 585 U.S. at 400 (Gorsuch, J., dissenting). Users' privacy interests in their location data stored with NetChoice members—a common practice in today's digital age—can easily be protected by common-law bailment principles. This Court has long recognized that when bailors entrust their property with bailees, they retain their Fourth Amendment property interests and the privacy interests

attached to that property. It should similarly hold that when individuals create a modern-day travel log of their movements and store it with an online service provider (here, Google), they have temporarily bailed their property, but they retain their property and privacy interests in that property. This fact—that a user retains control over their Location History data and the information contained therein—distinguishes this case from *Carpenter v. United States*, 585 U.S. 296 (2018), and this Court's previous third-party doctrine cases concerning government inspection of business records, in which customers had no property interest. *See generally United States v. Miller*, 425 U.S. 435 (1976); *Smith v. Maryland*, 442 U.S. 735 (1979).

To be clear, amicus agrees with petitioner that *Carpenter* dictates the conclusion that the government's collection of users' Location History data here was a search under the reasonable-expectation-of-privacy test established in *Katz v. United States*, 389 U.S. 347 (1967), should this Court apply that test. Pet. Br. 22-31. However, amicus urges this Court to adopt a property-based bailment approach as an *independent* basis for Fourth Amendment protection. Doing so would provide what *Katz* cannot: a stable, administrable rule grounded in traditional property concepts that would not shift based on the ever-evolving societal view of what constitutes a reasonable expectation. Lower courts could simply look at whether the individual retains the hallmarks of ownership over the location data held by an online service provider—*e.g.,* by reviewing the relevant user agreement or terms of service. Further, the *Katz* test "has never been the only way" to prove a Fourth Amendment interest, *Carpenter*, 585 U.S. at 405 (Gorsuch, J., dissenting), and *Katz* did not "narrow the Fourth Amendment's scope," *Jones*, 565 U.S. at 408.

By treating common-law bailment as an independent basis for establishing Fourth Amendment interests, this Court can avoid altogether the "two amorphous balancing tests" associated with the *Katz* test and its related third-party doctrine. *See Carpenter*, 585 U.S. at 397 (Gorsuch, J., dissenting).

ARGUMENT

Under a Property-Based Fourth Amendment Approach, Individuals Have a Protectable Privacy Interest in Their Location Data Property Stored with Online Service Providers.

A property-based approach that looks to the law of bailment is faithful to both the Fourth Amendment's text and original meaning. Its adoption would steer this Court's Fourth Amendment jurisprudence back to the "property-based concepts that have long grounded" this Court's search-and-seizure analysis. *Carpenter*, 585 U.S. at 322 (Kennedy, J., dissenting); *see also Jones*, 565 U.S. at 405. And just as importantly, users' personal data would be better protected. Bailment principles confirm that individuals do not lose their privacy interests just because the data is temporarily stored, with the user's permission, with an online service provider.

A. The Court Should Apply Property-Based Bailment Principles to the Fourth Amendment.

1. This Court has long recognized "the significance of property rights in search-and-seizure analysis," *Jones*, 565 U.S. at 405, and property-based concepts "have long grounded the analytic framework that pertains in these cases," *Carpenter*, 585 U.S. at 322 (Kennedy, J., dissenting). Bailments are one of those core concepts. "[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." *Id.*

at 399 (Gorsuch, J., dissenting) (quoting J. Story, *Commentaries on the Law of Bailments* § 2, p. 2 (1832)). The person receiving the item (the bailee) has a legal duty to protect and use the item "according to the terms of the parties' contract if they have one, and according to the 'implication[s] from their conduct' if they don't." *Id.* at 399 (quoting James L. Buchwalter, et al., *Bailment Contract as Governing Rights, Duties, and Liabilities of Parties*, 8 C.J.S. Bailments § 36, pp. 468-69 (2017)). Bailees are essentially custodians, who are responsible for the safety of items entrusted with them. If bailees fail to fulfill their legal duties, they are liable for conversion. *Id.* And more importantly for this case, it is clear that the owner of the property (the bailor) "retains a vital and protected legal interest" in that property during the bailment, including the privacy interests attached to the property. *Id.* at 400.

Bailment is not foreign to this Court's Fourth Amendment jurisprudence. For example, in *Ex Parte Jackson*, 96 U.S. 727 (1878), this Court held that sealed letters placed in the mail are "fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles." *Id.* at 733. It did not matter that the letters were given to a third party, this Court reasoned, because "[t]he constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, *wherever they may be*." *Id.* (emphasis added). An individual's private papers entrusted with another party for delivery receive the same Fourth Amendment protection as though those papers were "subjected to search in one's own household." *Id.* at 732.

More recently, in *United States v. Jones*, 565 U.S. 400 (2012), this Court recognized that bailment can play a role in property-based Fourth Amendment analysis. *Id.* at 404 n.2. There, this Court discussed how the car involved in the search was not registered in Jones' name, but "he had at least the property rights of a bailee," and thus had a property and privacy interest in the car being tracked. *Id.*; *see also id.* at 425 (Alito, J., concurring) (discussing bailment). Additionally, in *Carpenter*, the dissenting opinions discussed bailment but ultimately concluded the argument was not preserved and the facts did not support a bailor-bailee relationship. *Carpenter*, 585 U.S. at 329 (Kennedy, J., dissenting) (arguing that the third parties holding the CSLI data "were not bailees"); *id.* at 383 n.6 (Alito, J., dissenting) (stating that the facts of the case do not support that a bailment is involved); *id.* at 406 (Gorsuch, J., dissenting) (recognizing that the petitioner forfeited a property-based bailment argument).

2. Applying property-based bailment principles to the Fourth Amendment is not just consistent with precedent. It is also well supported by the text and aligns with the Amendment's original meaning.

a. The Fourth Amendment states that individuals are protected against "unreasonable searches and seizures" of "their persons, houses, papers, and effects" by the government. That wording reflects the Amendment's "close connection to property," *Jones*, 565 U.S. at 405, and indicates that, at a minimum, the Amendment protects those "particular places and things," *Carpenter*, 585 U.S. at 392 (Gorsuch, J., dissenting).

Location data stored with online service providers, like the Location History data at issue here, falls under the text's purview. Because the collected and stored location data is essentially a travel journal or travel log, it is

the "modern-day equivalent[] of an individual's own 'papers' or 'effects.'" *Carpenter*, 585 U.S. at 332 (Kennedy, J., dissenting); *see also id.* at 405 (Gorsuch, J., dissenting). This is true "even when those papers or effects are held by a third party," *id.* at 332 (Kennedy, J., dissenting), because, under bailment principles, those papers and effects remain one's property.

Also instructive is the Amendment's use of the word "their" to qualify whose property is protected. *Carpenter*, 585 U.S. at 352-53 (Thomas, J., dissenting); *id.* at 362 (Alito, J., dissenting); *id.* at 391 (Gorsuch, J., dissenting). Asking "if a house, paper, or effect [is] *yours* under law," is a simple question to answer—or at least easier than trying to gauge ever-changing societal expectations in the digital age. *Id.* at 397-98 (Gorsuch, J., dissenting). And in a bailment, it is clear that individuals who bail their property to online service providers do not lose their property interests in that property—it is still "theirs." Although bailors temporarily entrust their property with bailees, bailees do not take ownership over the property. *Id.* at 399.

b. This Court has emphasized the importance of preserving the Fourth Amendment's "original meaning" and furthering its "basic purpose[s]" when analyzing whether a "search" has occurred. *Kyllo v. United States*, 533 U.S. 27, 40 (2001); *Carpenter*, 585 U.S. at 303, 305. The Amendment must be "construed in light of what was deemed an unreasonable search and seizure when it was adopted." *Kyllo*, 533 U.S. at 40 (citation omitted). And it is this Court's role to "assure[] preservation of that degree of privacy," especially "as technology enhance[s] the Government's capacity to encroach upon areas normally guarded from inquisitive eyes." *Carpenter*, 585 U.S. at 305 (citing *Kyllo*, 533 U.S. at 34).

This Court has been clear that the "basic purpose" of the Fourth Amendment "is to safeguard the privacy and security of individuals against arbitrary invasions by government officials." *Id.* at 303 (citation omitted). The Amendment "was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era" that allowed government officials "to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley v. California*, 573 U.S. 373, 403 (2014); *see also Carpenter*, 585 U.S. at 303 (citation omitted). Indeed, "[o]pposition to such searches" was "one of the driving forces behind the Revolution itself." *Riley*, 573 U.S. at 403. Accordingly, the Amendment aims "to secure 'the privacies of life' against 'arbitrary power,'" and "to place obstacles in the way of a too permeating police surveillance." *Carpenter*, 585 U.S. at 305 (citations omitted).

In its commitment to promoting these goals, this Court for decades has protected individuals from the government's use of "sense-enhancing technology" to obtain information "otherwise unknowable." *Kyllo*, 533 U.S. at 34; *Carpenter*, 585 U.S. at 312. Otherwise, it would leave individuals and their privacy "at the mercy of advancing technology." *Kyllo*, 533 U.S. at 35; *Carpenter*, 585 U.S. at 305 (citation omitted). It is also why this Court has "take[n] account of more sophisticated systems that are already in use or in development" when adopting a new rule. *Kyllo*, 533 U.S. at 36; *Carpenter*, 585 U.S. at 313. Only then can this Court "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo*, 533 U.S. at 34. Applying property-based bailment principles to the Fourth Amendment best fulfills these ideals.

B. Bailment Principles Confirm that the Fourth Amendment Protects Individuals' Property Rights in their Location Data.

Similar to a letter trusted with the postal service, individuals' location data created and stored with NetChoice members and other online service providers should be constitutionally protected from examination and inspection under bailment principles. Collected location data is the modern-day equivalent to a travel log, such that it is an individual's property. Temporarily entrusting property digitally with an online service provider does not strip individuals of their property or privacy interests in that property. *Carpenter*, 585 U.S. at 399 (Gorsuch, J., dissenting). The policies, practices, and terms of service of companies such as Google, Lyft, and Airbnb often confirm that users—not the companies—retain ultimate authority over the creation, modification, and removal of user location data. That degree of user control sets this type of data apart from the business records at issue in this Court's prior Fourth Amendment cases where individuals had no comparable ownership or property interest. Moreover, the far greater precision of this location data amplifies the magnitude of the property and privacy interests at stake here, further warranting robust Fourth Amendment protection.

1. Online service providers, like NetChoice members Google or Amazon, offer a variety of online services, including location history services and AI-driven interactions (*e.g.*, Google Assistant or Alexa). These services allow users to create, edit, and save records of their location over time with an online service provider, much like a person writing and keeping entries in a travel log. For example, Airbnb provides location history services to users by storing, displaying, and sharing their past reservations by

city, country, and date. Lyft similarly offers comprehensive location and ride history services by providing users with detailed records of past trips, including mapping of pickup locations and drop-off locations. Relevant here, Google offers a Location History service that allows users to create and save records of their locations. In each scenario, users entrust their private data with online service providers and expect those providers to protect the data.

Users also often have property rights to their location data. For instance, as Google explains, Location History data is "created, edited, and stored by and for the benefit of Google users who opt into the service and choose to communicate their location information to Google for storage and processing." J.A.12. In fact, Google describes its users' Location History data as a "*history or journal* that Google users can choose to create, edit, and store to record their movements and travels." J.A.16 (emphasis added). Google does not, for its own purposes, "save information about where a particular mobile device has been to a user's account—even when the device-location feature is turned on and applications on the device are using location data." J.A.18.

Rather, users must take "additional specific steps" before Google begins to save their Location History data. *Id.* If users take those steps, their Location History data "is communicated to Google for processing and storage on Google's cloud-based servers." *Id.* But in Google's own words, "it is the user who controls" the Location History data. J.A.19. "The user can *review, edit, or delete"* their location data "from Google's servers at will." *Id.* (emphasis added). Google only stores a user's Location History data "in accordance with the user's decisions (*e.g.*, to opt in or out, or to save, edit, or delete the information)." J.A.20.

Google also makes clear that while "the contents of [a user's] journal are reflected on a map in one's Google account rather than in a written document, the locations and travels recorded therein are fundamentally the contents of the journal, capable of being reviewed, edited, and deleted by the user." J.A.29. Further, "Google's privacy policy consistently refers to user data (including Location History) as 'your information,' which can be managed, exported, and even deleted from Google's servers at 'your' request." Pet. 31-32 (citing 4th Cir. J.A. 39); *see* Pet. Br. 21 (collecting other examples). In the end, it is the users—not Google—who control, edit, and delete their data, and even Google itself views Location History data as the user's property.[1]

2. Users' ability to control and delete their location data distinguishes that data from the business records at issue in many of the prior Fourth Amendment decisions relied on by the government. *See United States v. Miller*,

---

[1] To be clear, user agreements do not create free-floating property or privacy interests, but to the extent they do identify such interests in particular data, that should be sufficient for Fourth Amendment purposes under the bailment principles discussed here. Further, user agreements are just one example of how individuals *may* obtain property and privacy interests in their data. As another example, Congress can (and does) grant individuals property and privacy interests in their data via statute. *See*, *e.g.*, *Other Digital Content* (Copyright.gov), https://www.copyright.gov/registration/other-digital-content; Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, § 264, 110 Stat 1936, 2033. What matters is that the individual has a property interest in the data, regardless of the source. *See* Laura K. Donohue, *Functional Equivalence and Residual Rights Post-Carpenter: Framing a Test Consistent with Precedent and Original Meaning*, 2018 Sup. Ct. Rev. 347, 389-91 (2018) (identifying sources that provide individuals with "ownership interest in *digital* documents or records"); Pet. Br. 17-19 (collecting examples).

425 U.S. 435, 440 (1976); *Smith v. Maryland*, 442 U.S. 735, 742-43 (1979); *Carpenter*, 585 U.S. at 300-01. Unlike users of Google's Location History service, none of the individuals in the government's cited cases personally owned or had property interests in the personal information at issue in those cases.

Miller. The government investigated Miller for tax evasion by subpoenaing his bank for records of his canceled checks, deposit slips, and monthly statements. *Miller*, 425 U.S. at 437-38. The Court noted that Miller could not assert "ownership nor possession" of the documents because they were "business records of the banks." *Id.* at 440.

Smith. This case concerned a pen register, a device that records the outgoing phone numbers a customer dials on a landline. *Smith*, 442 U.S. at 736 n.1, 737-38. The Court held that the records from the pen register constituted the business records of the telephone company, in which the customer had no property or privacy interest. *See id.* at 742-45.

Carpenter. There, the business records at issue were cell service location information ("CSLI"), which were just time-stamped records automatically generated by and for the wireless carrier whenever a cell phone connected to a cell site. *Carpenter*, 585 U.S. at 300-01. Carpenter, the individual asserting that these records were protected under the Fourth Amendment, "did not create the records, he d[id] not maintain them, he [could not] control them, and he [could not] destroy them." *Id.* at 342 (Thomas, J., dissenting).

Another important distinction between the type of location data at issue here and the CSLI in *Carpenter* is that the former is much more precise and unique to a specific

individual than the latter. The location information at issue here would allow the government to know where a person is within meters, including travel between or within buildings. Pet.App.271a-272a. As an example, with the click of a button the government could retroactively know how you spent two hours at home on August 14, 2025: one hour inside the house, thirty minutes outside in your fenced-in backyard, and then thirty minutes in your detached garage. And it could obtain that information, with no judicial oversight, even though the home is a place where "*all* details are intimate details" and where you are supposed to be "safe from prying government eyes." *Kyllo*, 533 U.S. at 37.

A property-based bailment approach would prevent this obvious invasion of privacy. It would recognize that "[c]onsenting to give a third party access to private papers that remain [one's] property is not the same thing as consenting to a *search of those papers by the government*." *Carpenter*, 585 U.S. at 390 (Gorsuch, J., dissenting). And it would be consistent with the societal expectation that "law enforcement agents and others would not—and, indeed, in the main, simply could not—secretly monitor and catalogue every single movement" individuals make with their cell phones. *United States v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J., concurring); *see also Carpenter*, 585 U.S. at 310. Few, if any, believe that law enforcement has the resources to physically track every location and everyone in or near it 24/7, let alone do it retrospectively or in one's home. Yet that is precisely what the government's overbroad application of the third-party doctrine in this case would allow. A geofence warrant, like the one in this case, would permit law enforcement to obtain the identities of several online service providers' users who were in a particular location at a particular time.

Law enforcement, however, "need not even know in advance whether they want to follow a particular individual, or when." *Carpenter*, 585 U.S. at 312. That is the type of arbitrary government surveillance "the Framers, 'after consulting the lessons of history,' drafted the Fourth Amendment to prevent." *Id.* at 320 (citation omitted).

CONCLUSION

Society has become highly digitized. Cell phones, in particular, are no longer merely a "technological convenience." *Riley v. California*, 573 U.S. 373, 403 (2014). Personal information that was once created and stored on tangible objects is now created and stored with NetChoice members and the other online service providers who facilitate user participation in the digital age. But that digitization does not "make the information any less worthy of the protection for which the Founders fought." *Id.* This Court's Fourth Amendment jurisprudence should acknowledge that reality, and a property-based bailment approach is the most principled way to do so here.

Respectfully submitted,

PAUL TASKE
NETCHOICE
1401 K Street, N.W.
Suite 502
Washington, DC 20025
(202) 845-8817

ROBERT A. VAN KIRK
AMY MASON SAHARIA
CHARLES L. MCCLOUD
Counsel of Record
ATTICUS W. DEPROSPO
BRETT V. RIES
WILLIAMS & CONNOLLY LLP
680 Maine Avenue, S.W.
Washington, DC 20024
(202) 434-5000
lmccloud@wc.com

Counsel for Amicus Curiae NetChoice

MARCH 2, 2026

APPENDIX A

NetChoice Association Members	
• Airbnb, Inc. • Amazon.com, Inc. • Automattic Inc. • Discord Inc. • Dreamwidth Studios • Duolingo, Inc. • EarnIn • eBay Inc. • Etsy, Inc. • Google LLC • Hims & Hers Health, Inc. • JPMorganChase & Co. • Lyft, Inc. • Meta Platforms, Inc. • Netflix, Inc.	• Nextdoor Holdings, Inc. • OfferUp, Inc. • OpenAI • PayPal Holdings, Inc. • Pindrop Security • Pinterest, Inc. • Reddit • StubHub, Inc. • Snap Inc. • Swimply • TikTok • Turo Inc. • Travel Tech • Waymo LLC • Wing • X Corp. • YouTube