No. 24-922

In the Supreme Court of the United States

JAMES HARPER, *Petitioner,*

v.

DOUGLAS O'DONNELL, ACTING COMMISSIONER OF INTERNAL REVENUE SERVICE, ET AL.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the First Circuit

BRIEF OF PROJECT FOR PRIVACY & SURVEILLANCE ACCOUNTABILITY AS *AMICUS CURIAE* SUPPORTING PETITIONER

GENE C. SCHAERR
Counsel of Record
ERIK S. JAFFE
AARON C. WARD
SCHAERR | JAFFE LLP
1717 K Street, NW, Suite 900
Washington, DC 20006
(202) 787-1060
gschaerr@schaerr-jaffe.com

Counsel for Amicus Curiae

APRIL 30, 2025

QUESTION PRESENTED

Did the First Circuit improperly extend the third-party doctrine to allow the warrantless search of customer-owned data subject to contractual guarantees of privacy and reasonable and actual customer expectations of privacy?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

INTRODUCTION, SUMMARY, AND INTERESTS OF *AMICUS CURIAE*[1]

This case presents an important, recurring issue about the extent to which the Fourth Amendment protects personal data stored on a third party's server—an arrangement necessary to function in modern society. Although this Court rebuked excessively broad interpretations of the third-party doctrine in this very context in *Carpenter* v. *United States,* 585 U.S. 296, 305, 316 (2018), lower courts—including the First Circuit—continue to treat *Carpenter* as the exception rather than the rule. This Court should grant certiorari to clarify the core rule that customer data stored with third parties still carries a reasonable expectation of privacy and remains protected by the Fourth Amendment.

Carpenter correctly recognized that the Fourth Amendment protects privacy interests that would have been recognized as reasonable at the Founding. Such expectations set the baseline for measuring modern encroachments on privacy, notwithstanding advances in technology that make it easier to invade people's privacy. Under such baseline expectations of privacy, merely storing property or information with third parties, under contractual assurances of the privacy and security of such information or property,

---

[1] This brief was not authored in whole or in part by counsel for any party and no person or entity other than *amicus curiae* or its counsel has made a monetary contribution to the brief's preparation or submission. Counsel of record for all parties received timely notice of the intent of *amicus curiae* to file this brief.

does not vitiate reasonable expectations of privacy, particularly as against the government.

The First Circuit ignored that basic principle and this Court's guidance, treating limited-purpose disclosure to and storage by a third party—here the cryptocurrency exchange Coinbase—as sufficient to destroy any expectation of privacy that Petitioner James Harper had in the Coinbase account that stored his Bitcoin. That decision was wrong and dangerous, and it should not be allowed to stand.

Moreover, proper resolution of whether people like Petitioner have an expectation of privacy in their digital data is of paramount importance to *Amicus* Project for Privacy & Surveillance Accountability, a nonprofit, nonpartisan organization concerned about a range of privacy and surveillance issues—from the surveillance of American citizens under the guise of foreign-intelligence gathering, to the monitoring of domestic activities under the guise of law enforcement.

Amicus agrees with Petitioner (at 12-19) that the third-party doctrine needed a facelift for the digital age. But this Court gave it one in *Carpenter*. The First Circuit's erroneous application of *Carpenter* has led courts to abandon all semblance of Founding Era privacy and conclude that Americans have no Fourth Amendment protections against a host of intrusive surveillance practices, from seizure of medical records to intrusive geofence warrants. That conclusion and similar holdings will continue to drastically undermine Americans' privacy as third-party storage becomes increasingly common and inescapable.

Amicus writes separately to emphasize that, as *Carpenter* clarified, Fourth Amendment protections

are not categorically lost when a person shares or stores her data with a third party while maintaining reasonable expectations and assurances of privacy. The Court should grant review to prevent a contrary understanding of *Carpenter* from continuing to erode Americans' privacy as third-party storage becomes ubiquitous and artificial intelligence becomes powerful enough to piece together intimate information from seemingly innocuous details about a target's life.

STATEMENT

Petitioner James Harper opened a Coinbase account to store and use Bitcoin, a pseudonymous cryptocurrency. Pet.4; App.4a. Under Coinbase's privacy policy, Harper had a reasonable expectation of privacy regarding his financial records, which remained his property, and Coinbase promised not to disclose such information absent Harper's consent or unless required by valid legal process. Pet.4-5; App.53a. Harper later transferred his Bitcoin holdings from Coinbase to a hardware wallet—a storage device similar to a thumb drive. He properly reported all required information to the Internal Revenue Service (IRS). App.4a n.1.

Harper later was caught up in an IRS fishing expedition from a John Doe summons to Coinbase that sought information on *all* Coinbase users (later slightly narrowed to all users having above a specified level of financial transactions). App.6a. The IRS had no probable cause or warrant for such a dragnet search of private financial records.

Based on the results of that dragnet, the IRS then demanded further information from Harper himself, again without a warrant and unconstrained by

probable cause. App.5a, App.58a. Harper sued the IRS challenging the search and seizure of his private records. App.8a-9a.

Eventually, Harper's claims were dismissed, App.8a-11a, and the First Circuit affirmed, holding that Harper had no reasonable expectation of privacy in his Coinbase account information because he had turned over that information to Coinbase, a third party, App.18a-20a.

ADDITIONAL REASONS TO GRANT REVIEW

I. This Court Should Correct the First Circuit's Misinterpretation of the Post-*Carpenter* Third-Party Doctrine.

The First Circuit's decision contravenes this Court's repeated holdings that the Fourth Amendment protects "that degree of privacy against government that existed when [it] was adopted." *Carpenter* v. *United States*, 585 U.S. 296, 305 (2018) (quoting *Kyllo* v. *United States*, 533 U.S. 27, 34 (2001)). This is true in the context of the third-party doctrine as well, and this Court should grant review to correct erroneous interpretations by lower courts which ignore this overarching constitutional principle.

A. The Fourth Amendment reasonableness inquiry is historically grounded and accounts for advances in technology.

A Fourth Amendment search occurs when the government gets access to information or items over which a person has a subjective and reasonable expectation of privacy. See *Katz* v. *United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Reasonableness, moreover, is "the ultimate touchstone

of the Fourth Amendment," *Brigham City* v. *Stuart*, 547 U.S. 398, 403 (2006).

The reasonableness inquiry, however, is not an "open-ended balancing test[.]" *Crawford* v. *Washington*, 541 U.S. 36, 67-68 (2004). When evaluating a person's expectations of privacy, a judge cannot "make difficult empirical judgments about the costs and benefits of [privacy] restrictions." *New York State Rifle & Pistol Ass'n, Inc.* v. *Bruen*, 597 U.S. 1, 25 (2022) (cleaned up). The Fourth Amendment, like other enumerated rights, is not "subjected to [such] a freestanding 'interest-balancing' approach." *District of Columbia* v. *Heller*, 554 U.S. 570, 634 (2008).

Rather, compliance with the Fourth Amendment "is measured in objective terms," *Ohio* v. *Robinette*, 519 U.S. 33, 39 (1996), and, as with other constitutional rights, is governed by the "historically fixed meaning" of a given right as "applie[d] to new circumstances," *Bruen*, 597 U.S. at 28. The Fourth Amendment thus protects "that degree of privacy against government that existed when the Fourth Amendment was adopted," *Carpenter*, 585 U.S. at 305 (citation omitted), while applying that standard to new technology, *id.* at 313.

B. *Carpenter* clarifies that contractually limited access to customer data by a third party does not automatically eliminate reasonable customer expectations of privacy or Fourth Amendment protections.

In addressing this historically grounded inquiry into reasonable expectations of privacy, *Carpenter* clarified that disclosure to a third party does not

automatically vitiate such expectations or the accompanying Fourth Amendment protections. 585 U.S. at 314. And, while the Court recognized that disclosing data to a third party can sometimes *diminish* an expectation of privacy over that data, even then the Court rejected any suggestion that "the fact of diminished privacy interests" meant that "the Fourth Amendment falls out of the picture entirely." *Ibid.* (cleaned up). Such obvious limits on using the third-party doctrine seem especially apt here, where the "disclosure" and storage of data with a third party was accompanied by specific contractual guarantees of ownership of and privacy regarding such data.

Carpenter also clarified that earlier third-party doctrine cases treated disclosure as a relevant—though by no means dispositive—factor in the privacy inquiry. See *Ibid.* (discussing *Smith* v. *Maryland*, 442 U.S. 735 (1979); then discussing *United States* v. *Miller*, 425 U.S. 435 (1976)). The Court then emphasized that it was not "disturb[ing] the application of" those cases, *id.* at 315, and—like the Court did in *Smith* and *Miller*—rejected "mechanically applying" the third-party doctrine, *id.* at 314.

C. Lower courts continue to misconstrue *Carpenter* by limiting it to its facts.

Despite *Carpenter*'s clear warning against allowing the third-party doctrine to degrade privacy via a "mechanical interpretation of the Fourth Amendment," 585 U.S. at 305 (cleaned up), lower courts have generally failed to heed that warning. Rather, they mechanically first ask if the information was disclosed to a third party and then treat this disclosure as a complete carveout from Fourth

Amendment protections unless the circumstances closely or identically match *Carpenter*'s narrow facts. The First Circuit followed this erroneous approach below, functionally limiting *Carpenter* to its facts.

The First Circuit began with a sweeping statement that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." App.49a (quoting *Smith*, 442 U.S. at 743-744); accord App.13a-14a (finding no expectation of privacy since Coinbase made clear that disclosure to law enforcement was *possible*). But *Carpenter* considered *Smith*'s statement dicta since *Smith* did not turn solely on the act of sharing. 585 U.S. at 314. The First Circuit then found enough factual differences with *Carpenter*—including the lack of automatic disclosure and the fact that the court considered the data insufficiently "intimate"—to conclude there was no reasonable expectation of privacy, with no further analysis. App.49a-53a.

Unfortunately, the First Circuit is not alone in applying this erroneous approach. For instance, the Seventh Circuit found there was no expectation of privacy in the same type of data at issue in *Carpenter* when used to track a person in real-time, because the tracking was not of long enough duration or retrospective. *United States* v. *Hammond*, 996 F.3d 374, 389-390 (7th Cir. 2021). Similarly, the Eleventh Circuit justified a geofence warrant, finding no expectation of privacy in cell-site location information that fell short of "near perfect surveillance." *United States* v. *Davis*, 109 F.4th 1320, 1330 (11th Cir. 2024). For its part, the Fifth Circuit, in ruling that geofence warrants are a Fourth Amendment search, reached

this result only after concluding the search was no more than "slightly distinguishable from *Carpenter*." *United States* v. *Smith*, 110 F.4th 817, 835 (5th Cir. 2024). And the Ninth Circuit found no expectation of privacy in location data from a rented electronic scooter because it was not "indispensable" as a means of short-term travel—without even considering whether other untracked methods of transportation were available. *Sanchez* v. *Los Angeles Dep't of Transp.,* 39 F.4th 548, 560 (9th Cir. 2022).

Notably absent from this widespread approach is any analysis of the central Fourth Amendment question: Whether a search of a person's personal data would be "deemed an unreasonable search and seizure when the Fourth Amendment was adopted." *Carpenter,* 585 U.S. at 305 (cleaned up). And it is difficult to square a categorical carveout from Fourth Amendment coverage with the fact that items, including personal papers and books, were commonly entrusted to third parties in bailments at the time of the Founding, as explored more deeply in Professor Adam J. MacLeod's *Amicus Curiae* Brief in Support of Petitioner; see also *Carpenter*, 585 U.S. at 399 (Gorsuch, J., dissenting).

This Court should reverse the decision below and clarify that *Carpenter* protects the degree of privacy that existed at the Founding, taking into account advances in technology and modern practices that often necessitate that data be held by a third party for limited purposes.

II. A Narrow Interpretation of *Carpenter* and a Broad Application of the Third-Party Doctrine Are Unworkable Given Modern Computing and Storage Technology and Would Shrink Privacy Well Below Founding Era Expectations.

This Court should also grant review to ensure that these Founding Era protections are not left "at the mercy of advancing technology." *Carpenter*, 585 U.S. at 305 (citation omitted). This Court has long recognized that, for the Fourth Amendment to mean anything, it "must take account of more sophisticated systems that are already in use or in development." *Kyllo*, 533 U.S. at 36. But a third-party doctrine that ignores the prolific rise in third-party data hosting and artificial intelligence would leave Fourth Amendment protections wholly "at the mercy of advancing technology"—exactly what the *Carpenter* Court feared.

A. Storage of information with third parties is necessary for modern life.

One "sophisticated system" that the Fourth Amendment must address to have any contemporary relevance is the rise of data storage.

The United States has gone from approximately 2,600 data centers in 2021 to over 5,300 in 2024.[2] But even this doubling of such centers in only a few years likely understates the trend: Each data center might

[2] Compare U.S. Int'l Trade Comm'n, *Data Centers Around The World: A Quick Look* 1 (May 2021), https://tinyurl.com/yya8apmr, with CloudScene, *Market Profile: United States of America* (2024), https://tinyurl.com/4nzy55jy.

be used by multiple hosts, and those hosts might, in turn, use overseas data centers.

This pervasive reliance on data storage is not merely a luxury. It is a necessity in modern life with no viable alternatives.[3] And increasingly, even data from normal personal computer use is stored on cloud systems such as OneDrive, Dropbox, or Google Drive. Indeed, recent surveys have found a remarkable 90% of enterprises and 70% of individuals use cloud services for data storage.[4] Moreover, this storage is often performed unknowingly or involuntarily, and a device user "may not know whether particular information is stored on the device or in the cloud." *Riley* v. *California*, 573 U.S. 373, 397 (2014).

This near-universal shift to cloud storage, encompassing virtually all data, demands translation forward of Founding Era privacy expectations to prevent the erosion of Fourth Amendment guarantees in the digital age. This is not a speculative threat, as courts have already used overly broad interpretations of the third-party doctrine to justify warrantless use of

---

[3] See Steven Arango, *Cloudy with a Chance of Government Intrusion: The Third-Party Doctrine in the 21st Century*, 69 Cath. U.L. Rev. 723, 733 (2020) ("alternatives to cloud storage do not eliminate the cloud's essentialness").

[4] Mariusz Michalowski, *55 Cloud Computing Statistics for 2025*, Spacelift (Jan. 1, 2025) (finding over 90% of businesses use at least some form of cloud storage), https://tinyurl.com/52w6s8kd; Martin Armstrong, *What's in the Cloud?*, Statista (Sept. 30, 2021) (finding over 70% of Americans use cloud computing), https://tinyurl.com/56p99zet; see also Darla Wynon Kite-Jackson, *2024 Cloud Computing TechReport,* Am. Bar Ass'n (Apr. 24, 2025) (finding 75% adoption among attorneys), https://tinyurl.com/27v8rchy.

sensitive data. Indeed, one man was charged with murder based on a dubious interpretation of data obtained from a warrantless seizure of data from his smart water meter[5]—only to be exonerated when audio data from his Amazon Echo proved inconclusive.[6] Although some of the online data in that case ultimately proved helpful to the accused, not all such data will. And if 70% of individuals truly have no protections in the data they store online, whether in traditional cloud storage or in recordings uploaded from an ever-listening smart speaker, then the Fourth Amendment is well on its way to becoming a mere parchment guarantee.

B. The increasing power of artificial intelligence makes an overly broad third-party doctrine an extraordinary threat to privacy.

Cabining *Carpenter* too closely to its facts also incentivizes a "divide and conquer" approach that allows advancing technology to erode the overall societal level of privacy. Even with normal human

---

[5] Police obtained the meter data from the utility provider's billing department and concluded that the suspect's water usage was unusually high, and he was likely cleaning up evidence of a murder. Aff. of Probable Cause to Obtain Search Warrant at 6-7, *Arkansas* v. *Bates*, No. CR-2016-370-2 (Ark. Cir. Ct., Benton Cnty. Feb. 22, 2016), available at https://tinyurl.com/3jp3p6hv. But the suspect claimed that the meter updated in irregular intervals and consolidated the water usage from his filling his hot tub earlier in the day into a single late-night report. See Sara Jerome, *Smart Water Meter Data Considered Evidence in Murder Case,* Water Online (Jan. 3, 2017), https://tinyurl.com/2rrn5jez.

[6] Nicole Chavez, *Arkansas judge drops murder charge in Amazon Echo case*, CNN (Dec. 2, 2017), https://tinyurl.com/4sjpddfv.

analysis, numerous forms of data stored with third parties, when aggregated, can be used to "generate[] a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *United States* v. *Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

For instance, cryptocurrencies are increasingly used to facilitate private activities such as donating to controversial political causes, linking cryptocurrency account information to commonly used, yet voluntarily disclosed, information.[7] And Internet Protocol (IP) headers—information broadcast to public networks every time a computer loads a new webpage—are currently not protected under most interpretations of the third-party doctrine. Yet combining these headers with Coinbase account information could be used to identify, and target, financial supporters of websites hosting unpopular speech—making this new technology a First Amendment threat too. See, *e.g.*, *Stanford* v. *Texas*, 379 U.S. 476, 484 (1965) (noting heightened Fourth Amendment concerns when expressive conduct is implicated); *United States* v. *Soybel*, 13 F.4th 584, 591 (7th Cir. 2021) (IP packets not protected by Fourth Amendment).

And the recent rise in the power and availability of artificial intelligence (AI) only exacerbates the potential harm from the misuse of personal data that Justice Sotomayor recognized in *Jones*, 565 U.S. at

---

[7] See, *e.g.*, Siddhant Kejriwal, *Is Monero Anonymous? How Untraceable is XMR?*, Coinbureau (Oct. 23, 2023) (describing Monero's "censorship-resistant blockchain"), https://tinyurl.com/5bf4zr79.

415. Machine learning algorithms can synthesize seemingly innocuous data—such as financial transactions, fitness metrics, browsing histories, or smart-home interactions—into detailed portraits revealing personal habits, health conditions, political affiliations, and social networks.[8] And such algorithms can do so much faster than humans. Thus, what would once have taken the government years to review can now be reviewed and summarized with the click of a button. Such easy and comprehensive invasions of privacy would have been anathema to Founding Era expectations and been seen as a terrible and dangerous governmental power if left unchecked.

If the Fourth Amendment is to continue to "take account of more sophisticated systems that are already in use or in development" in providing its protections, *Carpenter*, 585 U.S. at 313 (citation omitted), it should be responsive to the rise of generative AI and other AI systems as well. The fact that the First Circuit's misinterpretation of *Carpenter*—which mechanically applied the third-party doctrine—does not come close to accounting for this or other changes in technology is yet another powerful reason to grant review.

---

[8] See, *e.g.*, Barry Friedman, *Lawless Surveillance*, 97 N.Y.U.L. Rev. 1143, 1145 (2022) ("Search capacities and artificial intelligence have made combing through the information, collating it, and mining it, as simple as clicking a few buttons."); Auggie Alvarado, *The Mosaic Theory in Fourth Amendment Jurisprudence: The Last Bastion of Privacy in A Camera-Surveilled World*, 55 St. Mary's L.J. 849, 857-858 (2024) (interpreting *Carpenter* and *Jones*).

CONCLUSION

This Court should grant review to address widespread misinterpretations of *Carpenter* and mechanical but incorrect applications of the third-party doctrine as a near-total carveout from the Fourth Amendment's protections. Only by granting review and rejecting the approach adopted below can the Court ensure that the Fourth Amendment preserves the degree of privacy present at the Founding and does not leave the public at the mercy of advancing technology.

Respectfully submitted,

GENE C. SCHAERR
Counsel of Record
ERIK S. JAFFE
AARON C. WARD
SCHAERR | JAFFE LLP
1717 K Street NW, Suite 900
Washington, DC 20006
(202) 787-1060
gschaerr@schaerr-jaffe.com

Counsel for Amicus Curiae

April 30, 2025