No. 24-922

IN THE
Supreme Court of the United States

JAMES HARPER

Petitioner,

v.

DOUGLAS O'DONNELL, in his official capacity as Acting Commissioner of the Internal Revenue Service; INTERNAL REVENUE SERVICE; JOHN DOE IRS AGENTS 1–10,

Respondents.

On Petition for Writ of Certiorari to the U.S. Court of Appeals for the First Circuit

BRIEF AMICUS CURIAE OF COINBASE, INC. IN SUPPORT OF PETITIONER

ERIC TUNG
JONES DAY
555 S. Flower St.
Los Angeles, CA

NOEL J. FRANCISCO
Counsel of Record
MICHAEL BRADLEY
JONES DAY
51 Louisiana Ave., N.W.
Washington, DC 20001
(202) 879-3939
njfrancisco@jonesday.com

April 30, 2025

Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

OTHER AUTHORITIES

INTEREST OF AMICUS CURIAE[1]

Coinbase, Inc. is the largest digital-asset company in the United States and operates the country's largest, and only publicly traded, digital-asset trading platform. It is a leading provider of financial infrastructure for the crypto economy. Coinbase uses blockchain technology and digital assets to build a financial system that enables secure and easy crypto transactions. Its platform serves more than eight million transacting retail users and a substantial number of institutions that together engaged in over a trillion dollars of crypto trading in 2024.

The history of this case began when the Internal Revenue Service served Coinbase with a sweeping John Doe summons to produce personal and financial data for over 500,000 customers involved in millions of transactions across three full years. After Coinbase pushed back against that dragnet, the IRS narrowed the summons, demanding records for over 14,000 customers related to 8.9 million transactions across the same three years. The government never claimed to have particularized reasonable suspicion that any of those individuals failed to comply with the tax laws. Coinbase vigorously resisted the narrowed summons too—and succeeded in persuading the district court to narrow it still more—but eventually complied in accord with a court order, on pain of contempt.

---

[1] At least 10 days before this brief's filing deadline, amicus notified the parties' counsel of record of its intent to file this brief. No party's counsel authored any part of this brief, and no person or entity other than amicus, its members, or its counsel made a monetary contribution intended to fund the brief's preparation or submission.

This case directly affects Coinbase's interest in protecting the privacy rights of its users and in the correct application of this Court's doctrine on constitutional guarantees against warrantless government demands for third-party service providers to surrender users' personal information. If the First Circuit's ruling is allowed to stand, the Fourth Amendment will give no protection to millions of law-abiding Americans who routinely share intimate personal information with the third parties that ubiquitously store, transmit, or provide services based on that data. Coinbase files this amicus brief to explain its involvement in the history of this case, describe the unprecedented sweep of the John Doe summons, and urge the Court to curb the lower courts' unduly maximalist application of the third-party doctrine.

SUMMARY OF ARGUMENT

The Internal Revenue Service served a summons demanding that Coinbase surrender personal and financial information for 500,000 of its customers with respect to millions of crypto transactions spanning three years. Coinbase refused, and the government went back to the drawing board. The IRS next sought an enforcement order on a narrowed summons—one that still sought to mine the private information of 14,355 Coinbase customers with respect to 8.9 million financial transactions spanning three years. Despite Coinbase's continued resistance—and after a further (but slight) narrowing of the summons—the district court ultimately compelled Coinbase to comply. The First Circuit has now held that Coinbase customers' expectation of privacy in that information is unrea-

sonable—even though the court agreed with petitioner James Harper that the government could likely use the information to trace users' every crypto transaction in the past and monitor every crypto transaction in the future.

That holding is not only wrong. It sets a dangerous precedent. "[F]ew could have imagined a society" in which the government could force third parties to surrender "detailed, encyclopedic, and effortlessly compiled" personal and financial information with "just the click of a button" and "at practically no expense"—all without triggering the protections of the Fourth Amendment. *See Carpenter v. United States*, 585 U.S. 296, 309, 311 (2018). But that is just what the First Circuit allowed. This Court should grant certiorari, restore order to the third-party doctrine that the First Circuit misapplied, and protect Americans' privacy interests in digital information stored by third-party service providers.

This brief makes three points. First, Coinbase fought vigorously, in the proceedings that gave rise to Harper's lawsuit, to protect its customers' privacy rights in their personal and financial information. Second, the IRS John Doe summons at the heart of this case is unprecedented in its sweep. Last, the Court should intervene to clarify that the third-party doctrine does not allow the IRS to conduct dragnet searches like the one blessed by the courts below. This Court's guidance is especially important here because this case involves a new technology—blockchain—that is particularly susceptible to surveillance abuse.

ARGUMENT

I. Coinbase Fought to Protect Its Customers' Privacy Rights in Their Information.

Coinbase routinely cooperates with lawful government requests for information. But Coinbase, concerned for its customers' privacy rights, resisted the IRS's overbroad John Doe summons here. It tried to intervene to oppose the IRS's ex parte petition to serve the summons, refused to voluntarily comply with the summons, and advocated for its customers' privacy and notice rights in the course of opposing the IRS's enforcement petition. Coinbase complied with the summons under court order and on pain of contempt.

A. Coinbase took many steps to protect its customers' privacy interests against the overbroad IRS summons.

This case arises from an earlier one involving Coinbase. In 2016, the IRS petitioned the U.S. District Court for the Northern District of California for leave to serve a John Doe summons on Coinbase. *See* ECF 1, *United States of America v. John Doe*, No. 3:16-cv-06658 (N.D. Cal. Nov. 17, 2016). A John Doe summons is an "ex parte third-party summons issued 'where the IRS does not know the identity of the taxpayer[s] under investigation.'" *Harper v. Werfel*, 118 F.4th 100, 104 (1st Cir. 2024) (*Harper II*) (citation omitted). The IRS represented that it was investigating American crypto users who, the IRS said, might have underreported taxable gains on crypto transactions.

The summons asked Coinbase to produce transaction records, security settings, user profiles, correspondence, wallet registration information, and

reams of other information for every account for which Coinbase had records that showed a U.S. address, telephone number, email domain, or bank account in 2013, 2014, or 2015. ECF 2-6, at 13–15, *John Doe* (N.D. Cal. Nov. 17, 2016). That summons was breathtaking in scope: it targeted the personal and financial data of roughly 500,000 Coinbase accountholders. ECF 46, at 1*, United States v. Coinbase, Inc.*, No. 3:17-cv-01431 (N.D. Cal. July 27, 2017).

1. Coinbase moved to intervene to oppose the summons.

After the IRS named John Doe as the defendant in its ex parte action, Coinbase moved to intervene "to present . . . legal and factual arguments in opposition to the summons." ECF 19, at 1, *John Doe* (N.D. Cal. Jan. 11, 2017) (notice of motion). Coinbase argued that although it would "cooperat[e] with government entities in investigating illegal activities or other abuses of Coinbase services," it was also "strongly committed" to "protecting the important privacy interest of its account holders." *Id.* (memorandum). The district court granted the IRS leave to serve the summons. *Harper v. Rettig*, 675 F. Supp. 3d 190, 198 (D.N.H. 2023) (*Harper I*).

2. Coinbase refused to voluntarily comply.

The IRS served its summons on Coinbase. Concerned for its customers' privacy rights and viewing the summons as an overreach, Coinbase refused to comply. *See United States v. Coinbase, Inc.*, 2017 WL 5890052, at *1 (N.D. Cal. Nov. 28, 2017). So the IRS petitioned to enforce the summons. ECF 1, *Coinbase* (N.D. Cal. Mar. 16, 2016). Several Coinbase accountholders moved to intervene in the enforcement

action so that they could move to quash the summons. The court set a hearing on that motion.

At the hearing, Coinbase supported the intervenors' motion and notified the court that Coinbase would oppose the enforcement petition because the summons was "overly broad." ECF 38, at 25–26, 33–34, *Coinbase* (N.D. Cal. July 7, 2017). The IRS did not deny that no court had ever enforced a John Doe summons "this broad." *Id.* at 6. And the court later revealed that it "wouldn't have enforced the earlier summons" because of its massive overbreadth. ECF 76, at 7, *Coinbase* (N.D. Cal. Nov. 14, 2017).

After the hearing, and confronted with Coinbase's resistance and arguments, the IRS acknowledged the overbreadth of its summons by narrowing it considerably. With minor exceptions, the revised summons sought information about any Coinbase account that saw at least $20,000 of any transaction type—buy, sell, send, or receive—in 2013, 2014, or 2015. But that summons still requested a slew of information: it covered 8.9 million transactions involving 14,355 accountholders. ECF 46, at 7, *Coinbase* (N.D. Cal. July 27, 2017).

3. Coinbase opposed the revised summons and advocated for its customers' rights.

"[T]o protect its customers" from the summons, Coinbase continued firmly to "oppose[] the enforcement petition." *Id.* at 1. It denounced the revised summons as "overly broad" and as a "misguided" and "massive fishing expedition" designed to let the government "scour" the "private financial records of millions of transactions by thousands of law abiding account holders." *Id.* at 1, 18. It argued that the IRS

could not "paw through" the records of U.S. taxpayers when the agency had not proved that the summons would advance a proper enforcement interest. *Id.* at 10. Coinbase objected that the IRS could not claim a "realistic expectation" of finding in the "huge mountain" of summonsed documents "something that might somehow reveal, in some small part, non-compliance" when all the accountholders did was buy, sell, or transfer digital currency (conduct that is not itself illegal or inherently suspicious). *Id.* at 22. And it argued that the IRS had failed to meet the statutory conditions for enforcement.

Coinbase requested a hearing on the enforcement petition. *Id.* at 24–25. It also asked the court to notify affected accountholders, and give them a chance to object before Coinbase provided their information to the IRS, in the event that the court granted the petition. *Id.* at 25.

4. Coinbase underscored the illegality of the summons at an enforcement hearing.

Coinbase repeated those arguments at a hearing on the enforcement petition. Coinbase began by explaining the dual commitment that it espoused throughout the summons proceedings. On the one hand, Coinbase "wants to cooperate with the government" in accord with lawful legal process. ECF 76, at 20, *Coinbase* (N.D. Cal. Nov. 14, 2017). Coinbase "ha[s] a team that does nothing but respond to valid subpoenas," which it receives and responds to "all the time." *Id.* at 45. The company "ha[s] systems set up to do that," and the system and team are "able to do [that] in a much more efficient way." *Id.* The reason why is that those subpoenas are "much more specific

than" the dragnet IRS John Doe summons that Coinbase resisted here. *Id.* Coinbase had never seen a warrantless request this sweeping.

That fact mattered because, on the other hand, and as Coinbase explained, the company "built [its] systems in a very careful way to try to protect" personal identifiable information "at every level" to ensure that the company "protect[s] a customer's privacy." *Id.* at 44. That concern for customer privacy spurred Coinbase to argue that the IRS was "abus[ing]" a "powerful tool" in order to "invade" the "privacy of individuals, of U.S. citizens." *Id.* at 8, 27. The summons was "wildly overbroad" and was "not legitimate" in "manner" or "scope." *Id.* at 5, 29. And—Coinbase warned—if *this* summons were enforceable, the government "could target anybody" it wanted and obtain their personal information from a third party recordholder. *See id.* at 7.

B. The district court required only a "minimal" showing and ordered Coinbase to comply.

In spite of these arguments, the district court granted the enforcement petition in part, denied Coinbase's request for an evidentiary hearing, and ordered Coinbase to produce taxpayer ID numbers, names, birthdates, addresses, and "records of account activity"—including transaction logs, post-transaction balances, and the names of transaction counterparties—for the 14,355 targeted accountholders. *Coinbase*, 2017 WL 5890052, at *8–9. The court stressed that the IRS's burden to show a legitimate investigation purpose was "minimal" and that the statute that governs enforcement requests did not require the agency to

show probable cause for the inquiry or even reasonable suspicion of wrongdoing on the part of the John Does. *Id.* at *6–7. Still, the court agreed with Coinbase that the narrowed summons was overbroad. So the court did not allow the IRS to compel the production of several kinds of documents that were unnecessary to the agency's stated investigative purpose. *Id.* at *7. Yet the court also did not notify affected Coinbase accountholders or afford them an opportunity to object.

Coinbase obeyed the enforcement order on pain of contempt. In 2019, the IRS informed Harper that it had obtained "information" that he might not have correctly reported his taxable crypto transactions. Pet. at 6. Harper then filed this lawsuit.

The courts below correctly recognized that Coinbase opposed the IRS's fishing expedition at every stage. The district court noted that Coinbase "did not comply" with the summons, "opposed the petition" for enforcement, and "made the IRS satisfy additional procedural hurdles" in the enforcement proceeding. *Harper I*, 675 F. Supp. 3d at 198, 207. The First Circuit likewise remarked that Coinbase "opposed the summons," "continued to oppose the narrowed summons," and produced the records only in the face of a "judicial enforcement order." *Harper II*, 118 F.4th at 105, 114.

Coinbase litigated as it did not because it is uncooperative. At the hearing on the enforcement petition, when Coinbase pointed out that it "wants to cooperate with the government" but that it must oppose this unlawful John Doe summons, the district court acknowledged that Coinbase is a "very legitimate company" that the IRS turned to because it knew that Coinbase

kept diligent records. ECF 76, at 20, *Coinbase* (N.D. Cal. Nov. 14, 2017). Coinbase opposed the summons because it is an unlawful encroachment on Coinbase users' privacy rights.

II. The Summons that Coinbase Resisted Was Unprecedented in Its Sweep.

The John Doe summons that Coinbase resisted and that led to the government's acquisition of Harper's personal and financial information was not only unlawful. It was unprecedented in its sweep. The summons targeted 14,355 Americans. The IRS did not have particularized reasonable suspicion that a single one of them was evading his or her tax obligations. The summons also covered 8.9 million transactions. And it requested information across three full years.

Yet the true scope of the summons is far wider—and more chilling. Cryptocurrency transactions are recorded on the blockchain, a digital ledger that preserves user privacy through pseudonymous addresses. *United States v. Gratkowski*, 964 F.3d 307, 309 & n.2 (5th Cir. 2020). Every blockchain address—which is like a bank-account number—corresponds to a public key or wallet address. Each public key or wallet address in turn derives from a private key, which is "secret, like [a] password[]." *United States v. Harmon*, 474 F. Supp. 3d 76, 81 (D.D.C. 2020).

The blockchain, which records every crypto transaction, *id.*, preserves anonymity because it does not reveal the identities of the accountholders whose public keys or wallet addresses the ledger records. Blockchain technology thus ensures privacy in financial transactions.

But user anonymity vanishes—and the blockchain becomes susceptible to easy surveillance—when the government acquires information that allows it to match a public key or wallet address to a user's identity. *Matter of Search of One Address in Washington, D.C., Under Rule 41*, 512 F. Supp. 3d 23, 26 (D.D.C. 2021). When that happens, "anyone aware of that information can easily ascertain *all* transactions the person has made using that address—or track future transactions." *Harper II*, 118 F.4th at 109 n.9 (emphasis added). And "exposure" of exactly that anonymity-shattering information "was a reasonably likely consequence" of the IRS summons that Coinbase resisted and Harper challenges. *Id.*

Armed with that vital information, the IRS now can scan the blockchain for every transaction that the user whose public key or wallet address it holds has ever made *or will ever make* on the blockchain. Even if a user creates a new address, publicly available software allows the government to trace the old address to the new one and to continue monitoring that user's crypto transactions indefinitely. Law enforcement "widely relie[s] upon" that kind of tracing. *United States v. Sterlingov*, 719 F. Supp. 3d 65, 84 (D.D.C. 2024). So the IRS's acquisition of information through the John Doe summons allows the agency to "effectively obtain[] a real-time monitor" of every crypto transaction that has been or will be executed by over 14,000 U.S. citizens. Pet. at 33.

The summons thus breaks new ground. Coinbase is aware of no comparable warrantless acquisition by the government, through compulsory third-party production, of as sweeping a body of information about

American taxpayers whom the government lacks particularized reason to suspect of tax noncompliance.

III. The Court Should Grant the Petition to Clarify the Third-Party Doctrine.

This Court should grant the petition. The First Circuit based its holding on two decisions from the 1970s that it said "squarely" defeated Harper's privacy claim. That conclusion was wrong: the court overread those decisions by failing to discern their limiting principles. This Court should enforce those limits, which *Carpenter v. United States* underscored. And this Court's guidance is especially important because this case involves a technology, blockchain, that is acutely susceptible to surveillance abuses.

A. The Court should clarify that *Miller* and *Smith* do not allow the IRS to acquire troves of personal and financial information—including about a user's every past and future blockchain transaction—just because a third party holds that information.

Government intrusion into a sphere that a person reasonably expects to preserve as private is ordinarily a search under the Fourth Amendment and thus requires a warrant supported by probable cause. *Carpenter*, 585 U.S. at 304 (discussing *Katz v. United States*, 389 U.S. 347 (1967)). Harper argued below that the John Doe summons was a warrantless search that violated his Fourth Amendment right because he had a reasonable expectation of privacy in the records that Coinbase produced. *See Harper II*, 118 F.4th at 108.

The First Circuit rejected that argument on the ground that Harper's expectation of privacy was unreasonable. *Id.* at 107–110. The court reached its holding based on the third-party doctrine, according to which a person generally "has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 107 (quoting *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979)). That doctrine, said the First Circuit, "squarely" defeated Harper's argument because the records that Coinbase produced are "directly analogous" to the bank records at issue in *United States v. Miller*, 425 U.S. 435 (1976), a decision in which this Court rejected a person's reasonable expectation of privacy in subpoenaed records, held by third-party banks, about his financial transactions. *See Harper II*, 118 F.4th at 107–08.

Several sitting members of this Court have criticized or expressed concern about the third-party doctrine or the *Katz* reasonableness test that it modifies. Justice Sotomayor has observed that the third-party doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *United States v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring). Changed social and technological circumstances pose "difficult questions" for the doctrine. *Id.* at 418.

Justice Gorsuch has asked what would remain of the Fourth Amendment under a wooden application of the third-party doctrine in the digital age. "Today," he has noted, "we use the Internet to do most everything. Smartphones make it easy to keep a calendar, corre-

spond with friends, make calls, [and] conduct banking." *Carpenter*, 585 U.S. at 387 (Gorsuch, J., dissenting). "Even our most private documents" "now reside on third party servers." *Id.* In Justice Gorsuch's view, "People often *do* reasonably expect that information they entrust to third parties, especially information subject to confidentiality agreements, will be kept private." *Id.* at 389. So it is "pretty unlikely" that the Fourth Amendment allows the "government [to] demand a copy of all your e-mails from Google or Microsoft without implicating your Fourth Amendment rights." *Id.* at 388.

And Justice Thomas has criticized the *Katz* reasonableness test, which the third-party doctrine modifies, for "distort[ing]" Fourth Amendment jurisprudence and lacking any "basis in the text or history" of the Amendment. *Id.* at 343, 346 (Thomas, J., dissenting).

The Justices' concerns are weighty. But even on the third-party doctrine's own terms, this John Doe summons invaded a sphere in which over 14,000 Americans had a reasonable expectation of privacy against a warrantless IRS trawl for extensive personal and financial information.

The First Circuit was mistaken to rule that the third-party doctrine of *Miller* and *Smith* "squarely" defeated Harper's Fourth Amendment privacy claim. *Harper II*, 118 F.4th at 107. Consider *Miller*, which began in a government investigation of an illegal distillery operation. The government received an informant's tip, found Miller's coconspirators in possession of distillery apparatus, and discovered suspicious evidence at a warehouse rented by Miller. 425 U.S. at

437. The government then served two "narrowly directed" subpoenas—"issued in blank by the clerk of the District Court, and completed by the United States Attorney's office," *id.*—on two banks at which Miller had accounts, *id.* at 445 n.6. The subpoenas sought "all records of accounts" in Miller's name over nearly four months. *Id.* at 437–38. The bank presidents "compl[ied] without protest," *id.* at 443, and showed the investigating agents "checks, deposit slips, two financial statements, and three monthly statements," *id.* at 438.

This Court rejected Miller's argument that the subpoenas were a Fourth Amendment search. The Court stated that it "must examine the nature of the particular documents" at issue "to determine whether there is a legitimate 'expectation of privacy' concerning their contents." *Id.* at 442 (citation omitted). And the Court concluded that the subpoenaed bank records "contain[ed] only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Id.* A bank depositor "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." *Id.* at 443. The same is true "even if the information" that the depositor shares with the bank "is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* Because Miller had no reasonable expectation of privacy in the bank records, the Court held, no Fourth Amendment search occurred.

Now consider *Smith*. Police were investigating a robbery. They had a description of the robber and of a car reportedly seen near the crime scene, eyewitness testimony that connected the suspect to that car, and a tip that a man identifying as the robber was placing threatening calls to the victim. 442 U.S. at 737. A local telephone company, "at police request" and without any legal or judicial process, agreed to install a pen register—a mechanical device that records the numbers dialed on a telephone—at its central office in order to record the numbers dialed from the suspect's home phone during a single day. *Id.*

The Supreme Court rejected Smith's argument that the use of the pen register was a Fourth Amendment search. The Court found it "important" to "begin" its *Katz* analysis by "specifying precisely the nature of the state activity that is challenged." *Id.* at 741. Stressing the pen register's "limited capabilities," the Court noted that the register did not record the content of phone calls or even reveal whether the call connected. *Id.* at 741–42. The pen register merely recorded the digits dialed. The Court also said that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743–44. And because Smith had "voluntarily conveyed" to the telephone company "information that it had facilities for recording and that it was free to record," *id.* at 745, he had no reasonable expectation of privacy.

The third-party doctrine of *Miller* and *Smith* has three pivotal limiting features. Together, those features show that the doctrine does not exempt the John Doe summons from Fourth Amendment protection.

First, the disputed investigative acts in *Miller* and *Smith* each targeted a single individual whom the government had particularized reason to suspect of a crime. *Miller*, 425 U.S. at 437; *Smith*, 442 U.S. at 737. The John Doe summons, by contrast, targeted over 14,300 Americans—not one of whom the IRS had particularized reason to suspect of tax noncompliance.

Second, the investigative acts in *Miller* and *Smith* were narrow in scope and posed no risk of ongoing surveillance. *Miller*, 425 U.S. at 437–38, 445 n.6 (noting that the subpoenas were "narrowly directed" to cover less than four months' records); *Smith*, 442 U.S. at 737, 742 (noting the pen register's "limited capabilities" and its use for only one day to track the digits dialed on a home phone). Yet the John Doe summons covers 8.9 million transactions over 3 full years. And the summonsed information, which reveals the identities of Coinbase accountholders, likely lets the IRS reconstruct the users' crypto transactions in the past, and monitor all their blockchain transactions indefinitely in the future. The summons is, then, for crypto users a "dragnet-type law enforcement practice[]." *See United States v. Knotts*, 460 U.S. 276, 283–84 (1983).

Third, the third parties in *Miller* and *Smith* complied voluntarily with the investigative requests; neither acted under court-ordered compulsion. *Miller*, 425 U.S. at 437–38; *Smith*, 442 U.S. at 737. But Coinbase, unlike the banks in *Miller* and the telephone company in *Smith*, refused to comply with the information requests voluntarily; it complied only in the face of a "judicial enforcement order" and on pain of contempt. *See Harper II*, 118 F.4th at 114. A customer

whose third-party service provider believes—as Coinbase does—that personal information is worth protecting and that it should not be surrendered simply whenever law enforcement requests it has a more reasonable expectation of privacy in that information than does a customer whose third-party service provider hands personal information over to the government merely upon request, apart from judicial process.

The First Circuit hit wide of the mark in missing these differences. It embraced exactly the kind of "mechanical interpretation of the Fourth Amendment" that this Court has roundly "reject[ed]," and its wooden application of 1970s precedents failed to "take account of [the] more sophisticated" realities on the ground. *See Kyllo v. United States*, 533 U.S. 27, 35–36 (2001). The Fourth Amendment "assures preservation of that degree of privacy against government that existed" when the amendment was adopted, *id.* at 34, but the First Circuit's decision "leaves" citizens "at the mercy of advancing technology." *see id.* at 34–35. For it is at least "dubious," "[g]iven the ubiquity—and necessity—in the digital age of entrusting corporations like Google, Microsoft, and Apple with highly sensitive information," that "users voluntarily relinquish their right to privacy" just by using digital technology to conduct financial transactions. *See United States v. Smith*, 110 F.4th 817, 835 (5th Cir. 2024). *Miller* and *Smith* require courts to examine the nature of the documents at issue and to specify precisely the nature of the challenged state action. The First Circuit failed to heed that command.

B. The Court should enforce *Carpenter*'s limitation of the third-party doctrine.

This Court's decision in *Carpenter* confirmed the third-party doctrine's limited reach. In *Carpenter*, police officers arrested men suspected for robbery. One suspect confessed that he and a crew of at-large accomplices collaborated in the heists. He identified accomplices and gave the FBI some of their cellphone numbers. The FBI reviewed the man's phone records to identify other numbers that might belong to accomplices. "Based on that information," prosecutors applied for court orders to obtain cellphone records for the additional suspects. 585 U.S. at 301. A magistrate judge issued orders that directed third-party service providers—wireless network carriers—to produce timestamped phone-location records, known as cell site location information (CSLI), for Carpenter. *Id.* at 301–02.

The Court held that the government engaged in a Fourth Amendment search when it accessed seven days' CSLI. *Id.* at 310 n.3. In reaching that holding, the Court clarified the third-party doctrine. First, the Court rejected the doctrine's sufficiency as a test for Fourth Amendment privacy claims. "[N]o single rubric definitively resolves which expectations of privacy are entitled to protection." *Id.* at 304. By the same token, the fact "that [personal] information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection." *Id.* at 309. After all, *Miller* and *Smith* "did not rely solely on the act of sharing" information; those decisions focused on the "nature of the particular documents sought." *Id.* at 314 (quoting *Miller*, 425 U.S. at 442).

Nor does the fact that third-party service providers "generat[e]" and keep records "for commercial purposes" in the ordinary course of business "negate" a person's "anticipation of privacy" in the information contained in those records. *Id.* at 311. Cellphone users connected to the wireless network "continuously reveal[]" their locations to their wireless carriers, and the carriers use that information routinely, but those facts are not dispositive. *Id.* at 309. So when "[t]here is a world of difference between the limited types of personal information addressed in *Smith* and *Miller*" and third-party records that lack "comparable limitations," courts must reject "mechanical[]" applications of the third-party doctrine and instead "contend with" "seismic shifts in digital technology." *Id.* at 313–14.

Those principles dictated that *Miller* and *Smith* should not be "extend[ed]" to "novel circumstances" involving "qualitatively different" records than those precedents discussed. *Id.* at 309. "[F]ew could have imagined a society" in which the government could make third parties surrender "detailed, encyclopedic, and effortlessly compiled" information with "just the click of a button" and "at practically no expense." *Id.* at 309, 311. And CSLI "implicates privacy concerns far beyond those considered in *Smith* and *Miller*." *Id.* at 315.

The First Circuit misapplied *Carpenter*. The information summonsed by the IRS lacks "comparable limitations" to the information at issue in *Miller* and *Smith*. *See id.* at 314. Coinbase's information is detailed, compiled without government effort, and available at the click of the mouse for little-to-no cost to the government. Armed with Coinbase's records, the IRS

can "effortlessly compile[]" "detailed," encyclopedic information about all past and future transactions of 14,355 American users, "at practically no expense" to the government. *See id.* at 309, 311. Nobody "could have imagined a society in which" the IRS could "achieve[] near perfect surveillance" of thousands of blockchain users' crypto transactions by strapping a financial "ankle monitor"—pegged to users' wallet addresses—onto anyone the government thinks might be evading his or her tax obligations. *See id.* at 309, 311–12. The summonsed information, then, implicates privacy concerns unlike those at stake in *Miller* and *Smith*. Instead, the summons, like the "reviled" general warrants of the colonial era, allows the IRS to "rummage through" crypto users' information "in an unrestrained search for evidence of criminal activity" in respect of tax law. *See Riley v. California*, 573 U.S. 373, 403 (2014).

Indeed, the government had a far weaker basis to conduct a warrantless search here than it did the search held unjustified in *Carpenter*. Law enforcement had particularized, evidence-based reasons to seek a court order for Carpenter's CSLI. *Carpenter*, 585 U.S. at 301–02. The IRS had nothing comparable—for any of the 14,355 targeted Coinbase users. Law enforcement in *Carpenter* sought CSLI for one individual. The IRS summonsed information regarding over 14,000. And *Carpenter* held that seven days' CSLI was too long. *Id.* at 310 n.3. The IRS demanded three years' information—and that information is the portal to even more monitoring. Recall, too, that the summonsed information allows the government to surveil *all* the user's crypto transactions on the block-

chain: *all* past transactions (including those that predate 2013), *all* future actions (including those far beyond 2015), and even those that do not take place on the Coinbase exchange. *See supra* Part II. The CSLI in *Carpenter* did not generate comparable ongoing, around-the-clock surveillance opportunities interminably.

The First Circuit acknowledged some of these facts but then brushed them aside. The court "d[id] not doubt" that "exposure of a person's identity" on the blockchain "opens a potentially wide window into that person's financial activity contained on that ledger." *Harper II*, 118 F.4th at 109. And the court agreed with Harper that a "reasonably likely consequence of the IRS summons" was the "exposure" of information that lets the government "easily ascertain all transactions the person has made using that address—or track future transactions." *Id.* at 109 & n.9. Yet the court waved this specter away, saying that it "ma[de] no difference" to the "conclusion that [Harper] lacked a reasonable expectation of privacy." *Id.* at 109 n.9. Under *Carpenter*, which confirms *Miller* and *Smith*'s limiting principles, that proposition cannot be right.

C. The Court's guidance is particularly needed on the Fourth Amendment's application to blockchain technology.

As noted, the First Circuit's decision is particularly troubling given the nature of blockchain technology. One purpose of cryptocurrency and blockchain technology—"seismic shifts in digital technology," *see Carpenter*, 585 U.S. at 313—is to enhance and secure their users' privacy by pseudonymizing financial transactions. *See, e.g.*, Paul Belonick, *Transparency Is*

the New Privacy: Blockchain's Challenge for the Fourth Amendment, 23 Stan. Tech. L. Rev. 114, 136 (2020) (explaining that blockchain technology "deeply cloaks computer operators' true identities"). So even if it were true that users are "unlikely to expect that the information *published on the Bitcoin blockchain* will be kept private," *Gratkowski*, 964 F.3d at 312 (emphasis added), what compromises user privacy is divulgence that *links* that public information with the private information that the John Doe summons dredged up. *See Harper II*, 118 F.4th at 109 n.9 (admitting that the summons was likely to yield information that allowed the IRS to "pierc[e]" the blockchain's "veil of anonymity").

Users have a reasonable expectation of privacy at least in that combined set of information. Justice Sotomayor has "doubt[ed]" that Americans would "accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year." *Jones*, 565 U.S. at 418 (concurring opinion). Justice Gorsuch thinks it "pretty unlikely" that the Fourth Amendment allows the "government [to] demand a copy of all your e-mails from Google or Microsoft without implicating your Fourth Amendment rights." *Carpenter*, 585 U.S. at 388 (dissenting opinion). No less is true of the warrantless disclosure to the government of a list of every crypto transaction someone ever has made or ever will make.

* * *

The First Circuit is not alone in applying the third-party doctrine in the mechanical mode that this Court

rejected in *Carpenter*. Other courts continue to maximally interpret the doctrine while paying scant heed to its proper scope in the digital age. *See, e.g.*, *United States v. Soybel*, 13 F.4th 584, 591 (7th Cir. 2021); *United States v. Trader*, 981 F.3d 961, 968 (11th Cir. 2020). This momentum needs halting. Given how many, and how often, Americans entrust the intimate aspects of their lives to third-party digital service providers, the lower courts' overreading of *Miller* and *Smith* will, if unchecked, eviscerate Fourth Amendment privacy protections in most personal information. The Court should grant Harper's petition, reverse the First Circuit, and clarify the third-party doctrine in the digital era.

CONCLUSION

The Court should grant the petition.

April 30, 2025

Respectfully submitted,

ERIC TUNG
JONES DAY
555 S. Flower St.
Los Angeles, CA

NOEL J. FRANCISCO
Counsel of Record
MICHAEL BRADLEY
JONES DAY
51 Louisiana Ave., N.W.,
Washington, D.C.
(202) 879-3939
njfrancisco@jonesday.com

Counsel for Amicus Curiae