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 for DeFi Education Fund as Amicus Curiae in Support of Petitioner

J. Abraham Sutherland
106 Connally Street
Black Mountain, NC 28711
(805) 689-4577

Cameron T. Norris
Counsel of Record
Jeffrey S. Hetzel
Zachary P. Grouev
CONSOVOY MCCARTHY PLLC
1600 Wilson Blvd., Ste. 700
Arlington, VA 22209
(703) 243-9423
cam@consovoymccarthy.com

March 28, 2025

Attorneys for Amicus Curiae

TABLE OF CONTENTS

TABLE OF CITED AUTHORITIES

Cases

Other Authorities

INTEREST OF AMICUS CURIAE*

DeFi Education Fund is a nonpartisan research and advocacy group based in the United States. DEF's mission is to explain the benefits of decentralized finance, help achieve regulatory clarity for decentralized finance technology, and contribute to the realization of the transformative potential of decentralized finance for everyone. Decentralized finance is part of the cryptocurrency ecosystem. DEF advocates for the interests of decentralized finance users, participants, and software developers working to create new decentralized finance products using blockchain technology. Among other things, DEF educates the public about decentralized finance through op-eds, podcasts, and print media; meets with members of Congress to discuss decentralized finance and attendant issues; and submits public comments on proposed rulemakings that impact decentralized finance.

As part of its mission, DEF has an interest in educating courts about the nature of cryptocurrency technology. It also has an interest in a legal order that respects the constitutional rights and privacy interests of all cryptocurrency users.

---

* Under Rule 37.2, counsel for amicus curiae notified counsel for all parties of its intent to file this amicus brief more than 10 days before the due date. Under Rule 37.6, no counsel for a party authored this brief in whole or in part, and no person other than amicus, its members, or its counsel made a monetary contribution to its preparation or submission.

SUMMARY OF ARGUMENT

When the government forces a private company to hand over the personal cryptocurrency transaction records of 14,355 people without probable cause or a warrant, it violates the Fourth Amendment. The First Circuit concluded otherwise only by adopting a maximalist version of the "third-party doctrine" that warrants this Court's review. Third-party sharing defeats a person's Fourth Amendment rights only under limited circumstances, none of which were present here. The First Circuit's approach continues a concerning trend of courts treating third-party sharing as effectively dispositive, even after this Court said the opposite in *Carpenter*. And this case particularly warrants review because it involves a new technology, cryptocurrency, with heightened privacy concerns that make the application of the third-party doctrine especially inappropriate.

This Court's precedents do not support the First Circuit's version of the third-party doctrine. Before the 1970s, this Court held that people had Fourth Amendment rights in their records regardless of whether they shared them with third parties. For instance, when people shared records with third-party mail carriers or telephone companies, the Fourth Amendment still protected them. *See Ex Parte Jackson*, 96 U.S. 727 (1877); *Katz v. United States*, 389 U.S. 347 (1967). Then in two 1970s cases—*Smith v. Maryland* and *United States v. Miller*—this Court said that sharing records with third parties could, in some circumstances, defeat a person's privacy rights in those records. *See Smith v. Maryland*, 442 U.S. 735 (1979); *United States v. Miller*, 425 U.S. 435 (1976).

But *Smith* and *Miller* had major limitations. In both cases, the "third parties" cooperated with the government voluntarily, the information accessed through them was limited to a few records, and the search targeted just a single person. *Smith*, 442 U.S. at 742-46; *Miller*, 425 U.S. at 442-43. In *Carpenter*, this Court confirmed that the third-party doctrine should not be "exten[ded]" to new circumstances absent "comparable limitations" to those present in *Smith* and *Miller*. *Carpenter v. United States*, 585 U.S. 296, 309, 314 (2018). And for good reason: an unbounded third-party doctrine would remove privacy in most of modern life. *See id.* at 387 (Gorsuch, J., dissenting).

Yet the First Circuit extended the third-party doctrine dramatically. The government in this case acquired Jim Harper's cryptocurrency transaction history from Coinbase, a private exchange. To obtain these records, the government did not secure Coinbase's voluntary cooperation. Unlike the third parties in *Smith* and *Miller*, Coinbase refused to comply and produced the records only under threat of contempt. App.65a-66a; *United States v. Coinbase, Inc.*, 2017 WL 5890052 (N.D. Cal. Nov. 28). The government did not obtain minimal information. It obtained transaction histories with personal information for 8.9 million cryptocurrency transactions. *Coinbase, Inc.*, 2017 WL 5890052, at *8-9. The government's search was not tailored to a specific suspect. It sought the information of Harper along with 14,354 other innocent people. *Id.* And because of the nature of cryptocurrency, the government's access to millions of transactions also gave it access to these people's other transactions, indefi-

nitely into the past and future. It put their cryptocurrency affairs into a state of permanent surveillance with no probable cause or warrant. Nonetheless, the First Circuit ruled that the Fourth Amendment had no role to play, simply because Harper had chosen to share his affairs with Coinbase. App.12a-14a. And because what Harper shared was not "cell-site location information," *Carpenter* offered no help. App.15a.

The First Circuit's runaway third-party doctrine is wrong, and this Court should grant certiorari to correct it.

REASONS FOR GRANTING THE PETITION

Harper's brief explains the main problems with the third-party doctrine as articulated by the First Circuit and other courts of appeals. *See* Pet.Br.9-19. This brief explains why even under this Court's existing precedents, including *Smith* and *Miller*, the First Circuit's decision was wrong and should be reversed. It then explains why this case warrants review because of the special privacy concerns raised here given the nature of cryptocurrency.

I. This Court's third-party doctrine has always been limited.

A. The third-party doctrine did not exist before *Smith* and *Miller*.

Before *Smith* and *Miller*, the Fourth Amendment protected papers even when they were shared with third parties. Thanks to the nineteenth-century mail and telegraph systems, courts were long familiar with people conducting their business and communications through third-party intermediaries. But the Fourth

Amendment still protected those people's papers after they were shared with third parties. In *Ex Parte Jackson*, this Court interpreted the Fourth Amendment to mean that although people share letters with recipients and the government, "[n]o law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters." 96 U.S. at 733. To open a letter in the mail, the government had to obtain a "warrant." *Id.* "It did not matter that letters were bailed to a third party (the government, no less)." *Carpenter*, 585 U.S. at 400 (Gorsuch, J., dissenting). *Ex Parte Jackson* was unanimous; no justice suggested that third-party sharing defeated a person's Fourth Amendment rights.

Ex Parte Jackson reflected a broader commitment to privacy in matters shared with third parties. As Thomas Cooley explained a decade earlier, the Fourth Amendment "directly condemned" a postal officer "prying into private correspondence." Cooley, *A Treatise on the Constitutional Limitations Which Rest upon the Legislative Power of the States of the American Union* 306-07 n.2 (1868). The same reasoning applied to all sorts of matters shared with third parties: both "public correspondence … through the post office" and "private correspondence by telegraph" were protected by the Fourth Amendment against any government "prying." *Id.* And it would be equally unconstitutional, Cooley explained, for "a man's servants" to "be subpoen[a]ed to bring into court his private letters and journals." *Id.* The notion that such third-party sharing could justify warrantless searches into otherwise private matters, according to Cooley, "would be

met with general indignation" and viewed as "directly in the face of the law." *Id.*

Other Fourth Amendment cases long implicitly rejected the third-party doctrine. In *Hale v. Henkel*, this Court explained that the Fourth Amendment protected business correspondence and contracts between a man and six companies, even though the parties had all voluntarily shared the correspondence and contracts with each other in the ordinary course of business. 201 U.S. 43, 76-77 (1906), *overruled on other grounds* by *Murphy v. Waterfront Comm'n of N.Y. Harbor*, 378 U.S. 52 (1964). And in *Katz v. United States*, this Court held that the government conducted a search when it recorded a person's telephone conversations, even though the third-party phone company was always free to monitor them independently. 389 U.S. at 348-53; *see also United States v. Warshak*, 631 F.3d 266, 287 (6th Cir. 2010) ("In *Katz*, the Supreme Court found it reasonable to expect privacy during a telephone call despite the ability of an operator to listen in.").

In other words, the third-party doctrine is a modern innovation: it "largely traces its roots to" two 1970s decisions, *Smith* and *Miller*. *Carpenter*, 585 U.S. at 308; *accord id.* at 387-88 (Gorsuch, J., dissenting).

B. *Smith* and *Miller* created a limited third-party doctrine.

Smith and *Miller* should not be read to stand for more than they say. In those cases, this Court was careful not to make third-party sharing *sufficient* to

defeat a person's right to privacy. *See Carpenter*, 585 U.S. at 314 ("*Smith* and *Miller*, after all, did not rely solely on the act of sharing"). Instead, it said that third-party sharing could defeat a person's reasonable expectation of privacy in limited circumstances, and those circumstances are not present here. *Smith*, 442 U.S. at 742-46.

In *Smith*, the government asked a phone company to give it one day's worth of phone numbers dialed by a suspected robber. *Id.* at 737. The suspected robber, Smith, had already robbed a woman, called her and identified himself as the robber, and drove by her house to again identify himself as the robber. *Id.* The police asked his phone company to just confirm that he was calling her. *Id.* The police did not use coercion against the phone company. They just asked the phone company to record the numbers he dialed, which the phone company could easily access, and to pass them along. *Id.* at 737, 742-45. And they asked the phone company for very little information: a single day's worth of call records from a single person. *Id.* The call records would show nothing beyond the digits that he dialed. *Id.* at 741.

This Court rejected Smith's Fourth Amendment challenge. It emphasized the limited nature of the information obtained: the police did "not acquire the contents of communications." *Id.* at 741. Importantly, "[n]either the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed [wa]s disclosed" through the third-party. *Id.*; *see also Carpenter*, 585 U.S. at 314 ("telephone call logs reveal little

in the way of 'identifying information'"). The Court then went on to explain that the Fourth Amendment challenge also failed because everyone knows that they share the numbers they dial with the phone company, and thereby "assum[e] the risk" that the company will pass those numbers along to the police. *Smith*, 442 U.S. at 744. It did not have any reason to say what would happen if the police asked for more information or if the phone company did not go along voluntarily.

Miller involved similar limitations. The government asked a bank to give it a small number of bank records of one man, Miller, who was running a tax-evading whiskey distillery. 425 U.S. at 437. The government had already discovered the distillery and whiskey. *Id.* So it subpoenaed two banks for Miller's records. Again, the Court explained that the banks produced the records "without protest" and "voluntarily." *Id.* at 439, 442-43. The government collected from the bank only "two financial statements," "three monthly statements," and some "checks" and "deposit slips." 425 U.S. at 438. The information was roughly what could have been in the defendant's pocket. *See Riley v. California*, 573 U.S. 373, 400 (2014) ("someone could have tucked a paper bank statement in a pocket").

The Court rejected Miller's Fourth Amendment challenge. It explained that, by doing business with a bank, a depositor risks having the bank give the records of that business to the government. *Miller*, 425 U.S. at 444. Again, it did not opine on whether the government could acquire the information by force

from the banks or whether the government could acquire unlimited information. To the contrary, it emphasized that the bank documents were "not confidential communications but negotiable instruments to be used in commercial transactions" and that the banks themselves "betrayed" Miller's trust. 425 U.S. at 442, 443.

Smith and *Miller* thus involved at least three limiting circumstances that should cabin the third-party doctrine.

First, the third parties gave the records to the government "voluntarily." *Miller*, 425 U.S. at 439, 442. Under this Court's Fourth Amendment cases, coercion often separates lawful from unlawful searches. *See, e.g.*, *Bumper v. North Carolina*, 391 U.S. 543, 550 (1968); *Fernandez v. California*, 571 U.S. 292, 296 n.2, 298 (2014). In *Smith* and *Miller*, the Court thought of the Fourth-Amendment issue as analogous to confidential-informant cases where the defendant complains that a private party has "betrayed" his trust and "voluntarily cooperated" against him. *Miller*, 425 U.S. at 439, 443; *see id.* at 443 (collecting confidential-informant cases). So *Smith* and *Miller* should not extend to cases where the third party objects and the government resorts to coercion.

Second, the records accessed in *Smith* and *Miller* were limited. Neither case involved encyclopedic or intimate information—they involved a day's worth of phone numbers, *Smith*, 442 U.S. at 737, and a handful of business records, *Miller*, 425 U.S. at 438. This Court

has repeatedly held that Fourth Amendment protections are heightened when the government seeks a "deep repository" of information, "encyclopedic" information, or "intimate" information. *Carpenter*, 585 U.S. at 309, 311. So when *Smith* and *Miller* emphasized that the government's searches accessed only "limited" information, they did not mean that the government was free to use the same method to obtain millions of records or more sensitive information. *Smith*, 442 U.S. at 742.

And third, neither case targeted more than a single person, against whom the government already had strong evidence of criminality. In both cases, the defendants had already been caught red-handed. *Smith*, 442 U.S. at 737 (detailing all the evidence preceding the search); *Miller*, 425 U.S. at 437 (same). Probable cause likely existed against both Smith and Miller. The government did not ask for the papers of anyone else. Their reasoning should not be lightly extended to authorize "fishing expeditions" into the "private papers" of innocent persons, which this Court has repeatedly condemned. *FTC v. Am. Tobacco Co.*, 264 U.S. 298, 306 (1924) (Holmes, J.). The third-party doctrine, as articulated by this Court, cannot be read to authorize "dragnet type law enforcement practices" that intrude on the privacy of many people all at once. *United States v. Knotts*, 460 U.S. 276, 284 (1983).

C. *Carpenter* confirmed those limits.

Carpenter vindicated the more limited reading of *Smith* and *Miller*. In *Carpenter*, this Court held that the government could not obtain a defendant's cell-site location information, even though he shared that

information with a third party. The cell-site information consisted of reports regarding the defendant's cell phone location over the course of multiple days. 585 U.S. at 300-02. The Court explained that, despite the third-party sharing, the defendant had a successful Fourth Amendment argument against the government's warrantless access to those location reports. *Id.* at 313.

This Court explained that the original limitations of the third-party doctrine from *Smith* and *Miller* were not present. The reasoning of those cases held up for "telephone numbers and bank records." *Id.* at 309. And the third-party doctrine could be "extend[ed]" only to circumstances involving "comparable limitations." *Id.* at 309, 314. So when the government used a subpoena to access papers that were "detailed, encyclopedic, and effortlessly compiled," the third-party doctrine no longer applied. *Id.* at 309. The Court stressed the "deep repository of historical location information" accessed by the government. *Id.* at 311. This information could "revea[l] not only [the person's] particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Id.* (quoting *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)). And the search was easy to scale. The government could obtain the same records for everyone at "practically no expense." *Carpenter*, 585 U.S. at 311. Finally, the Court made clear that third-party sharing is not dispositive: "the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection." *Id.* at 309.

II. The First Circuit's expansion of the third-party doctrine warrants review.

Despite *Carpenter*, courts of appeals continue to read this Court's precedents to establish a maximalist third-party doctrine. No matter how the government got the information, no matter how much or how sensitive the information, and no matter how many people it targets, courts continue to hold that the Fourth Amendment offers no protection for information shared with third parties. This case illustrates the problem. It has all the hallmarks of an unconstitutional search that were missing in *Smith* and *Miller*. And it involves an advancing technology, cryptocurrency, that presents new privacy concerns of the sort that this Court has typically sought to protect.

A. This search was worse than the searches in *Smith* and *Miller*.

This Court does not need to overrule the third-party doctrine to correct course here. The search in this case was different in three important respects from the searches in *Smith* and *Miller*.

First, the government coerced Coinbase, the third party to whom Harper entrusted his records. To obtain the cryptocurrency transaction records at issue here, the government served a court-ordered summons on Coinbase, which Coinbase refused. *Coinbase, Inc.*, 2017 WL 5890052, at *8-9; *accord* App.6a-7a. The government then narrowed the summons, and again "Coinbase refused to comply[.]" *Coinbase, Inc.*, 2017 WL 5890052, at *1; *accord* App.7a. Finally, the government filed a request for enforcement and won a

court order forcing Coinbase to produce the documents. *Coinbase, Inc.*, 2017 WL 5890052, at *8-9 ("Coinbase is ORDERED to produce …"). Coinbase complied only under threat of judicial contempt. It did not "betra[y]" Harper's trust like a confidential informant. *Miller*, 425 U.S. at 443. It did not voluntarily cooperate with a "request" like the phone company in *Smith*. 442 U.S. at 737. And it did not give up the records "without protest" like the banks in *Miller*. 425 U.S. at 443. Its use of coercion to obtain private papers should have triggered different constitutional treatment. *See Weeks v. United States*, 232 U.S. 383, 397 (1914) ("the substance of the [Fourth Amendment] offense is the compulsory production of private papers"), *overruled by Elkins v. United States*, 364 U.S. 206 (1960); *see also United States v. Hubbell*, 530 U.S. 27, 55-56 (2000) (Thomas, J., concurring) (explaining traditional protections against such coercive process).

Second, the government's search accessed an unfathomable amount of sensitive information. This court-ordered disclosure covered three full years of account information. *Coinbase, Inc.*, 2017 WL 5890052, at *1-3. Not one day or a few months. *Cf. Smith*, 442 U.S. at 737; *Miller*, 425 U.S. at 437-38. For each customer of Coinbase, the government acquired his social security number and address, along with detailed reports about *all* of his "account activity," including his every transaction. *See Coinbase, Inc.*, 2017 WL 5890052, at *8-9. In total, the government obtained a combined 8.9 million transactions, giving it an "intimate window" into many lives. *Carpenter*, 585 U.S. at 311. It obtained records considerably more intrusive

than one day's telephone numbers, or a handful of financial statements and instruments. *Miller*, 425 U.S. at 438.

"Financial transactions can reveal much about a person's activities, associations, and beliefs." *Cal. Bankers Ass'n v. Schultz*, 416 U.S. 21, 78-79 (1974) (Powell, J., concurring). They reveal things like whether people have "alcohol, drug, and gambling addictions," *Riley*, 573 U.S. at 396, whom their customers are, *City of L.A. v. Patel*, 576 U.S. 409, 424 (2015), whether their purchases suggest "symptoms of disease," *Riley*, 573 U.S. at 395, and whom they associate with politically and religiously, *Carpenter*, 585 U.S. at 311. People already use cryptocurrency for all of these sensitive purposes. *E.g.*, *Cryptocurrencies And Medical Bills: The New Way To Pay For Healthcare?*, Healthcare Bus. Today (Nov. 3, 2022), perma.cc/72S8-DWSS (describing cryptocurrency payments for private healthcare services); The Giving Block, perma.cc/XP9U-GGYE (facilitating cryptocurrency donations to religious and charitable organizations).

And third, the government's inquiry was not tailored to one suspected criminal. It acquired personal account information of 14,355 people. *Coinbase, Inc.*, 2017 WL 5890052, at *2. Those 14,355 were not all likely criminals for whom the government had already established probable cause. They were everyday lawful users of cryptocurrency—people who were not accused of doing anything suspicious, not accused of using cryptocurrency for any illegal purposes, and not accused of failing to properly pay taxes. *See id.* at *4-

*6. The government's action here was a paradigmatic "fishing expedition." *Am. Tobacco Co.*, 264 U.S. at 306.

The First Circuit ruled against Harper because it adopted a maximalist interpretation of *Smith* and *Miller*. According to the First Circuit, this case fell "*squarely* within th[e] 'third party doctrine' line of precedent." App.13a (emphasis added). It was sufficient that Harper "voluntarily divulged information about his Bitcoin transactions to Coinbase." App.18a. The First Circuit read *Carpenter* to apply narrowly to "cell-site location information" and apparently little else. App.15a-18a. The Fourth Amendment, the First Circuit reasoned, would protect Harper's records only if they were created "several times every minute," if it thought that they were less "truly" shared with Coinbase, or if it thought that they involved a more "indispensable" activity. App.15a. The First Circuit acknowledged that Harper's "records may capture some intimate information," but it deemed that concern insufficient to overcome the fact of third-party sharing. App.15a.

The First Circuit's approach reflects a broader trend. In many cases, lower courts have taken *Smith* and *Miller* to create a near-absolute rule that third-party sharing defeats any reasonable expectation of privacy. They have held, for instance, that the government can force a third party to report patients' medical prescription histories, even though the third party promised confidentiality to the patients. *DOJ v. Ricco Jonas*, 24 F.4th 718, 739 (1st Cir. 2022); *see also United States v. Motley*, 89 F.4th 777 (9th Cir. 2023). Apparently going to the doctor is now "assum[ing] the

risk" that the government will take your records. *Ricco Jonas*, 24 F.4th at 739. Likewise, circuits have held that the government can force a third party to track and report a customer's IP history, including reports about which websites the defendant clicks on inside his home. *United States v. Soybel*, 13 F.4th 584, 590 (7th Cir. 2021); *see also United States v. Contreras*, 905 F.3d 853, 857 (5th Cir. 2018). Again, merely because internet services are provided by third parties, a user has "no reasonable expectation of privacy in this data." *Soybel*, 13 F.4th at 594.

Carpenter has barely budged how courts of appeals think about the third-party doctrine. In the courts of appeals, "*Carpenter* did not disturb the third-party doctrine." *Ricco Jonas*, 24 F.4th at 738. Instead, it created a "'narrow' exception" that "applies only to some cell-site location information." *United States v. Trader*, 981 F.3d 961, 967-68 (11th Cir. 2020). As these courts see it, "*Carpenter* refined the third-party doctrine for a specific type of digital data: historical location information as revealed by CSLI." *Soybel*, 13 F.4th at 591-92. In other words, the courts of appeals have, like the First Circuit here, reduced *Carpenter* to its facts and expanded the third-party doctrine beyond its proper scope. Because this case presents a recurring and unfortunate misreading of this Court's precedents, it warrants review.

B. Cryptocurrency technology presents special privacy concerns.

This Court has repeatedly admonished that when "advancing technology" makes searches more intrusive, Fourth Amendment doctrine must recalibrate to

"assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo v. United States*, 533 U.S. 27, 34-36 (2001). Here, the advancing technology of cryptocurrency made this search even more intrusive than it appears on the surface, further counseling against the extension of the third-party doctrine.

Unlike traditional financial transactions, cryptocurrency transactions are recorded on a public ledger visible to anyone. *See* CRS Report, *Cryptocurrency: The Economics of Money and Selected Policy Issues*, at 7 (Apr. 9, 2020), perma.cc/G8UA-SXD6. This public ledger, or "blockchain," lists the details of every cryptocurrency transaction ever made. It includes the sender and receiver, but only by pseudonymous addresses, which are essentially random strings of letters and numbers that are unique to and known only to the users. *See, e.g.*, Bitcoin Glossary, U.S.S.C., perma.cc/H5MY-6DJR. So while any person's transactions are public, onlookers cannot link them to that person unless they can match him to his pseudonymous address. *See* Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, at 6 (2009), perma.cc/5MZP-PAEX.

This privacy model works until someone is forced to reveal their identity. Typically, cryptocurrency users do not need to reveal their identities in connection with their pseudonymous addresses, so their transactions cannot easily be traced to them by unwelcome eyes. But once the government unmasks the identities behind a cryptocurrency transaction, like it did here,

the public-ledger system becomes a tool for surveillance. *See* Nakamoto, *supra*, at 6 ("if the owner of a key is revealed, linking [on the public ledger] could reveal other transactions that belonged to the same owner"). Once the government uncovers the name behind an address, it can search the public ledger to identify every transaction that the person ever made and every transaction that the person will ever make in the future with that address. The person can create another address, but public ledger software and analysts using it can identify and connect different addresses controlled by the same person based on interactions between the addresses. The government already uses these methods to trace cryptocurrency transactions. *E.g.*, *Matter of Search of Multiple Email Accts.*, 585 F. Supp. 3d 1, 8 (D.D.C. 2022); Brief for United States, *United States v. Gratkowski*, 964 F.3d 307 (5th Cir. 2020), at 7-8. ("law enforcement has used these services in numerous past investigations and found it to produce reliable results").

The upshot is that the disclosure of a cryptocurrency address raises heightened privacy concerns not presented by the disclosure of traditional financial transactions. By collecting the cryptocurrency transaction records of 14,355 people, *Coinbase, Inc.*, 2017 WL 5890052, at *8-9, the government effectively accessed transactions indefinitely into the past and future. It can now use the information it collected to review transactions outside of the Coinbase ecosystem and on any other public network where the addresses interact. *See, e.g.*, *Letter to Dep't of Financial Protection and Innovation from Chainalysis*, at 3 (Aug. 2022), perma.cc/F7TC-HSM6 (detailing this ability);

Matter of Search of Multiple Email Accts., 585 F. Supp. 3d at 8 (similar).

The First Circuit acknowledged these heightened privacy concerns but said that the third-party doctrine makes them irrelevant. The court "d[id] not doubt that because digital currency transactions are recorded on a public ledger, exposure of a person's identity opens a potentially wide window into that person's financial activity contained on that ledger." App.17a-18a. It "agree[d] with Harper and his amici" that the government's search here would "pierc[e] the veil of anonymity" to allow it to track unrelated transactions. App.17a n.9. As it explained, "anyone aware of th[e] information" that the government obtained here "can easily ascertain all transactions the person has made using that address—or track future transactions." *Id.* Nonetheless, for the First Circuit, that fact "makes no difference in our conclusion that [Harper] lacked a reasonable expectation of privacy." App.18a n.9.

But when faced with similar concerns caused by new technology, this Court has consistently taken the opposite approach. It has explained that, when "advancing technology" makes a search more intrusive, courts must "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo*, 533 U.S. at 34-35. "[C]hanging technology and social practice often trigger a need for legal adaptation." Kerr, *Foreword: Accounting for Technological Change*, 36 Harv. J. Law & Public Pol'y 403, 403 (2013); *see also* Kerr, *An Equilibrium-Adjustment Theory of the Fourth*

Amendment, 125 Harv. L. Rev. 476, 534 (2011). If Fourth Amendment doctrine did not recalibrate to "the inexorable march of technological progress," then "its guarantees [would] wither and perish." *Warshak*, 631 F.3d at 285.

This Court has therefore sought to limit the "power of technology to shrink the realm of guaranteed privacy." *Kyllo*, 533 U.S. at 34. When new technology would "expose to the government far more" than previous precedents contemplate, this Court has adamantly protected against such exposure. *Riley*, 573 U.S. at 396. For example, although this Court long allowed government agents to surveil someone's home from outside using photography, *see, e.g.*, *Dow Chem. Co. v. United States*, 476 U.S. 227 (1986), it did not allow them to do so using thermal-imaging technology, *see Kyllo*, 533 U.S. at 41. Likewise, although this Court long allowed the government to tail vehicles on public roads, *Jones*, 565 U.S. at 412 (citing *Knotts*, 460 U.S. at 286), it did not allow such tracking remotely with GPS technology, *Jones*, 565 U.S. at 412. And although this Court long allowed government agents to search the contents of items in an arrestee's immediate possession, *see United States v. Robinson*, 414 U.S. 218 (1973), it did not allow such searches of cell phones, a new technology that put an arrestee's personal history and affairs in his immediate possession, *Riley*, 573 U.S. at 396.

This case—where the government acquired three years of cryptocurrency records from 14,355 people—is a crucial case for technological recalibration. Be-

cause of the traceability of cryptocurrency transactions on the public ledger, the search here "expose[d] to the government far more" than an analogous search of traditional bank records. *Riley*, 573 U.S. at 396. It gave the government effectively *all* transactions of 14,355 cryptocurrency users, forever. *See Coinbase, Inc.*, 2017 WL 5890052, at *8-9. The First Circuit's extension of the third-party doctrine to this new context did not recalibrate for the "power of technology to shrink the realm of guaranteed privacy." *Kyllo*, 533 U.S. at 34. Had it done so, it would have ruled differently. Because this case involves heightened privacy concerns presented by new technology, it presents an especially strong opportunity to stop the runaway third-party doctrine.

CONCLUSION

This Court should grant certiorari.

March 28, 2025

J. Abraham Sutherland
106 Connally Street
Black Mtn., NC 28711
(805) 689-4577

Cameron T. Norris
Counsel of Record
Jeffrey S. Hetzel
Zachary P. Grouev
CONSOVOY MCCARTHY PLLC
1600 Wilson Blvd., Ste. 700
Arlington, VA 22209
(703) 243-9423
cam@consovoymccarthy.com

Attorneys for Amicus Curiae