No. 23-1565

UNITED STATES COURT OF APPEALS
FOR THE FIRST CIRCUIT

JAMES HARPER.,

Plaintiff-Appellant,

v.

DANIEL WERFEL, in his official capacity as Commissioner of the Internal Revenue Service; and INTERNAL REVENUE SERVICE,

Defendant-Appellees.

On Appeal from the United States District Court
for the District of New Hampshire

BRIEF FOR DEFI EDUCATION FUND AS AMICUS CURIAE SUPPORTING APPELLANT AND URGING REVERSAL

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

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

Counsel for Amicus Curiae DeFi Education Fund

CORPORATE DISCLOSURE STATEMENT

DeFi Education Fund is a non-profit based in the United States. Counsel for amicus curiae DeFi Education Fund certifies that amicus curiae has no parent corporation and no publicly held corporation owns 10% or more of any stock in amicus curiae.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Rules

Other Authorities

INTEREST OF AMICUS CURIAE

DeFi Education Fund ("DEF") 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. This brief explains important characteristics of cryptocurrency and their Fourth Amendment implications. For example, it explains how the government's collection of cryptocurrency data gives it access to vast amounts of unrelated information, unlike when it collects traditional bank records.

All parties to this appeal have consented to the filing of this amicus curiae brief. No party's counsel or other person except amicus curiae and its counsel authored this

brief or contributed money to fund its preparation or submission. Fed. R. App. P. 29(A)(4)(e).

INTRODUCTION & SUMMARY OF ARGUMENT

This case presents this Court with its first opportunity to consider the Fourth Amendment rights of cryptocurrency users. DeFi Education Fund respectfully urges it to do so with three important considerations in mind.

First, when it comes to Fourth Amendment protections in information held by third parties, district courts should stop treating *Carpenter v. United States* as an aberration or second-class opinion. The district court here denied Jim Harper's Fourth Amendment right to privacy in his cryptocurrency transactions by limiting *Carpenter* to its facts and then exaggerating two older cases that themselves never announced a broad and unqualified rule. But *Carpenter* is the Supreme Court's most recent and authoritative statement of the so-called "third-party" doctrine. 138 S. Ct. 2206 (2018). It reduced the two cases that created that doctrine to "life support." *Id.* at 2272 (Gorsuch, J., dissenting). And those two cases never made the broad claims with which the district court endowed them; they turned on "limit[s]" in numerosity, sweep, and nature. *Smith v. Maryland*, 442 U.S. 735, 742 (1979); *see also United States v. Miller*, 425 U.S. 435, 442-43 (1976). Absent "comparable limitations," which the government cannot show here, *Carpenter* controls. 138 S. Ct. at 2219.

Second, cryptocurrency is not traditional banking. The government's request here was a search under *Carpenter* largely because of features distinctive to cryptocurrency technology, which the district court failed to understand and this brief explains in detail. The district court distinguished *Carpenter* because "virtual currency

exchange records do not reveal similarly intimate details about a user's life," JA084. But they do. Cryptocurrency transactions are traceable on a public ledger, visible to anyone. Users make transactions through pseudonymous addresses. When the government collected the users' information here, it connected their real-life identities to their pseudonymous addresses. It therefore acquired not only the reported information, but also the equivalent of a window into every other transaction by every user. From transactions made on Coinbase, it can now view each person's transactions not made on Coinbase. And from transactions during one time period, it can now view transactions indefinitely into the past and future. The government's request in this case therefore implicated every user's every transaction, now and forever, including their "familial, political, professional, religious, and sexual associations." *Carpenter*, 138 S. Ct. at 2218 (internal quotations omitted). It gave the government a "detailed, encyclopedic, and effortlessly compiled" synopsis of the lives of Harper and 14,354 others. *Id.* at 2216. The government's collection of traditional bank records, by contrast, gives it no similar access. Accordingly, courts cannot treat them as the same under *Carpenter*.

Last, these technological features of cryptocurrency implicate another line of Supreme Court cases. When old precedents meet new technology, courts must "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 (2001). "When confronting new concerns wrought by digital technology," the Court has admonished against "uncritically extend[ing] existing precedents." *Carpenter*, 138 S. Ct. at 2222. So

for example, while the Fourth Amendment does not protect against outside visual surveillance, it does once the government uses thermal-imaging technology. *Kyllo*, 533 U.S. at 35. While it does not protect against manually following a car on public roads, it does once the government uses a GPS tracker. *United States v. Jones*, 565 U.S. 400, 412 (2012). And while it does not protect against searches of items in pockets incident to arrest, it does when those items include modern-day cell phones. *Riley v. California*, 573 U.S. 373, 395 (2014). In every case, the new technology would lead the government to obtain vastly *more information* than earlier cases anticipated, so the earlier cases no longer apply. Therefore, even if this Court thinks that earlier cases allowing searches of bank records would otherwise apply here, the nature of cryptocurrency technology—which allows the government to access unlimited unrelated transactions—requires recalibration.

ARGUMENT

This case presents the question whether, when the federal government collects by force three years of detailed cryptocurrency records for 14,355 Americans, including Harper, it conducts a Fourth Amendment search. The government here collected records of each user's name, social security number, address, and every cryptocurrency transaction over the course of those years. *See United States v. Coinbase, Inc.*, 17-cv-01431, 2017 WL 5890052, at *8-9 (N.D. Cal. Nov. 28); D. Ct. Doc. 30-11 at 3-4. Altogether, the government collected information about *8.9 million* transactions. *Id.* When Harper asserted his rights against the collection of that information, the district court held that

the Fourth Amendment, which "safeguard[s] the privacy and security of individuals against arbitrary invasions by governmental officials," *Carpenter*, 138 S. Ct. at 2213, has nothing to say about this.

Affirming the district court's dim view of the Fourth Amendment would be a mistake. First, this case falls within the prevailing rule that Americans have a reasonable expectation of privacy in information shared with third parties, not the exception carved out by *Smith v. Maryland* and *United States v. Miller*, a pair of older decisions that "did not rely solely on the act of sharing." *Carpenter*, 138 S. Ct. at 2219. Second, the district court's denial of that protection ignored distinctive characteristics of cryptocurrency's blockchain technology, including that the government can use the information that it collected to review every person's unrelated past and future transactions. And third, the implications of this new technology also mean that the Court cannot extend old precedents that fail to "preserv[e]" the same "degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo*, 533 U.S. at 34-35.

I. *Carpenter* is the rule, not the exception.

The "touchstone" Fourth Amendment inquiry is whether a person has a "reasonable expectation of privacy" in the information that the government collects. *California v. Ciraolo*, 476 U.S. 207, 211 (1986) (quoting *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)). If he does, then the government must get a warrant or fall within an exception to collect his information. *Id.* Before the Supreme Court's two decisions in the 1970s, courts recognized that people had reasonable expectations

of privacy even in information shared with third parties. Those two cases—*Smith v. Maryland* and *United States v. Miller*—created an exception to that general rule, but only when the information accessed was "limited" in numerosity, sweep, and nature. *Smith*, 442 U.S. at 742; *see also Miller*, 425 U.S. at 442-43. In *Carpenter*, the Supreme Court further cabined *Smith* and *Miller*. It held that absent "comparable limitations" on the information accessed, "solely . . . the act of sharing [with a third party]" no longer divests a person of his reasonable expectation of privacy. 138 S. Ct. at 2219. The district court here could only rule against Harper by denying *Carpenter* its import and authority.

A. The Fourth Amendment always protected information shared with third parties.

Before *Smith* and *Miller*, people undeniably had Fourth Amendment rights in information like Harper's. The government was forbidden from forcing third parties to disclose information that they held about another person's transactions or affairs. For example, if a person conducted business transactions through the mail, the government could not access those transactions—even through the government's own mail carriers—without a warrant. *Ex parte Jackson*, 96 U.S. 727, 733 (1877). When a person shared his letters with the recipient and various "officials connected with the postal service," the government still could not collect them. *Id.*; *accord* 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) (unlawful "to permit letters to be opened at the discretion of a ministerial officer").

Fourth Amendment doctrine has consistently recognized broad rights against searches of similar information shared with third parties. *See, e.g.*, *United States v. Stokes*, 829 F.3d 47, 52 (1st Cir. 2016) (applying *Ex Parte Jackson* as binding law after *Smith* and *Miller*); *Walter v. United States*, 447 U.S. 649, 658-60 (1980) (holding that government violated Fourth Amendment by reviewing contents of mail opened by unintended third-party recipient *and* voluntarily shared with the government by that third party). Even before *Carpenter*, courts held that the same principles meant the government could not collect the contents of emails, even though they are shared with third-party service providers. *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010). Email users explicitly consent to the third-party providers searching the contents of their emails. *Id.* But that act of sharing does not deprive them of their Fourth Amendment rights in that content. That makes sense. Under standard legal principles, sharing private information with third parties neither constitutes "consent" nor an "assumption of risk" with respect to the government's later search. *Carpenter*, 138 S. Ct. at 2263 (Gorsuch, J., dissenting).

The seminal *Katz v. United States* likewise showed that sharing something with a third party doesn't render it unprotected. *Katz* held that the government conducted a search when it recorded a person's telephone conversations from a "public telephone booth." 389 U.S. at 348. It was widely recognized before and since that, "[a]t the time *Katz* was decided, [third party] telephone companies had a right to monitor calls." *Warshak*, 631 F.3d at 287. They even had a right to monitor calls in exactly the situation

presented in *Katz*, where doing so would "protect [the telephone company] against the improper and illegal use of their facilities." *Bubis v. United States*, 384 F.2d 643, 648 (9th Cir. 1967); *see Katz*, 389 U.S. at 354 ("[caller] was using the telephone in question to transmit gambling information"). And of course, the contents of a telephone call are openly shared with the call's recipient. But granting this "degree of access" to third parties in the phone company and the recipient of the phone call did not eliminate the caller's reasonable expectation of privacy in those contents. *Warshak*, 631 F.3d at 287; *see Katz*, 389 U.S. at 354.

The district court failed to appreciate this background when it dismissed Harper's Fourth Amendment claim. It held that in all circumstances except those involving cell-site location information, a person has no Fourth Amendment rights in what he "turns over to third parties" or "reveal[s] … to another." JA082-83. It did not grapple with any of this history. *Id.* Would the district court overrule *Ex Parte Jackson* and *Katz*? They are pillars of Fourth Amendment law.

B. *Smith* and *Miller* created a narrow exception.

Miller and *Smith* created an exception to the rule otherwise protecting information held by third parties. *See Carpenter*, 138 S. Ct. at 2216 ("th[e] third-party doctrine largely traces its roots to *Miller*"). Although the district court treated *Miller* and *Smith* as unqualified, they were not. They identified rare circumstances under which the government can overcome the general rule that people retain a reasonable expectation

of privacy in matters accessible to third parties. Three factors turned out to be essential to *Miller* and *Smith*.

First, the information accessed in those cases was "limited" in terms of the *amount* of data gathered. *Smith*, 442 U.S. at 742. In *Miller*, the government collected only "two financial statements," "three monthly statements," plus "checks" and "deposit slips." 425 U.S. at 438. The information was hardly more than what could have been in the defendant's pocket. *See Riley*, 573 U.S. at 400 ("someone could have tucked a paper bank statement in a pocket"). The papers covered less than four months of intermittent (at best) activity. *Miller*, 425 U.S. at 438. The government did *not* access a "deep repository" of information, *Carpenter*, 138 S. Ct. at 2218, and *Miller* nowhere said that it could.

In *Smith*, the Court again stressed that the government gathered minimal information. The government collected only the "numbers" dialed from the defendant's landline for a *single day*, and seemingly only a single number. *Smith*, 442 U.S. at 737 (emphasis added). "[L]aw enforcement official[s] could not even determine from the use of a pen register whether a communication existed." *Id.* at 741 (quoting *United States v. New York Tel. Co.*, 434 U.S. 159, 167 (1977)). "Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed [was] disclosed." *Id.* Only upon emphasizing these limits did the Court conclude that the collection was not a search. *Id.* It was essential that "telephone call logs reveal little in the way of 'identifying information.'" *Carpenter*,

138 S. Ct. at 2219 (quoting *Smith*, 442 U.S. at 742). They were the opposite of "detailed" or "encyclopedic." *Id.* at 2216.

Second, the information accessed in *Miller* and *Smith* was limited in the number of people affected. Both involved targeted, constrained inquiries, directed at a single person. They were not and could not be scaled. In *Miller*, the government got bank records of one man because they had discovered enormous evidence of criminal wrongdoing in his warehouse. 425 U.S. at 437. In *Smith*, the government got one day's worth of phone numbers from one man because he was visually identified as the person making calls in connection with a crime. *Smith*, 442 U.S. at 737.

Neither case went any further. They did not involve "dragnet type law enforcement practices." *United States v. Knotts*, 460 U.S. 276, 284 (1983). They did not "direct fishing expeditions into private papers on the possibility that they may disclose evidence of crime." *FTC v. Am. Tobacco Co.*, 264 U.S. 298, 306 (1924) (Holmes, J.). They did not "run[] against everyone." *Carpenter*, 138 S. Ct. at 2218; *see also id.* at 2219 ("shifts in digital technology … made possible the tracking of not only Carpenter's location *but also everyone else's*" (emphasis added)). They did not involve information "effortlessly compiled." *Id.* at 2216. Allowing the government to collect the information in those limited, targeted circumstances therefore did not upset the "appropriate balance between … legitimate privacy interests and the government's need to search." *Wood v. Clemons*, 89 F.3d 922, 929 (1st Cir. 1996).

Third, *Smith* and *Miller* were limited in the *nature* of the information revealed. They did not reveal the "privacies of life." *Carpenter*, 138 S. Ct. at 2217 (internal quotations omitted). And they did not reveal "familial, political, professional, religious, and sexual associations." *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). To the contrary, *Smith* involved mere numbers dialed, without any information about why they were dialed or what was said (if anything). The Court emphasized that "telephone call logs reveal little in the way of 'identifying information,'" let alone intimate information. *Carpenter*, 138 S. Ct. at 2219 (quoting *Smith*, 442 U.S. at 742). *Miller* likewise involved checks that the Court emphasized were "not confidential communications but negotiable instruments to be used in commercial transactions." 425 U.S. at 442. They therefore did not "provid[e] an intimate window into a person's life." *Carpenter*, 138 S. Ct. at 2217.

Smith and *Miller* never purported to control the collection of information that was not "limited" along these dimensions. *Smith*, 442 U.S. at 742.

C. *Carpenter* confirmed the prevailing rule.

Carpenter further cabined *Smith* and *Miller* and now expresses the prevailing rule. Though the district court gave *Smith* and *Miller* overwhelming weight and limited *Carpenter* to its facts, the Supreme Court in *Carpenter* viewed things the opposite way. It explained that *Smith* and *Miller* "did *not* rely solely on the act of sharing." 138 S. Ct. at 2219 (emphasis added). *But see* JA082 (district court treating them as if they did). *Carpenter* read *Smith* and *Miller* to be limited to "telephone numbers and bank records."

Id. at 2216. It then held that their outcome could be "extend[ed]" to other third-party circumstances *only if* those circumstances involved "comparable limitations." *Id.* at 2219.

Carpenter held that cell-site location information was protected because it did not involve "comparable limitations." *Carpenter*, 138 S. Ct. at 2219. The cell-site location information consisted of reports, about every 15 minutes, about a cell phone's general location, usually accurate only to within a few square miles. *Id.* at 2212. The case involved two batches of information, one of two days and another of 127 days. *Id.* at 2212. The information was unequivocally shared with—indeed, compiled by—the third-party phone company. *Id.* at 2212. But it was still protected. The information was "detailed, encyclopedic, and effortlessly compiled." *Id.* at 2216. It could give the government access to a "deep repository of historical location information." *Id.* at 2218. It could do so against millions of Americans at "practically no expense." *Id.* And location information, unlike phone numbers or business checks, could "revea[l] not only [the person's] particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Id.* at 2217 (quoting *Jones*, 565 U.S. at 415). Therefore, "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 2217.

It is impossible to look at *Smith* and *Miller* the same way after *Carpenter*. Three dissenting Justices characterized it as a "reinterpretation of *Miller* and *Smith* [that] will have dramatic consequences for law enforcement, courts, and society as a whole." *Carpenter*, 138 S. Ct. at 2233 (Kennedy, J., joined by Thomas and Alito, J.J., dissenting).

The fourth characterized it as leaving "*Smith* and *Miller* on life support." *Id.* at 2272 (Gorsuch, J., dissenting). The Court has not applied *Smith* or *Miller* since.

II. This case falls within the *Carpenter* rule.

This case falls within the *Carpenter* rule, not the *Smith* and *Miller* exception. When the government forced the disclosure of 14,355 Americans' identifying information and crypto transactions over a three-year period, it violated their reasonable expectations of privacy. It not only collected drastically more and broader information than those cases involved, but also acquired enough information to track users' unrelated transactions, including off-Coinbase transactions that are indelibly recorded on the blockchain, infinitely into the past and future. Because "[f]inancial transactions can reveal much about a person's activities, associations, and beliefs," *Cal. Bankers Ass'n v. Shultz*, 416 U.S. 21, 78-79 (1974) (Powell, J., concurring), the users had a reasonable expectation of privacy in this data.

A. The data collection was broad and intrusive.

Some of the reasons this case falls within *Carpenter* are obvious. The government acquired *three full years* of account information. *United States v. Coinbase, Inc.*, 2017 WL 5890052, at *8-9 (N.D. Cal. Nov. 28). Not one day or a few months. *Smith*, 442 U.S. at 737; *Miller*, 425 U.S. at 438. It acquired that information from 14,355 people. *Coinbase, Inc.*, 2017 WL 5890052, at *8-9. Not a lone person. *Smith*, 442 U.S. at 737; *Miller*, 425 U.S. at 438. The targets were people like Harper, who was not accused of doing anything suspicious, using his cryptocurrency for any illegal purposes, or failing to properly pay

taxes. JA076. In fact, it is statistically unlikely that the data collected was based on suspicious activity because it is estimated that less than 0.2% of cryptocurrency uses are unlawful. CRS Report, *Cryptocurrency: Selected Policy Issues*, 19 (Feb. 15, 2023), perma.cc/4NVA-7CM2. These 14,355 people were unlike the conspicuous criminals in both *Smith* and *Miller*. And the government acquired an enormous amount of account information from each person. In addition to each user's social security number and address, it acquired detailed reports about *all* their "account activity," including their every transaction. *See Coinbase, Inc.*, 2017 WL 5890052, at *8-9. It acquired information about a combined *8.9 million* transactions. *Id.* That's a far cry from one telephone number, or from "two financial statements," "three monthly statements," plus some "checks" and "deposit slips." *Miller*, 425 U.S. at 438.

The district court denied Harper's Fourth Amendment claim because it was "*closely analogous to*" *Miller* and *Smith*. JA084. Far from close, his case is the opposite of *Smith* and *Miller*. The government cast a "dragnet." *Knotts*, 460 U.S. at 284. It went on a "fishing expeditio[n]." *Am. Tobacco Co.*, 264 U.S. at 306. Its collection "r[an] against everyone." *Carpenter*, 138 S. Ct. at 2218. So on its face, it fell beyond the reach of *Miller* and *Smith*.

B. Distinctive characteristics of cryptocurrency make this a search.

But due to unique characteristics of cryptocurrency, the collection here was much broader and more intrusive even than it first appears. The district court bypassed these characteristics, but they are central to the *Carpenter* analysis.

Cryptocurrency transactions are made through pseudonymous addresses. *See* CRS Report, *Introduction to Cryptocurrency* 1 (May 23, 2023), perma.cc/M377-BXXP. To transact with each other, cryptocurrency users select a random number between 1 and approximately 2^{256} to create a "private key," which, when coupled with a "public key," form a "wallet" that allows the user to interact with a blockchain. A wallet's public key is a cryptographically-generated string of letters and numbers—like "AJG163" but longer—that people colloquially refer to as an "address." Users send and receive cryptocurrency through their addresses.

Addresses must be pseudonymous because cryptocurrency transactions are *public*. *See* CRS Report, *Cryptocurrency: The Economics of Money and Selected Policy Issues* 7 (Apr. 9, 2020), perma.cc/G8UA-SXD6. Unlike traditional financial transactions, cryptocurrency transactions are publicly recorded on an immutable ledger that is visible to anyone. *Id.* This public ledger, or "blockchain," lists every cryptocurrency transaction ever made on that network. It lists the quantity of cryptocurrency transferred and the time of the transaction. And it lists the sender and receiver, but only by their pseudonymous addresses, or public keys. *See, e.g.*, Bitcoin Glossary, U.S.S.C., perma.cc/H5MY-6DJR.

When a person makes a cryptocurrency transaction, the transaction is posted to the public ledger. But because it is posted using pseudonymous addresses, only the user typically knows that the transaction is his or hers. Onlookers and the government can identify transaction participants only if they can match a public key to an identifiable

person. *See* Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, at 6 (2009), perma.cc/5MZP-PAEX. Because people do not need to identify themselves in connection with the pseudonymous addresses, they can ensure that their transactions, although posted publicly, cannot easily be traced to them by unwelcome eyes.

But this works only until someone is compelled to identify an address as his. Once that happens, the public-ledger system actually becomes a tool for complete surveillance. *See* Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, at 6 (2009), perma.cc/5MZP-PAEX ("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 knows that an address belongs to someone, it can identify every transaction that the person ever made and every transaction that the person will ever make in the future with that public key. After all, those transactions will all be posted and searchable on the public ledger. And while a person can create another address, public ledger software and analysts using it can easily identify and connect different addresses controlled by the same person based on interactions between the addresses. *E.g.*, *Matter of Search of Multiple Email Accts.*, 585 F. Supp. 3d 1, 8 (D.D.C. 2022) (detailing ledger analysis).

The upshot is that when the government forces the disclosure of someone's cryptocurrency addresses, *all other limits become meaningless*. By collecting a cryptocurrency transaction record or address, the government not only collects the reported information, but also gets a surveillance monitor that tracks a user's every transaction,

both in the past and continuing into the future. That is what the government did here.[1] For every one of the 14,355 users whose addresses it collected, the government can therefore now use its knowledge of each person's address to review the public ledger and identify all their other, unrelated transactions. It can even review their transactions outside of the Coinbase ecosystem and on any other public network where the address interacts. *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). If Jim Harper or anyone else transferred money to another public address, off-Coinbase, to make a private transaction, the government would now be able to identify that transaction—and all future transactions associated with that second address—as his.

For the same reason, the government can also use this information to access transactions at any time, past or future. The government is not at all constrained to the formally requested transactions from 2013 to 2015. Because the ledger is public, all the government needs is to connect the addresses with identifying information. With that in hand, the government can simply search for the same addresses on the public ledger before and after its date range. The court's order against Coinbase might as well have said that it must produce all of those 14,355 users' transactions for all time. *Cf. Carpenter*,

[1] The government collected "transaction logs" for every user, *Coinbase*, 2017 WL 5890052, at *8-9, which it acknowledged include the hashes that identify transactions on the public ledger.

138 S. Ct. at 2218 ("the retrospective quality of the data here gives police access to a category of information otherwise unknowable").

These implications doom the government's actions under *Carpenter*. The government has collected *all* transactions, now and forever, of 14,355 cryptocurrency users. *See Coinbase*, 2017 WL 5890052, at *8-9. "Financial transactions can reveal much about a person's activities, associations, and beliefs." *Cal. Bankers Ass'n*, 416 U.S. at 78-79 (Powell, J., concurring). They reveal "familial, political, professional, religious, and sexual associations." *Carpenter*, 138 S. Ct. at 2217. They will reveal "intimate" activities. *Kyllo*, 533 U.S. at 37. They reveal things like whether people have "alcohol, drug, and gambling addictions," *Riley*, 573 U.S. at 396, who their customers are, *City of Los Angeles 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*, 138 S. Ct. at 2217. 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). A collection of cryptocurrency account information is therefore a request for "an intimate window into a person's life." *Carpenter*, 138 S. Ct. at 2217. And the government collected that information here on an incalculable scale without any individualized suspicion.

Anyone can view and confirm for themselves how this works. For the popular cryptocurrency "ether," for example, all transactions can be viewed on a public-ledger explorer such as etherscan.io. A recent sample is viewable in the "Latest Transactions" section on the homepage. When you click on any transaction, you can see the pseudonymous addresses of the participants, which allows you to also see any of their other transactions. Collecting the real-life identities behind those pseudonymous addresses allows the government to determine a person's every activity.

None of this is unduly speculative. Courts deciding Fourth Amendment limits *must* take into account whether the information that the government gathers "could, in combination with other information," produce the sort of "detailed" record that triggers protection. *Carpenter*, 138 S. Ct. at 2218. In fact, the government already tracks cryptocurrency activities in the attempt to link people to transactions that it finds on public ledgers. It has enlisted small armies of agents and contractors to "analyz[e] blockchain and de-anonymiz[e] [crypto] transactions" to be "able to track, find, and work to seize crypto." Moore, *Operation Hidden Treasure Is Here. If You Have Unreported Crypto, Get Legal Advice*, Forbes (Mar. 6, 2021), perma.cc/642S-X729. When it ascertains identities behind addresses, it uses that information to link them to all their other, unrelated transactions. *E.g., Matter of Search of Multiple Email Accts.*, 585 F. Supp. 3d at 8 (explaining how cryptocurrency "anonymizing techniques fail when pitted against algorithms that analyze transactions on the blockchain"); Statement of Facts, *United States v. Lichtenstein*, 1:23-cr-00239, Doc. 1-1, 3-6, 15-16 (D.D.C. Feb. 7, 2022) (detailing

ledger analysis); 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"); *155 Virtual Currency Assets*, 20-cv-2228, 2021 WL 1340971, at *2 (D.D.C. Apr. 9) (similar).

And while some everyday or sensitive cryptocurrency uses might be nascent today, "the rule the Court adopts 'must take account of more sophisticated systems that are already in use or in development.'" *Carpenter*, 138 S. Ct. at 2218 (quoting *Kyllo*, 533 U.S. at 36); *see also Riley*, 573 U.S. at 395 ("We expect that the gulf between physical practicability and digital capacity will only continue to widen in the future."). If they are not already, ordinary uses of cryptocurrency to conduct personal affairs are on a trajectory to become mainstream. Devon, *Nearly 75% of Retailers Plan to Accept Cryptocurrency Payments Within the Next 2 Years*, CNBC (July, 29, 2022), perma.cc/76HX-T8Q3; Denton, *Visa and PayPal Could Fall Behind Crypto Dollars. Why That Matters*, Barron's (Aug. 23, 2023), perma.cc/JZX9-YSDG; Reeves, *46 Million Americans Now Own Bitcoin, as Crypto Goes Mainstream*, Newsweek (May 11, 2021), perma.cc/ES26-YC27; CRS Report, *Introduction to Cryptocurrency* 1 (May 23, 2023), perma.cc/M377-BXXP. The rule today will affect the lifetime of cryptocurrency users' privacy.

When the district court distinguished *Carpenter* because "virtual currency exchange records do not reveal similarly intimate details about a user's life," JA084, it was just plain wrong. At a minimum, this Court should reverse so the district court can decide at summary judgment—and with the benefit of discovery—how to account for

these implications, which will confirm that the government's collection of information here was a "search" under *Carpenter*.[2]

III. Technological recalibration requires protection of cryptocurrency data.

Another line of Supreme Court precedent separately counsels reversal. When confronted with "advancing technology," courts must recalibrate Fourth Amendment protections if needed to "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. The Supreme Court has stated and applied this limitation many times. "When confronting new concerns wrought by digital technology," courts must refuse "to uncritically extend existing precedents." *Carpenter*, 138 S. Ct. at 2222. Cryptocurrency presents especially acute privacy concerns because, thanks to the features of blockchain technology described above, accessing superficially limited records unlocks an unprecedented trove of unrelated past and future records. But despite the new implications of cryptocurrency technology, the district court uncritically relied on traditional-finance precedents like *Miller* to deny Harper's Fourth Amendment claim. JA083-84.

[2] The Court should not uphold the search on the basis that it was "reasonable." *See* JA089-92. The district court acknowledged that the government did not have a warrant or meet "an exception to the warrant requirement per se." JA089. It also acknowledged that neither the Supreme Court nor this Court has ever held that the IRS "third-party summons procedure" would satisfy the Fourth Amendment if it were a search. JA089-90. It would not. *United States v. Tiru-Plaza*, 766 F.3d 111, 115 (1st Cir. 2014) ("Warrantless searches are *per se* unreasonable, unless they fall within a well-defined and specifically enumerated exception to the warrant requirement.").

"It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." *Kyllo*, 533 U.S. at 33-34. "[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 (2013); *see also* Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 Harv. L. Rev. 476, 534 (2011). In response to changing technology, the Supreme Court has therefore sought to limit the "power of technology to shrink the realm of guaranteed privacy." *Kyllo*, 533 U.S. at 34. In so doing, it has instructed courts to "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Id.* at 34-35. When new technology would "expose to the government far more" than previous precedents contemplate, Fourth Amendment rules must recalibrate to protect against that exposure. *Riley*, 573 U.S. at 396. 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.

The Supreme Court has applied technological recalibration time after time. In each circumstance, the Court has refused to allow the government to collect information based on old precedents where new technology would vastly increase the amount of information that it can collect.

Outside surveillance meets thermal imaging. Under old Fourth Amendment precedents, government agents could surveil someone's home from outside. *E.g.*, *Dow*

Chem. Co. v. United States, 476 U.S. 227 (1986). "Visual surveillance was unquestionably lawful." *Kyllo*, 533 U.S. at 31. But the cases allowing outside surveillance did not anticipate thermal-imaging technology, which allows government agents sitting outside to detect what is happening within a home based on heat patterns. In *Kyllo*, the Supreme Court refused to extend its original precedents in the context of this new technology. *Id.* "The Agema Thermovision 210 might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath." *Id.* at 121. Extending the previous precedents, the Court held, "would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment." *Id.* at 34. So those precedents gave way.

Vehicle tailing meets GPS tracking. Under old Fourth Amendment precedents, government agents could always tail vehicles on public roads in-person from their own vehicles. *See Jones*, 565 U.S. at 412 (citing *Knotts*, 460 U.S. at 286). The Supreme Court has said that the government could follow cars on public roads even with large teams of agents and multiple vehicles. *Id.* But the precedents allowing in-person tailing did not anticipate GPS technology, which allows the government to track cars' movements for an extended period of time without actually following them. *Id.* In *Jones*, the Supreme Court refused to extend its original precedents in the context of this new technology. *Id.*

Search incident to arrest meets cell phones. Under old Fourth Amendment precedents, government agents could always search the contents of items on an arrestee's person. *See Chimel v. California*, 395 U.S. 752 (1969). That would include, for

example, the contents of a wallet, cigarette pack, or anything else in his pocket. *United States v. Robinson*, 414 U.S. 218 (1973). But the precedents allowing searches incident to arrest did not anticipate cell phones, which put an arrestee's personal history and affairs in his pocket. In *Riley*, the Supreme Court refused to extend its original precedents to allow searches incident to arrest of this new technology. When it was suggested that searches of physical items and cell phones are the same, the Court said "[t]hat is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together." *Riley*, 573 U.S. at 378.

Other examples abound. *Compare Lopez v. United States*, 373 U.S. 427, 438 (1963) (in-person eavesdropping constitutional), *with Katz* (electronically-aided remote eavesdropping unconstitutional); *compare Smith*, 442 U.S. 735 (access to rudimentary phone-company call records constitutional), *with Carpenter*, 138 S. Ct. 2206 (access to sophisticated phone-company location records unconstitutional).

Financial-record collection meets cryptocurrency technology. In considering the Fourth Amendment rights of cryptocurrency users, this Court should follow this pattern. Even if the Court concludes that the government could acquire three years of bank records from 14,355 people under *Miller*, the nature of cryptocurrency technology alone generates privacy concerns not contemplated by *Miller*. Cryptocurrency technology "expose[s] to the government far *more*" than the explicitly accessed transactions. *Riley*, 573 U.S. at 397. The government accesses unrelated and separate

transactions. And it accesses transactions for all time moving forward. When the government accessed Miller's bank records, it did not acquire the ability to see every time he used money or the deposits he would make ten years later. This Court must "contend with the seismic shifts in digital technology," by which the government *does* acquire those abilities when it accesses the Coinbase records of Harper and those like him. *Carpenter*, 138 S. Ct. at 2217. Although the district court uncritically extended *Miller* to this new context, this Court should not. Otherwise, the Fourth Amendment's guarantees "will wither and perish." *Warshak*, 631 F.3d at 285.

CONCLUSION

The district court's judgment should be reversed.

Respectfully submitted,

s/ Cameron T. Norris

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

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

Counsel for Amicus Curiae DeFi Education Fund

CERTIFICATE OF COMPLIANCE

This brief complies with the Rules because, excluding the parts that can be excluded, it contains 6,303 words; and it has been prepared in a proportionally spaced face using Microsoft Word 2016 in 14-point Garamond font.

Dated: October 20, 2023 *s/ Cameron T. Norris*

CERTIFICATE OF SERVICE

I hereby certify that on October 20, 2023, I electronically filed the foregoing document with the United States Court of Appeals for the First Circuit by using the CM/ECF system. Counsel for all parties are registered as ECF Filers and they will be served by the CM/ECF system.

Dated: October 20, 2023 *s/ Cameron T. Norris*