No. 23-1565

In the United States Court of Appeals for the First Circuit

JAMES HARPER,

Plaintiff-Appellant,

v.

DANNY WERFEL, IN HIS OFFICIAL CAPACITY AS COMMISSIONER OF THE INTERNAL REVENUE SERVICE; INTERNAL REVENUE SERVICE; JOHN DOE IRS AGENTS 1-10,

Defendants-Appellees,

AMICUS CURIAE BRIEF OF COIN CENTER IN SUPPORT OF THE PLAINTIFF-APPELLANT JAMES HARPER & REVERSAL

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW HAMPSHIRE, CONCORD
NO. 1:20-CV-00771-JL, JUDGE JOSEPH N. LAPLANTE

EDWARD M. WENGER
JOHN CYCON
emwenger@holtzmanvogel.com
jcycon@holtzmanvogel.com

HOLTZMAN VOGEL BARAN TORCHINSKY & JOSEFIAK PLLC
2300 N Street NW, Suite 643A
Washington, DC 20037

(202) 737-8808 (phone)

(540) 341-8809 (facsimile)

Counsel for Amicus Curiae Coin Center

CORPORATE DISCLOSURE STATEMENT.

Pursuant to Rules 26.1(a) and 29(a)(4)(A) of the Federal Rules of Appellate Procedure, Amicus Curiae Coin Center states that it is a not-for-profit corporation, does not have a corporate parent, does not issue stock, and no publicly held corporation owns 10 percent or more of it.

/s/ Edward M. Wenger
EDWARD M. WENGER

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

Rules

Constitutional Provisions

STATEMENT OF IDENTITY AND INTEREST OF AMICUS CURIAE[1]

Coin Center is an independent, nonprofit research center focused on the public policy issues facing cryptocurrencies like Bitcoin and others. Coin Center's mission is to build a better public understanding of these technologies and to promote a regulatory climate that preserves the freedom to innovate using blockchain technologies. Coin Center often produces and publishes policy research from respected academics and experts, educates policymakers at all levels of government and the media about blockchain technology, and promotes sound public policy. For all these reasons, Coin Center offers the following to assist the Court as it considers the novel constitutional and statutory issues presented here.

[1] Pursuant to Federal Rule of Appellate Procedure 29(a)(2), counsel for both the Appellant and the Appellees have provided consent for Amicus Curiae Coin Center to submit this brief for the Court's consideration. No party's counsel authored this brief in whole or in part, and no one besides Amicus Curiae contributed money to fund the brief's preparation or submission.

INTRODUCTION & SUMMARY OF THE ARGUMENT

Cryptocurrencies, which include Bitcoin, Ethereum, and similar technologies, provide a medium for payments, savings, and other economic activity that differ in considerable ways from traditional means of currency exchange. Thanks to digital software with fixed rules of operation, cryptocurrency facilitates the transfer of value without reliance on a "middleman," like a bank or other financial institution. It allows people to transact with each other directly, securely, and privately. And it now bolsters the American economy. Some 59 million Americans already use it, and this creates jobs, drives economic growth, and spurs innovation.

Cryptocurrency is far from perfect. Like the early days of the internet, there are growing pains as cryptocurrency users learn, adjust, and explore the possibilities of this new technology. But ultimately, cryptocurrency, more than any method before it, allows people to transact without ceding their privacy to others.

This point is critical, and it underscores the district court's error. Cryptocurrency users can rest assured that, so long as they do not share their personal identifying information in a way that could link them to their cryptocurrency public addresses, *nobody in the world* can see or publicize what they choose to do with their assets. They do not have to share their credit-card numbers with every stranger with whom they transact. They do not have to share their personal identifying information with financial institutions. They need not subject their every transaction to the

supervision and approval of a bank that may not share their interests or their values. In other words, cryptocurrency users have developed and adopted a technology that allows them to conduct their affairs with genuine personal agency and privacy.

Cryptocurrency technology has many additional features and advantages. It allows people to transfer value across long distances without meeting in person and without middlemen. It secures transactions with mathematically robust systems that guarantee the validity and irreversibility of every transaction. It allows people to protect against inflation by using a store of value whose supply cannot be increased except according to predetermined formulas. And it has empowered impoverished people in developing countries who lack access to credit cards and bank accounts.[2] For instance, Venezuelans have written that cryptocurrency sustained them amid economic turmoil.[3] And human rights advocates say that "when currency catastrophes struck Cuba, Afghanistan, and Venezuela, Bitcoin gave our compatriots refuge."[4]

---

[2] Tamara White & Abraham White, *Figure of the Week: The Rapidly Increasing Role of Cryptocurrencies in Africa*, BROOKINGS (Jan. 27, 2022), *available at* brook.gs/3rXkT2v; *Bitcoin Adoption and Its Impacts on the Developing World*, THE GUARDIAN (NIGERIA) (Oct. 28, 2021), *available at* bit.ly/38vSSIF; Caitlin Ostroff & Jared Malsin, *Turks Pile Into Bitcoin and Tether to Escape Plunging Lira*, WALL ST. J. (Jan. 12, 2022), *available at* on.wsj.com/3auskZj.

[3] Carlos Hernández, *Bitcoin Has Saved My Family*, N.Y. TIMES (Feb. 23, 2019), *available at* nyti.ms/3mlajiV.

[4] Letter from Ire Aderinokun, et al. to Congress in Support of Responsible Crypto Policy (Jun. 7, 2022), *available at* bit.ly/3ziQQad.

At bottom, cryptocurrency serves, and will continue to serve, a vital and vibrant role throughout the globe. But if the district court's order is allowed to stand, and if the IRS can continue to access information related to cryptocurrency transactions without first obtaining a warrant, these advancements will be all for naught.

ARGUMENT

I. CRYPTOCURRENCY WAS DELIBERATELY CONCEIVED TO FACILITATE PRIVACY IN MONETARY TRANSACTIONS.

Cryptocurrency was designed to ensure that every person who wants to conduct financial transactions using digital currency rather than conventional currency can do so. In so doing, it was designed to ensure that the parties to those financial transactions willnenjoy the utmost level of privacy. This point, fundamental to how cryptocurrency operates, was lost on the district court judge, which in turn drove its mistaken dismissal of Mr. Harper's lawsuit.

The district court's error was in assuming that cryptocurrency exchanges and traditional bank transactions are an apples-to-apples comparison. They are, however, nothing of the sort. While typical bank transactions do indeed involve the transfer of personal identifying information to a third party (i.e., a bank), a quick description of the cryptocurrency process is warranted to show how and why the district court went astray.

Cryptocurrency transactions are recorded on public ledgers. These public ledgers, available for viewing online, list alphanumerical "addresses" associated with the participants in cryptocurrency transactions. They *do not*, however, reveal any other information (particularly private or personal identifying information) about senders and recipients. In other words, cryptocurrency transactions are uniquely private, and the parties to a cryptocurrency transaction have an expectation that this privacy will be maintained.

A cryptocurrency program consists of a system of fixed rules of operation designed to facilitate secure and reliable transactions. Any given cryptocurrency's rules may vary, but they tend to share common features. Cryptocurrency (generally speaking) operates using open-source code, which is a computer program that anyone can view, copy, and use without the need to buy it or seek a license. No single person or corporation creates or guarantees the operation of this technology. A person who wants to use cryptocurrency may do so simply by downloading and operating the program on his computer.

This point is critical. A cryptocurrency user *does not need* to share his personal identifying information, such as his name, address, and taxpayer ID, with *anyone* (including a financial institution) to use the technology. He need not provide it to a bank or similar middleman, because the technology eliminates the need for such

middlemen. Indeed, he need not share his identifying information even with the parties with whom he transacts.

After downloading the program, a person generates a "private key," which is a random but unique string of several letters and numbers. This key is generated by the program that person is using, and it is unique to that person. Unless he shares it or unless his computer is stolen or hacked, nobody else has access to it. A person's "private key" is mathematically linked to a "public address," which is another string of letters and numbers. The address is similarly unique to the person. In some ways, a "public address" is like a username, and a "private key" is like a password.

To conduct a cryptocurrency transaction, a receiver provides a sender with his public address. The sender writes a transaction message to that public address, which specifies the quantity of cryptocurrency that he is sending (e.g., one bitcoin). The sender then digitally signs that message with his private key to show that he is authorizing the transfer.

Other users of the cryptocurrency then review and validate the transaction message through a process called "mining." These "miners" check that the message is correctly signed and that the public address sending the information has sufficient cryptocurrency to fund the transaction. Critically, miners do not have *any* personal or business relationships with other users—and they do not have any information except for the public addresses of the cryptocurrency-transaction participants. In

fact, their payment comes in the form of an automatic cryptocurrency receipt in exchange for any mathematically correct work they perform reviewing and validating transactions.

The mining process results in a public listing of the transaction on a public ledger. That public listing, however, includes no information other than the public addresses of the sender and receiver, the quantity transferred, and the time of the transaction. While anybody can view any transaction on the public ledger, no one can (in the normal course) link the transactions on the public ledger with any particular individual's identity. The public ledger shows a series of transactions by public addresses that could (as far as the public knows) belong to anybody in the world. So, when a person's transactions are posted to the public ledger, she may be the only one who knows that those transactions are hers.

To illustrate the cryptocurrency transactional process, imagine a cryptocurrency user named Bob. Bob's private key is "BBB," and his address is "XYZ123." So long as Bob does not tell anybody that he controls that cryptocurrency address, nobody will know.

Bob uses his cryptocurrency address to engage in a transaction with another user, Alice. Alice's cryptocurrency address is "ABC555." Bob signs a message with his corresponding private key, "BBB," to authorize the transaction. Miners will then validate Bob's signature to complete the transaction. They will make sure that Bob

used the correct private key and that Bob's key controlled the amount that he intended to send. If the signature is valid, then the public ledger will list Bob and Alice's transaction. The format of the listing may vary, but it will look something like this:

[Date and time] [Amount] XYZ123 → ABC555.

Anybody can see that listing on the public ledger. Bob and Alice can both confirm their transaction on the public ledger because they know that those two addresses belong to them. But to anyone who does not know to whom those addresses belong, the listing would simply show two random addresses. Bob and Alice may choose to keep their addresses to themselves and thereby keep their transactions private.

As cryptocurrency has grown in popularity, totalitarian governments around the world began to crack down on it. The Chinese government banned banks from participating in transactions relating to cryptocurrency in 2013. It then threatened to label Bitcoin mining an "undesirable" industry and phase it out of existence. It began blocking websites that offered cryptocurrency trading services. And finally, in 2021, it outright banned all cryptocurrency trading and mining. *See* Andrey Sergeenkov, *China Crypto Bans: A Complete History*, CoinDesk (Sep. 29, 2021), *available at* bit.ly/38HVEuz.

When Canadian Prime Minister Justin Trudeau punished truckers for demonstrating against his vaccine mandates, he singled out cryptocurrency and sought to freeze the cryptocurrency activities of his opponents (because cryptocurrency is not controlled by any central government or bank, Prime Minister Trudeau's efforts were only partly effective). *See* Aoyon Ashraf & Danny Nelson, *Canada Sanctions 34 Crypto Wallets Tied to Trucker 'Freedom Convoy'*, YAHOO! News (Feb. 16, 2022), *available at* yhoo.it/39eDIrT. The Iranian government has banned cryptocurrency mining multiple times, purportedly to save electricity. *See* Yasno Haghdoost & Arsalan Shahla, *Iran Orders Crypto-Mining Ban to Save Power During Winter Crunch*, BLOOMBERG (Dec. 28, 2021), *available at* bloom.bg/3v4QKR5. A handful of other governments have followed suit and banned it entirely. *See* Marco Quiroz-Gutierrez, *Crypto Is Fully Banned in China and 8 Other Countries*, FORTUNE (Jan. 4, 2022), *available at* bit.ly/3LmhFh3.

Meanwhile, cryptocurrency has helped support pro-freedom and pro-democracy protesters and communities around the world.[5] Human rights activists

[5] Adriana Hamacher, *Hong Kong Protests Are Accelerating Bitcoin Adoption*, YAHOO! (Sep. 2, 2019), *available at* yhoo.it/3wIowuN; Alex Gladstein, *In the Fight Against Extremism, Don't Demonize Surveillance-Busting Tools like Signal and Bitcoin*, TIME (Jan. 26, 2021), *available at* bit.ly/3Gbpc07; Colin Harper, *Nigerian Banks Shut Them Out, So These Activists Are Using Bitcoin to Battle Police Brutality*, COINDESK (Oct. 16, 2020), *available at* bit.ly/38BhEaR; Eamon Barrett, *Ukraine Tweeted It Was 'Now Accepting Cryptocurrency Donations.' In two days, $12 Million Worth of Bitcoin, Ethereum, and USDT Poured in*, FORTUNE (Feb. 28,

from around the globe have attested that "[w]hen crackdowns on civil liberties befell Nigeria, Belarus, and Hong Kong, Bitcoin helped keep the fight against authoritarianism afloat." Letter from Ire Aderinokun, et al., *supra* n.4. As one freedom-fighting Ukrainian explained, cryptocurrency "literally saved the lives of my friends and many Ukrainians. Without it, we would not have been able to raise money so quickly to pay for protective equipment for soldiers in the early days of the Russian invasion." *Id.*; *see also* Jillian Deutsch & Aaron Eglitis, *Putin's Crackdown Pushes Independent Russian Media Into Crypto*, BLOOMBERG (May 10, 2022), *available at* bloom.bg/3zsX6fL.

II. BECAUSE THE PARTIES TO A CRYPTOCURRENCY TRANSACTION ARE THE ONLY ONES TO EXCHANGE PERSONAL INFORMATION, THEY HAVE A FOURTH AMENDMENT PROTECTED REASONABLE EXPECTATION OF PRIVACY IN THAT INFORMATION.

The above reveals a self-evident point—individuals who use cryptocurrency have a reasonable expectation of privacy that the Fourth Amendment protects. The Fourth Amendment enshrines "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. The founding generation crafted the Fourth Amendment as a "response to the reviled 'general warrants' and 'writs of assistance' of the colonial

---

2022), *available at* https://fortune.com/2022/02/28/ukraine-crypto-donations-tweet-bitcoin-ethereum-usdt-russia-invasion/; Roger Huang, *Dissidents Are Turning to Cryptocurrency as Protests Mount Around the World*, FORBES (Oct. 19, 2020), *available at* bit.ly/3KzA4q6.

era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley v. California*, 134 S. Ct. 2473, 2494 (2014). The antithesis of the Fourth Amendment is a regime by which the government can ascertain the private details of citizens' lives effortlessly and without suspicion of illegality. The Fourth Amendment was thus intended to "place obstacles in the way of a too permeating police surveillance." *United States v. Di Re*, 332 U.S. 581, 595 (1948). Its "basic purpose" is "to safeguard the privacy and security of individuals" against the government. *Camara v. Mun. Court of S.F.*, 387 U.S. 523, 528 (1967).

An individual has a reasonable expectation of privacy in "his or her personal affairs." *United States v. Haddix*, 239 F.3d 766, 767 (6th Cir. 2001). A person loses a reasonable expectation in matters that he "knowingly exposes to the public." *Katz v. United States*, 389 U.S. 347, 351 (1967). But a person enjoys an enhanced expectation in matters that he takes affirmative steps to keep private. *Id*. at 352. When he "shuts the door" to a phone booth, *id*., or places his "personal effects inside a doublelocked footlocker," *United States v. Chadwick*, 433 U.S. 1, 11 (1977), for instance, he manifests an expectation of privacy that is reasonable and receives constitutional protection. And when the government transgresses a person's "reasonable expectation of privacy," it has conducted a search. *United States v.*

Jones, 565 U.S. 400, 406 (2012); *see also Katz*, 389 U.S. at 360 (Harlan, J., concurring).

Cryptocurrency "shuts the door" to financial transactions, meaning that the Fourth Amendment protects those transaction from warrantless government surveillance. Indeed, the Bitcoin "white paper," a computer science article written by Bitcoin's creator to introduce the technology to the world, described this as cryptocurrency's "new privacy model." Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 6 (2009), *available at* bit.ly/3uwVr5J. As the white paper explained, when two users complete a transaction using Bitcoin, the public can see "that someone is sending an amount to someone else." *Id.* But, without more information, the public would not be able to "link[] the transaction to anyone." *Id.*

If a user's personal identifying information is linked to an address, all that changes. At that point, a person may access the public ledger and identify that user's transactions. Such a person could search for the user's address and establish that user's personal transaction history, determine what causes he has supported, and uncover intimate details about his private affairs. The Bitcoin white paper warned of this vulnerability: "[I]f the owner of a key is revealed, linking [on the public ledger] could reveal other transactions that belonged to the same owner." *Id.*

There are two ways for an outsider to link someone's personal identifying information to his public address. First, the user might simply share his address.

Sharing his public address would make it easy to identify all his transactions, but it would also make it easier to transact with him, and some users are willing to do this. Second, the user could share the details of one of his transactions, which would allow someone to locate that transaction on the public ledger and deduce that the public address involved was his. They could then search for other, unrelated transactions connected to the same address. *See* Complaint at ¶¶ 14-19, *United States v. 155 Virtual Currency Assets*, No.: 20-cv-2228 (RC), 2021 WL 1340971 (D.D.C. Apr. 9, 2021) (explaining law enforcement's use of "sophisticated, commercial services" to identify a user's multiple addresses).

A problem arises if a third person, someone who is *not* a party to that cryptocurrency transaction, learns the real name of one of the individuals who takes part in the cryptocurrency transaction (i.e., the identity of someone behind the cryptocurrency transaction). If that happens, the third party can use the public ledger as a comprehensive database of all transactions sent to or received by that person. In other words, the expectation of privacy that a cryptocurrency-transaction participant would otherwise enjoy has been obliterated.

Although steps can be taken to increase the difficulty of linking multiple transactions, those steps are rare and often do not suffice. For example, although a user can create multiple private keys and multiple addresses to use in different transactions, public ledger analysts are often able to identify connected addresses.

And if their addresses become known to others, then those others could find all the transactions using those addresses. Public ledger analysts may also find all transactions using other addresses by analyzing the activity of their known addresses. In other words, if Bob and Alice were forced to reveal that they took part in the above transaction, they would each also effectively reveal their participation in a wide range of other, unrelated transactions.

III. BECAUSE PARTIES TO CRYPTOCURRENCY EXCHANGES HAVE A FOURTH AMENDMENT PROTECTED REASONABLE EXPECTATION OF PRIVACY IN THEIR PERSONAL INFORMATION, THE IRS CANNOT ISSUE A JOHN DOE SUMMONS WITHOUT A VALID WARRANT.

What necessary follows is also self-evident. John Doe Summonses require the disclosure of individuals' personal identifying information along with the details of their transactions, and thereby reveal sensitive details about their personal affairs. This means that John Does Summonses violates the reasonable expectations of privacy of both senders and receivers in cryptocurrency transactions. It follows that John Doe Summonses constitute a search without a warrant. And that means that John Doe Summonses violate the Fourth Amendment.

The foregoing demonstrates that cryptocurrency users have chosen to exchange currency using a technology explicitly designed to preserve personal agency and protect enhanced privacy in transactions—they, in no uncertain terms, have taken the steps necessary to enhance their reasonable expectation of privacy. *See Katz*, 389 U.S. at 352. This means that cases addressing such things as "orderly

taking under compulsion of process," *United States v. Morton Salt Co.*, 338 U.S. 632, 651-52 (1950), "administrative agency subpoenas [seeking] corporate books or records," *See v. Seattle*, 387 U.S. 541, 544 (1967), laws requiring people to unilaterally furnish evidence to the government, *Chandler v. Miller*, 520 U.S. 305, 313 (1997), and laws requiring businesses to report details of their transactions to the government, *Airbnb, Inc. v. City of N.Y.*, 373 F. Supp. 3d 467, 472 (S.D.N.Y. 2019), do not apply writ large to cryptocurrency transactions. The "substance of the offense" under the Fourth Amendment "is the compulsory production of *private papers*," whatever the means. *Hale v. Henkel*, 201 U.S. 43, 76 (1906) (emphasis added).

In other words, courts may not "uncritically extend existing precedents" under the Fourth Amendment without adjusting for "new concerns wrought by digital technology." *Carpenter v. United States*, 138 S. Ct. 2206, 2222 (2018). Instead, "the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish." *United States v. Warshak*, 631 F.3d 266, 285 (6th Cir. 2010). At bottom, courts must "assure[] 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). And the deliberately private nature of cryptocurrency technology and the detailed picture of a person's affairs

that can emerge if that privacy is transgressed means that the Fourth Amendment prevents warrantless obtainment of that information.

Indeed, even when the government stops short of invading a reasonable expectation of privacy, it still conducts a search if it violates a person's property rights. *See Florida v. Jardines*, 569 U.S. 1, 11 (2013); *Jones*, 565 U.S. at 405. The property-rights-based approach "ask[s] if a house, paper or effect was *yours* under law." *Carpenter*, 138 S. Ct. at 2267-68 (Gorsuch, J., dissenting) (emphasis added). To determine whether something was yours, courts look to preexisting property law and other sources of positive law. *Id*. at 2267 (Gorsuch, J., dissenting); *see also United States v. Miller*, 982 F.3d 412, 432-33 (6th Cir. 2020).

Traditionally, "[t]he protection of private property extended to letters, papers, and documents." *Id*. at 432. If someone accessed such documents without consent, they would commit "trespass to chattels." *Id.* at 433. Accordingly, if the government inspected someone's mail without a warrant, it would violate the Fourth Amendment. *Ex parte Jackson*, 96 U.S. 727 (1877). In modern terms, it follows that even the opening of digital "files" without consent could therefore "be characterized as a 'trespass to chattels' and an illegal 'search.'" *Miller*, 982 F.3d at 433. Personal information and data about one's activities are the "modern-day" versions of the "papers" and "effects" that the Fourth Amendment protects. *See Carpenter*, 138 S. Ct. at 2267 (Gorsuch, J., dissenting).

Here, the personal information subject to John Doe Summonses is the modern-day equivalent of the "papers" and "effects" of the parties to the transaction. The government's collection of public cryptocurrency addresses could lead to the collection of a vast number of receipts detailing otherwise private matters. "[W]arrantless searches" that result in government collection of this sort of material "are per se unreasonable under the Fourth Amendment" unless a "specifically established and well-delineated exception[]" applies, such as for exigent circumstances. *City of Ont. v. Quon*, 560 U.S. 746, 760 (2010) (cleaned up); *see also Katz*, 389 U.S. at 357; *Arizona v. Gant*, 556 U.S. 332, 338 (2009). This, in turn, means that John Doe Summonses are "unreasonable" because they do not satisfy the warrant requirement or any exception to the warrant requirement.

This case underscores how far behind the IRS has lagged with respect to crafting clear regulatory and legal guidance for users and companies in the Bitcoin space. Indeed, in 2013, after two congressional hearings on Bitcoin and the release of the Financial Crimes Enforcement Network's ("FinCEN") virtual currency guidance, the U.S. Government Accountability Office ("GAO") criticized the IRS for its failure to make any attempt at developing regulatory guidance or clarity with respect to Bitcoin and other virtual currencies. *See* GOVERNMENT ACCOUNTABILITY OFFICE, REPORT TO THE COMMITTEE ON FINANCE, U.S. SENATE. VIRTUAL ECONOMIES AND CURRENCIES: ADDITIONAL IRS GUIDANCE COULD REDUCE TAX

COMPLIANCE RISKS, Ref. No. GAO-13-516 (May 2013), *available at* http://www.gao.gov/assets/660/654620.pdf. The GAO report suggested that "[b]y not issuing guidance, IRS may be missing an opportunity to address these compliance risks and minimize their impact and potential for noncompliance." *Id.* For another year, the IRS continued to avoid the issue.

The IRS's attempt to catch up, however, has resulted in potential widespread Fourth Amendment violations. In April 2014, the IRS finally issued informal guidance, IRS Notice 2014-21. *See* INTERNAL REVENUE SERVICE, VIRTUAL CURRENCY GUIDANCE: VIRTUAL CURRENCY IS TREATED AS PROPERTY FOR U.S. TAX PURPOSES; GENERAL RULES FOR PROPERTY TRANSACTIONS, IR 2014-21 (Mar. 2014). That guidance is very brief, stating simply that Bitcoin and similar convertible virtual currencies would be classified as property and subject to capital gains treatment for tax reporting. The IRS received thirty-six public comments relating to its guidance, but it failed to respond or take any other action to clarify ambiguities raised by those commenters. *See* TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION, AS THE USE OF VIRTUAL CURRENCIES IN TAXABLE TRANSACTIONS BECOMES MORE COMMON, ADDITIONAL ACTIONS ARE NEEDED TO ENSURE TAXPAYER COMPLIANCE, Ref. No. 2016-30-83 (Sep. 2016), *available at* https://www.treasury.gov/tigta/auditreports/2016reports/201630083fr.pdf.

Two years on, in 2016, the Treasury Inspector General for Tax Administration ("TIGTA") issued a frank report criticizing the IRS for its continued failure to develop any "compliance initiatives or guidelines for conducting examinations." *Id.* It further noted that the IRS had formulated no "methodology for gathering data on virtual currency use in taxable transactions—data that are necessary to analyze the risk of noncompliance and to estimate its significance." *Id*. The TIGTA report stressed that "[b]y virtue of the [2013] FinCEN rulings, the IRS has significant tools available to help ensure that virtual currency exchanges are following the law" and chided the IRS for its lack of action over the intervening three years. *Id*. It stated, "[s]ince the GAO issued its report on virtual currencies three years ago, the IRS's position on virtual currency as a tax compliance risk requiring additional oversight has remained relatively unchanged." *Id*. Two letters from Congress followed, citing the TIGTA report and imploring the IRS to take a more strategic approach.[6]

The IRS has been repeatedly told that it has catching up to do on Bitcoin. Unfortunately, given its decision to employ John Doe Summonses to cover this

[6] *See* Letter from Chairman Orrin G. Hatch, Chairman Kevin Brady, and Chairman Vern Buchanan to John Koskinen, Commissioner Internal Revenue Service (May 17, 2017), *available at* https://waysandmeans.house.gov/wp-content/uploads/2017/05/2017.05.17-Coinbase-Letter-Hatch-BradyBuchanan.pdf; Letter from Congressman Jared Polis and Congressman David Schweikert to John Koskinen, Commissioner, Internal Revenue Service (Jun. 2, 2017), *available at* https://polis.house.gov/uploadedfiles/060217_ltr_irs_digital_currency.pdf.

ground, the IRS intends to catch up all at once by aggressively demanding swaths of private customer information. In so doing, the IRS has been using a mechanism that contravenes other healthy public-private relationships that have blossomed between Bitcoin companies and other regulators. In other words, the John Doe Summons approach is little more than a dragnet research project aimed not at any particularized suspicion of tax evasion, but squarely at the technology as a whole. While the IRS desperately needs to engage in expansive research, the courts long ago made clear that the government may not do so at the expense of the Fourth Amendment.

To be certain, the public addresses sought by John Does Summonses will provide enough information to the IRS about private transactions to allow the government to identify many more individuals who have transaction in the public ledger. The government can then figure out other information about the individuals involved in those transactions. Using those transactions, it can ascertain other, unrelated activities of those individuals, regardless of the amount involved in such other transactions and no matter when they occurred.

This is not a hypothetical risk. When the government learns the identities of participants in cryptocurrency transactions—using other constitutionally compliant means, such as warrants—the government takes that information and pays public-ledger analysts to determine what other transactions the participants have engaged in and what other addresses might belong to the participants. The government has

enlisted agents and contractors to "analyz[e] blockchain and de-anonymiz[e] [crypto] transactions" to be "able to track, find, and work to seize crypto." *See* Guinevere Moore, *Operation Hidden Treasure Is Here*, FORBES (Mar. 6, 2021), *available at* bit.ly/3Cnjh6k. One transaction is a gateway that gives the government access to a person's entire transaction history. *See id.*

Indeed, the government brags about how effective this method of surveillance can be at unearthing a cryptocurrency user's personal affairs.[7] Allowing the IRS to retain sensitive personal information will thereby cause the disclosure of a detailed and intimate transaction history that will paint a mosaic of a person's life. It will do so without a warrant, without probable cause, and even without statutorily defined limiting factors or an opportunity for pre-compliance review. The Fourth Amendment was intended to provide a bulwark against such transgressions.

Such personal information will present to the government a montage of a person's life incomparable to that generated by financial reporting requirements. The

[7] *See* Brief for United States, *United States v. Gratkowski*, 964 F.3d 307 at 7-8 (5th Cir. 2020) ("[L]aw enforcement has used these services in numerous past investigations and found it [sic] to produce reliable results."); Complaint at ¶¶ 14-19, *155 Virtual Currency Assets*, 2021 WL 1340971 ("[G]enerally, the owners of BTC addresses are not known unless the information is made public by the owner (for example, by posting the BTC address in an online forum or providing the BTC address to another user for a transaction)," but "analyzing the public transactions can sometimes lead to identifying both the owner of a BTC address and any other accounts [i.e., addresses] that the person or entity owns and controls").

government will be able to obtain this information in an environment in which these persons take careful and affirmative steps to preserve their privacy. In addition, given the frequency of government data breaches (including one recently at the IRS), this personal information could allow the public widespread access to this personal information. Not only would private-transaction information be made public, but private individuals could become open to physical attacks and robbery.[8]

The summons as enforced effectively transforms an activity intended and designed to reveal minimal private information about participants into an activity that reveals significant private information to the wide expanses of the federal government. In that sense, if a transaction on a public ledger is somewhat like driving a car on a public road, reporting the participants to that transaction is like putting a GPS tracker on that car. And the Supreme Court has made crystal clear that the government may not do so without a warrant.

John Doe Summonses allows the government to access intrusive details about cryptocurrency users. Disclosure to the government about identifiable personal

[8] Kelly Phillips Erb, *IRS Contractor Pleads Guilty To Stealing And Disclosing Tax Return Information*, Forbes (Oct. 13, 2023), *available at* https://www.forbes.com/sites/kellyphillipserb/2023/10/13/irs-contractor-pleads-guilty-to-stealing-and-disclosing-tax-return-information/?sh=537cbe077cb2; Minyvonne Burke & Cristian Santana, *Elderly N.C. Couple Was Held Hostage In Their Home And Robbed Of $156,000 In Cryptocurrency*, NBC NEWS (Jul. 29, 2023), *available at* https://www.nbcnews.com/news/crime-courts/elderly-nc-couple-was-held-hostage-home-robbed-156000-cryptocurrency-rcna97056.

addresses will provide a window not only into the transactions being reported, but also into an individual's full, and entirely unrelated, cryptocurrency-transaction history. The disclosure will therefore uncover a detailed picture of a person's personal activities, potentially including intimate activities far beyond the immediate scope of the summons, and even if users have taken a series of steps to protect their transactional privacy. Without a warrant, forcing these disclosures violate the Fourth Amendment.

IV. ABOVE AND BEYOND THE FOURTH AMENDMENT VIOLATION, JOHN DOE WARRANTS CONSTITUTE A STATUTORY ABUSE OF PROCESS.

One other point bears mentioning. A John Doe Summons must be invoked by a court, and "a court may not permit its process to be abused." *United States v. Powell*, 379 U.S. 48, 58 (1964). An abuse would occur "for any . . . purpose reflecting on the good faith of the particular investigation." *Id.* This standard does not allow "the IRS to become an information-gathering agency for other departments." *United States v. La. Salle Nat'l Bank*, 437 U.S. 298, 317 (1978). As the Supreme Court has noted, there may someday exist a "need to prevent other forms of agency abuse of congressional authority and judicial process." *Id.* at 318 n.20.

Beyond the constitutional concerns described above, allowing the IRS to access the sort of information the John Doe Summonses request will provide the means for the IRS, any other agency that obtains the summoned records, and any

person with whom this information is shared (either legally or through a breach of IRS-maintained records) to compile a behavioral history of private individuals. The information disclosed to the IRS would allow the IRS to compile information beyond simply the means to find out about customer tax obligations. This excessive amount of information amounts to an abuse of the summons process by the IRS.

CONCLUSION

For all these reasons, this Court should reverse the district court's dismissal of Mr. Harper's lawsuit.

Dated: October 20, 2023

Respectfully submitted,

/s/ Edward M. Wenger

Edward M. Wenger
John Cycon
HOLTZMAN VOGEL BARAN
TORCHINSKY & JOSEFIAK PLLC
2300 N Street NW, Suite 643A
Washington, DC 20037
(202) 737-8808 (phone)
(540) 341-8809 (facsimile)
emwenger@holtzmanvogel.com
jcycon@holtzmanvogel.com

Counsel for
Amicus Curiae
Coin Center

CERTIFICATE OF COMPLIANCE

1. This document complies with the type-volume and word-count limits of Fed. R. App. P. 27(d) because, excluding the parts of the document exempted by Fed. R. App. P. 32(f), this document contains 5,381 words.

2. This document complies with the typeface and type-style requirements of Fed. R. App. P. 27(d) because this document has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Times New Roman font.

/s/ Edward M. Wenger
EDWARD M. WENGER

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that, on this 20th day of October, 2023, a true copy of this Amicus Brief was filed electronically with the Clerk of Court using the Court's CM/ECF system, which will send by email a notice of docketing activity to the registered Attorney Filer on the attached electronic service list.

/s/ Edward M. Wenger
EDWARD M. WENGER