No. 24-___

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 A WRIT OF CERTIORARI TO THE U.S. COURT OF APPEALS FOR THE FIRST CIRCUIT

PETITION FOR A WRIT OF CERTIORARI

February 21, 2025

Sheng Li
Counsel of Record
John J. Vecchione
Mark S. Chenoweth
NEW CIVIL LIBERTIES ALLIANCE
4250 N. Fairfax Dr.,
Suite 300
Arlington, VA 22203
(202) 869-5210
sheng.li@ncla.legal
Counsel for Petitioner

QUESTION PRESENTED

The Internal Revenue Service used a subpoena to obtain without a warrant from a cryptocurrency exchange three years of transaction records concerning over 14,000 of the exchange's customers, including Petitioner James Harper's records. Mr. Harper's contract with the exchange made clear that the records belonged to him and that the exchange would protect his privacy. The transaction records at issue opened an especially intimate window into Harper's life because they not only revealed his historical cryptocurrency transactions but also enabled tracking of his transactions into the future. The court below relied on the third-party doctrine to hold that IRS's warrantless search and seizure of Harper's financial records did not violate the Fourth Amendment.

The question presented is:

Does the Fourth Amendment permit warrantless searches of customer records held by third-party service providers if the records are contractually owned by the customer, or if those records enable surveillance of future behavior? If not, does the third-party doctrine need to be discarded or modified to prevent such searches?

PARTIES TO THE PROCEEDING

Petitioner is James Harper.

Respondents are Acting Commissioner of Internal Revenue Douglas O'Donnell, the Internal Revenue Service; John Doe IRS Agents 1-10.

RELATED PROCEEDINGS

Pursuant to Rule 14.1(a)(iii) of this Court, Petitioner certifies that he is unaware of any related proceedings to this matter before this Court or any trial or appellate state or federal court.

TABLE OF CONTENTS

TABLE OF APPENDICES

TABLE OF AUTHORITIES

Page(s)

Cases

Constitutional Provisions

Statutes

Other Authorities

PETITION FOR A WRIT OF CERTIORARI

James Harper respectfully seeks a writ of certiorari to review the judgment of the United States Court of Appeals for the First Circuit.

OPINIONS AND ORDERS BELOW

The panel opinion of the First Circuit (App.1a) is reported at 118 F.4th 100. The decision of the district court dismissing Petitioner's complaint (App.37a) is reported at 675 F.Supp.3d 190.

JURISDICTION

The First Circuit entered judgment on September 24, 2024. On December 5, 2024, Justice Jackson extended the time to file a petition for writ of certiorari until February 21, 2025. This Court has jurisdiction under 28 U.S.C. § 1254(1).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The Fourth Amendment to the United States Constitution provides in relevant part:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause[.]

STATEMENT OF THE CASE

This case presents a fundamental and recurring question regarding Fourth Amendment protections in the digital age: Does the third-party doctrine eliminate all constitutionally protected privacy and property interests in financial records merely because they are stored with a third-party service provider? The government's warrantless acquisition of vast amounts of sensitive financial information—without any individualized suspicion—stands in stark contrast with both the original meaning of the Fourth Amendment and recent decisions of this Court, underscoring the need for constitutional protections to adapt to modern digital realities.

The third-party doctrine originated in *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), where this Court held that individuals lack a reasonable expectation of privacy in records shared with third parties. As members of this Court have recognized, that doctrine was wrongly conceived in the first place and is especially maladapted to the modern era of the internet, cloud storage, and widespread digital transactions. *Carpenter v. United States*, 585 U.S. 296, 388 (2018) (Gorsuch, J., dissenting); *United States v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

To be sure, *Carpenter* limited the third-party doctrine by holding that it does not apply to historical cell-site location information, recognizing that modern digital records can reveal deeply personal details about individuals' lives. Yet lower courts, as here, have struggled to extract a coherent principle from *Carpenter*, defaulting instead to an outdated and

overly broad reading of *Miller* and *Smith*. Fourth Amendment protection is thereby denied to vast troves of sensitive information—including financial records—which are shared and stored with third parties as a matter of modern necessity.

Here, the government obtained detailed financial records from 14,355 individuals—encompassing 8.9 million transactions—without a warrant and without any particularized suspicion of wrongdoing. In contrast to the targeted investigations in *Miller* and *Smith*, which involved limited data concerning individual suspects over brief periods, the broad summons here represents an indiscriminate dragnet search covering years of transactions. This is the very type of general warrant that the Framers designed the Fourth Amendment to prevent.

Since the Founding, the Fourth Amendment has protected from warrantless search a person's "papers and effects." This category includes digital financial records. Being stored on a third-party service provider does not result in a waiver of rights where, as here, the underlying contract specifies that the records belong to the customer. The First Circuit's refusal below to recognize contractual terms as a basis for Fourth Amendment protection makes digital privacy virtually impossible.

The government's collection of cryptocurrency transaction records in this case exacerbates constitutional concerns. Unlike traditional financial records, cryptocurrency transactions place pseudonymous identifiers on a public blockchain, which means the government's access enables surveillance of an individual's financial activities far

into the future. Such pervasive surveillance was unimaginable in the technological context of *Miller*.

The Court should grant this petition to resolve the growing uncertainty surrounding the third-party doctrine and to affirm that the Fourth Amendment prevents warrantless mass surveillance of financial records. Absent the Court's intervention, the lower court's ruling will effectively strip millions of Americans of meaningful privacy protections over their most sensitive financial data—simply because they use modern financial service providers.

I. FACTUAL BACKGROUND

In 2013, Petitioner James Harper opened an account with Coinbase, Inc., a digital currency exchange that facilitates transactions in cryptocurrencies such as Bitcoin. Amend. Compl. ECF3 at 5–6. In doing so, Harper entered into a binding contract with Coinbase—one that expressly guaranteed the privacy and security of his financial information. *Id.* at 6. Under the terms of this contract, Coinbase assured Harper that it would safeguard his sensitive data, maintaining confidentiality through stringent security measures, including encryption, physical access controls, and strict internal policies. *Id.* at 6–7.

The contract's Privacy Policy was unambiguous: Coinbase would not disclose Harper's personal financial information. *Id.* This promise was subject to limited exceptions—which are standard in such contracts—including (i) his explicit consent and (ii) valid, properly issued subpoenas, court orders, or similar legal processes. *Id.* at 8.

Harper used Coinbase to deposit Bitcoin and conduct transactions in that cryptocurrency. Harper reported and paid all taxes on his income and capital gains, including those related to his Bitcoin holdings. *Id.* at 8. He routinely converted Bitcoin to dollars between 2013 and 2016. To engage in these transactions, Harper, by necessity and relying on the contractual protections, entrusted Coinbase with personal financial information—his constitutionally protected papers and effects. Harper stopped using Coinbase in 2016 after transferring his remaining cryptocurrency to a hardware wallet. *Id.* at 8-9.

In November 2016, IRS filed an *ex parte* petition in the Northern District of California to serve a sweeping John Doe summons on Coinbase. *See United States v. Coinbase, Inc.*, No. 17-cv-01431, 2017 WL 5890052, at *1 (N.D. Cal. 2017).[1] IRS sought an extraordinary trove of financial records for millions of Coinbase users—including detailed transaction logs, account profiles, due diligence records, and even private correspondence between Coinbase and its customers from 2013 to 2015. *Id.*

Coinbase initially resisted, prompting IRS to seek judicial enforcement. In subsequent proceedings, the court narrowed IRS's demand. *Id.* at *2. But even this curtailed summons resulted in Coinbase producing

---

[1] Under 26 U.S.C. § 7609(f), an IRS John Doe summons requesting information on unnamed third parties must: (1) relate to the investigation of a particular person or an ascertainable group of persons, (2) for whom IRS has a reasonable basis to believe has violated federal tax law, and (3) seek information that is not readily available elsewhere.

detailed records of 8.9 million transactions from 14,355 account holders—including Harper. *Id.* at *4.

At no point was Harper notified that his private records had been seized.[2] Amend. Compl., ECF3 at 11, 16. He learned of IRS's actions only in August 2019, when he received a menacing letter from the agency. *Id.* at 14. The letter's message was unmistakable: "We have information that you have or had one or more accounts containing virtual currency but may not have properly reported your transactions involving virtual currency." *Id.* IRS had no basis for such a claim—Harper had paid every cent of tax owed. But the letter made clear that IRS had obtained his confidential financial data.

For Harper, this unlawful seizure was not merely an abstract privacy violation—it threatened his family's security. The custom of self-custody of cryptocurrency makes privacy a paramount protection. If criminals suspect that an individual holds significant cryptocurrency, they may resort to home invasion, kidnapping, or worse to steal it.[3] IRS's continued possession of his records—at risk of hacking

---

[2] At the time, Harper mistakenly believed that Coinbase summons did not encompass his records, in part because Coinbase had announced it would notify affected customers but never provided him with such notice.

[3] *See* Jeff John Roberts, *Violent Crypto Robberies Soar—Spurring Demand for 'Wrench Attack' Insurance*, Fortune Crypto (Feb. 3, 2025) https://fortune.com/crypto/2025/02/03/bitcoin-kidnapping-insurance/; "Known Physical Bitcoin Attacks" collected at https://github.com/jlopp/physical-bitcoin-attacks/blob/master/README.md

and breaches from IRS's systems—places him and his family at unnecessary risk.

And for what? IRS has made no move to enforce any tax obligation against Harper because there is none to enforce. The agency does not—and cannot—dispute that Harper has paid his taxes in full. Its continued retention of his private financial records serves no legitimate purpose and creates an ongoing and unjustifiable risk to Harper's privacy, security, and constitutional rights.

II. PROCEEDINGS BELOW

Harper filed this suit in July 2020, alleging that IRS had unlawfully accessed his private financial records in violation of the Fourth and Fifth Amendments and 26 U.S.C. § 7609(f). Amend. Compl. ECF3 at 17-26.

The district court dismissed the suit in March 2021, concluding that the Anti-Injunction Act (AIA), 26 U.S.C. § 7421, deprived it of subject matter jurisdiction. *Harper v. Rettig*, No. 20-CV-771-JD, 2021 WL 1109254, at *1, *7 (D.N.H. Mar. 23, 2021), *vacated and remanded,* 46 F.4th 1 (1st Cir. 2022). Harper appealed, and the First Circuit reversed. Relying on *CIC Services, LLC v. IRS*, 593 U.S. 209 (2021), the court held that the AIA bars only suits that seek to restrain "the assessment or collection of any tax"—not suits like Harper's that challenge IRS's information-gathering activities. *Harper v. Rettig*, 46 F.4th 1, 7 (1st Cir. 2022).

On remand, limited discovery confirmed that Harper's transaction records seized from Coinbase revealed his "wallet addresses" and "public keys." *See* App.17a n.9. These are analogous to bank account

numbers, but they are published on the blockchain. When linked to an individual, they provide a permanent window into every transaction that individual has conducted *or will conduct* using the funds at those addresses/keys. As the court below explained: "anyone aware of that information can easily ascertain all transactions the person has made using that address—or track future transactions." App.17a n.9.

Yet the district court again dismissed Harper's suit, holding that he had no Fourth Amendment interest in his own records. App.48a-57a. It further held that IRS's compliance with statutory procedures automatically rendered any seizure of Harper's records reasonable. App.57a-61a. The court rejected Harper's Fifth Amendment due process claim, ruling that he lacked both a property interest in his financial records and a protectable liberty interest in their privacy. App.62a-67a. Finally, it dismissed Harper's § 7609 claim. While it "assume[d], without deciding" that the Administrative Procedure Act (APA), 5 U.S.C. § 704, could provide a cause of action for violations of § 7609(f), it nonetheless concluded that neither Harper nor any other affected taxpayer could challenge a magistrate's *ex parte* determination that IRS had satisfied § 7609(f)'s requirements. App.72a, 80a.

The First Circuit affirmed. It held that the third-party doctrine arising from *Miller* foreclosed Harper's Fourth Amendment claim, reasoning—wrongly—that Harper did not have a privacy interest in the records he entrusted to Coinbase, even though his contract with Coinbase expressly limited their disclosure and allocated to Harper the right to exclude. App.13a. The

appellate court did not affirm the lower court's holding that IRS's compliance with statutory procedures could render any search reasonable under *United States v. Powell*, 379 U.S. 48 (1964), a case that interpreted the statute rather than the Fourth Amendment. Nor did it hold that IRS in fact complied with those procedures. The First Circuit further affirmed the dismissal of Harper's Fifth Amendment due process claim. And it affirmed the dismissal of his § 7609 claim, holding that IRS's decision to issue a John Doe summons was not a final agency action subject to judicial review. App.32a-36a.

The government seized Harper's private records without a warrant, without notice, and without providing him with an opportunity to object. It retains a permanent means to monitor Harper's historical and future financial activity, despite having no allegation that Harper has violated any tax law. Such unchecked surveillance is governmental abuse that the Fourth Amendment was designed to prevent.

REASONS FOR GRANTING THE PETITION

IRS's overbroad dragnet presents an important question regarding the proper scope of the third-party doctrine that demands resolution by this Court. In our digital era, this Court's review is essential to protect Fourth Amendment privacy interests against potentially catastrophic invasions.

The Court should grant this petition because it presents a crucial and recurring constitutional question regarding the Fourth Amendment's modern protections—specifically, whether the third-party doctrine nullifies those protections when an individual stores financial records with a third-party

service provider that has pledged by contract to protect those records from disclosure. There is deep skepticism about the third-party doctrine's continued viability. The petition also implicates a unique technological development whereby such a search reveals *all future transactions* of Americans like Harper. The Court has never faced an administrative third-party demand that allows the Government to monitor individuals' transactions in perpetuity.

Justice Sotomayor has observed that the third-party doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring). Likewise, Justice Gorsuch has echoed scholars who believe that the third-party doctrine "is not only wrong, but horribly wrong." *Carpenter*, 585 U.S. at 388 (Gorsuch, J., dissenting) (quoting Kerr, *The Case for the Third–Party Doctrine*, 107 MICH. L. REV. 561, 563 n.5, 564 (2009)).

Carpenter held that the third-party doctrine does not apply to the category of cell-site location information. But that ruling left lower courts with little guidance beyond that narrow category. As a result, courts continue to deny Fourth Amendment protection to highly sensitive data—digital analogues to "papers and effects"—that individuals must share with third-party service providers as a necessary part of modern life. Without this Court's intervention, the unchecked third-party doctrine will continue to swallow up the Fourth Amendment rights of millions of Americans, including Harper. This petition

presents the Court with at least three avenues to safeguard the Fourth Amendment in the digital age.

First, the Court should align the third-party doctrine with the original understanding of the Fourth Amendment, which was grounded in securing one's property—an interpretation that has reemerged in the Court's jurisprudence since *Jones*. This approach requires courts to assess whether an individual has a property interest in the records at issue based on contractual terms with the third party. *Carpenter*, 585 U.S. at 353-54 (Thomas, J., dissenting); *id.* at 388 (Gorsuch, J., dissenting). Here, the court below entirely ignored Harper's contractual rights and instead relied on *Miller*—a case that never addressed property interests or contract rights—to strip Harper of Fourth Amendment protection. The Court should grant review to clarify that a contractually assigned property interest can be the basis for Fourth Amendment protection of records stored with third parties.

Second, the Court should return the third-party doctrine to its foundations in discrete investigations, based on individualized suspicion. *Miller* and *Smith* never justified warrantless, dragnet surveillance. The third-party doctrine has always been constrained by both the *amount* of data collected and the *scope* of surveillance. Unlike the targeted collections in *Miller* and *Smith*, the government here obtained financial records of 14,355 Americans without any individualized suspicion of wrongdoing. This amounted to an unconstitutional dragnet search. The scope of the collection vastly exceeded data collections upheld by past precedents, spanning three full years of financial transactions rather than a single day or a

few months. The Court has already imposed guardrails on the warrantless public surveillance permitted under *United States v. Knotts*, 460 U.S. 276 (1983)—which is an extension of the third-party doctrine's "voluntary exposure" logic—by rejecting "dragnet type law enforcement practices." *See Id.* at 283-84 (1983); *Carpenter*, 585 U.S. at 311-13. The same guardrails should apply to the third-party doctrine.

Finally, the nature of the cryptocurrency records at issue presents an opportunity for the Court to address the third-party doctrine in the context of future surveillance. As the court below recognized, the records seized will allow IRS to "track [Harper's] future transactions," App.17a n. 9. Storing financial information about cryptocurrency transactions with Coinbase could not have extinguished Harper's expectation of privacy in all his cryptocurrency transactions.

Without this Court's intervention, the third-party doctrine threatens to leave Americans without meaningful privacy in their financial records—records that they must entrust to third-party service providers in the modern economy. The Court must act to ensure that the Fourth Amendment does not become a dead letter in the digital age.

I. THE COURT MUST REVISIT THE THIRD-PARTY DOCTRINE TO RESTORE FOURTH AMENDMENT PROTECTION TO DIGITAL RECORDS THAT AMERICANS ROUTINELY STORE WITH SERVICE PROVIDERS

This case presents an opportunity to update Fourth Amendment law to protect millions of

Americans who routinely engage in digital transactions, which require storing vast amounts of private data with third-party service providers. The confluence of outdated Fourth Amendment doctrine and contemporary information practices has severely undermined constitutional protections for Americans' private and personal records. For at least two decades, a guiding principle in the Court's Fourth Amendment jurisprudence concerning new technologies has been to ensure the "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). The third-party doctrine, as currently applied by lower courts, contradicts this principle and effectively nullifies Fourth Amendment protections for vast amounts of Americans' data.

Our national heritage is built on a fierce protection of private papers, a cornerstone that this non-textual Fourth Amendment doctrine undermines. This Court's corrective signal in *Carpenter* has not remedied the growing problem.

A. The Fourth Amendment Protected Private Papers at the Founding

The Fourth Amendment guarantees "[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. This protection is "indispensable to the full enjoyment of the rights of personal security, personal liberty, and private property," and its inclusion in the Bill of Rights was motivated by strong opposition to general warrants in both England and America on the eve of the

Revolutionary War. 3 Joseph Story, *Commentaries on the Constitution of the United States* § 1895 (1833).

Legal scholar Philip Hamburger noted: "If one goes back to the early Republic … it is difficult to find any federal executive body that could bind subjects to appear, testify, or produce records." *Is Administrative Law Unlawful?* 221 (2014). "[P]rivately owned papers were peculiarly protected: They were not subject even to general disclosure requirements, it being only government-owned records that were open to inspection." *Id.*

The Court has long protected individuals from being compelled by government authorities to produce their private papers. In *Boyd v. United States*, 116 U.S. 616 (1886), the Court struck down a government subpoena for business records, holding that such compulsory production was "unconstitutional and void" under the Fourth Amendment because it was akin to a general warrant. *Id.* at 618. The Court relied on Lord Camden's seminal opinion in *Entick v. Carrington*, which emphasized: "Papers are the owner's goods and chattels; they are his dearest property, and are so far from enduring a seizure, that they will hardly bear an inspection." *Id.* at 627–28 (quoting *Entick*, 19 How. St. Tr. at 1029).

Boyd equated the government's compelled production of private papers with "breaking into a house and opening boxes and drawers," concluding that both actions constituted an invasion of a person's "indefeasible right of personal security, personal liberty[,] and private property." *Id.* at 630. Justice Holmes relied on the Fourth Amendment to reject an administrative demand for business records in *FTC v. American Tobacco Co.*, explaining:

> Anyone who respects the spirit as well as the letter of the Fourth Amendment would be loath to believe that Congress intended to authorize one of its subordinate agencies to sweep all our traditions into the fire … and to direct fishing expeditions into private papers on the possibility that they may disclose evidence of crime.

264 U.S. 298, 305–06 (1924) (citation omitted).

This logic applies even when the records have been entrusted to a third-party agent bound by confidentiality. A decade before *Boyd*, the Court ruled that the Fourth Amendment protects letters and packages entrusted to the U.S. Postal Service. *Ex parte Jackson*, 96 U.S. 727 (1878). This Court has recognized that digital records are "private effects." *Riley v. California*, 573 U.S. 373, 399, 401 (2014); *see also United States v. Ackerman*, 831 F.3d 1292, 1304 (10th Cir. 2016) (Gorsuch, J.) (treating electronic files and images as papers or effects). This principle—that digital papers entrusted to third parties are protected—has been extended to electronic communications as well. *See Id.* at 1304–05 (relying on *Ex parte Jackson* to apply Fourth Amendment protections to emails stored by a third-party service provider); *United States v. Warshak*, 631 F.3d 266, 285–86 (6th Cir. 2010) (same).

B. The Third-Party Doctrine Emerged from the Post-*Katz* Deviation from the Fourth Amendment's Original Meaning

Until the latter half of the twentieth century, Fourth Amendment protections were firmly grounded in property rights. *See Jones*, 565 U.S. at 405. But that foundation was upended when this Court "deviated" from the traditional approach in *Katz v. United States*, 389 U.S. 347 (1967), redefining the Fourth Amendment's reach through Justice Harlan's now-familiar formulation: a search occurs when the government intrudes upon an expectation of privacy that society recognizes as reasonable. *Id.* at 361 (Harlan, J., concurring); *see also* Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 817 (2004) ("Existing scholarship generally teaches that the Supreme Court rejected the property-based approach … in 1967 when it decided *Katz*[.]"). The third-party doctrine was a direct product of this paradigm shift.

The doctrine took root in *United States v. Miller*, where Treasury agents had substantial evidence that Miller was operating an unregistered and untaxed still. 425 U.S. 435, 437 (1976). Relying on facially invalid subpoenas, they obtained Miller's bank records, including checks, financial statements, and deposit slips. *Id.* at 438. The Court held that Miller had "no legitimate 'expectation of privacy'" in those records because they were "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Id.* at 442. From that, the Court broadly concluded:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

Id. at 443 (citations omitted).

The Court extended the third-party doctrine in *Smith v. Maryland*, 442 U.S. 735, 742 (1979). There, police had evidence that Smith had robbed and begun stalking the complainant. *Id.* at 737. They asked the telephone company to install a pen register, hoping to confirm Smith as the source of threatening calls. *Id.* *Smith* ruled that short-term use of a pen register to record numbers dialed from a telephone was not a Fourth Amendment search. *Id.* at 742. It emphasized that when a person dials a phone number, he "voluntarily convey[s] numerical information to the telephone company." *Id.* at 744. The Court also pointed to the "limited capabilities" of the pen register, explaining that it could not reveal whether a conversation even took place, let alone its contents. *Id.* at 741-42.

This Court has not upheld a warrantless seizure or search under the third-party doctrine since *Smith*, more than 45 years ago, and the doctrine has faced

sustained criticism ever since.[4] Justice Brennan's dissent in *Miller* noted that the California Supreme Court had already rejected the doctrine under a state constitutional provision mirroring the Fourth Amendment. 425 U.S. at 447 (Brennan, J., dissenting) (citing *Burrows v. Superior Court*, 13 Cal.3d 238 (1974)). Since then, multiple states have likewise rejected the doctrine through constitutional rulings, amendments, or statutory provisions. *See, e.g., People v. Seymour*, 536 P. 3d 1260, 1272 (Colo. 2023); *see also* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 395-405 (2006) (listing states rejecting the doctrine).

The doctrine's problems have only grown with time. While *Smith* emphasized the "limited" nature of information obtained, some lower courts have since expanded the doctrine to cover vast categories of digital information—including email metadata and the IP addresses of websites visited. *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). As Justice Sotomayor has observed, the doctrine is "ill

---

[4] *See, e.g.*, Christopher Slobogin, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment* 151-64 (2007) (critiquing the third-party doctrine in the context of third-party subpoenas); Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 19-20 (2008) (characterizing Fourth Amendment protections for personal data as weak due to the third-party doctrine); Neil Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 WASH. U. L. REV. 1441, 1475-80 (2017) (asserting that the third-party doctrine as applied in a digital context undermines the core values of the Fourth Amendment).

suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring). She "doubt[ed] that people would accept without complaint the warrantless disclosure to the government of a list of every website they had visited in the last week, or month, or year." *Id.*

Justice Gorsuch has been even more direct, echoing broad consensus that the "third-party doctrine is not only wrong, but horribly wrong." *Carpenter*, 585 U.S. at 388 (Gorsuch, J., dissenting). He underscored the absurdity of its results: "Can the government demand a copy of all your e-mails from Google or Microsoft without implicating your Fourth Amendment rights? Can it secure your DNA from 23andMe without a warrant or probable cause? *Smith* and *Miller* say yes it can." *Id.* If the Fourth Amendment is to retain any relevance in the digital age, this Court must revisit the third-party doctrine and realign its scope, or else overturn it entirely, to prevent the government from sweeping up Americans' confidential digital data without judicial oversight.

C. *Carpenter* Did Not Provide Meaningful Limitations or Guidance Regarding the Third-Party Doctrine

Carpenter briefly addressed the third-party doctrine, but lower courts have continued to apply the doctrine well beyond its narrow foundations. They have keyed on what the Court called "the unique nature of cell phone location record[s]," 585 U.S. 296, 309, to distinguish *Carpenter* and apply the third-

party doctrine aggressively in cases involving other types of data.

The Seventh Circuit, for example, concluded that *Carpenter* "refined the third-party doctrine for [only] a specific type of digital data: historical location," and proceeded to allow warrantless surveillance of web addresses visited by users. *United States v. Soybel*, 13 F.4th 584, 591 (7th Cir. 2021); *accord United States v. Rosenow*, 50 F.4th 715, 738 (9th Cir. 2022); *United States v. Trader*, 981 F.3d 961, 968 (11th Cir. 2020). The First Circuit took an even narrower view of *Carpenter*, treating it as little more than a one-off exception and holding that the third-party doctrine permits the DEA to compel a state agency to hand over prescription drug records—information that, by the court's own admission, reveals "a patient's diagnosis or several potential diagnoses." *United States v. Ricco Jonas*, 24 F.4th 718, 738 (1st Cir. 2022). And the court below held that the third-party doctrine, despite *Carpenter*, permits warrantless and suspicion-free seizure of cryptocurrency records, which allow monitoring of future transactions.

While *Carpenter* sent a much-needed corrective signal, it failed to provide guidance to confine the atextual third-party doctrine to its proper place. The Court must revisit the third-party doctrine, reining it in with concrete guardrails, or else overturn it altogether, so Fourth Amendment protections can align with the realities of the digital age.

II. THIS CASE PRESENTS AN IDEAL VEHICLE TO REFORM THE THIRD-PARTY DOCTRINE FOR THE DIGITAL AGE

This petition presents an ideal vehicle for the Court to consider whether Fourth Amendment protection of data held by third-party service providers can be based on contracts with their customers. That question is teed up because the First Circuit did not analyze the contract before concluding that Harper lacked a property interest in his records stored at Coinbase. The court below instead relied on *Miller*—a case that did not involve any analysis of contract or property interests.

This case provides an opportunity for the Court to apply the original meaning of the Fourth Amendment to digital records, recognizing these records as modern-day equivalents of an individual's "papers" or "effects." Under the traditional approach, the question is not whether the information is held by a third party, but whether the records belong to the individual based on the terms of service with the third-party company. If the records belong to the individual, they qualify as "*his* papers or effects" and may not be searched or seized without a warrant or probable cause. *Carpenter*, 585 U.S. at 405 (Gorsuch, J., dissenting).

This petition would allow the Court to address this important Fourth Amendment question without grappling with whether to apply the atextual exclusionary rule that arises in the Fourth Amendment's criminal-law context. *Collins v. Virginia*, 584 U.S. 586, 609 (2018). Harper complied with the law and was providing IRS with all the tax information he was required to submit when it used a

blanket, dragnet third-party summons to abscond with his personal cryptocurrency transaction data.

A. The Court Should Clarify that the Third-Party Doctrine Does Not Negate Contractual Property Interests

The separate dissents of Justices Thomas and Gorsuch in *Carpenter* provide guidance on how customers can retain Fourth Amendment protection in data or records stored with a third-party service provider: contracts. 585 U.S. at 353-54 (Thomas, J., dissenting); *id.* at 388 (Gorsuch, J., dissenting). If a contract grants the customer a property interest in the records, then those records are the customer's "papers and effects." Here, Harper alleges that his contract with Coinbase establishes that the seized financial records belong to him. *See* Amend. Compl. ECF3 at 17. The Court should clarify that a contractually granted property interest can serve as the basis for Fourth Amendment protection, notwithstanding the third-party doctrine's effect on the expectation of privacy.

Under the third-party doctrine, a person is deemed to have no legitimate expectation of privacy in information voluntarily turned over to third parties. *Miller*, 425 U.S. at 442 (holding that a depositor has no legitimate expectation of privacy in information voluntarily conveyed to banks and exposed to employees in the ordinary course of business); *Smith*, 442 U.S. at 743–44. The reasoning in *Miller* and *Smith* is rooted in *Katz*'s expectation-of-privacy framework. This Court has since revived the pre-1967 property-based understanding of Fourth Amendment protections, emphasizing concern for government

trespass on the areas specifically enumerated in the Amendment—"persons, houses, papers, and effects." *Jones*, 565 U.S. at 407.

Expectations of privacy are irrelevant in determining whether a property-based search occurred. *Florida v. Jardines*, 569 U.S. 1, 11 (2013) ("[It] is unnecessary to consider [expectations of privacy] when the government gains evidence by physically intruding on constitutionally protected areas."). Therefore, the third-party doctrine should not apply when determining whether the government has violated the Fourth Amendment by intruding into digital papers and effects stored with a third party. Under the Fourth Amendment's original meaning, the focus is simply on whether papers or effects belong to the individual. No more is needed. *Carpenter*, 585 U.S. at 400 (Gorsuch, J., dissenting) ("Just because you entrust your data—in some cases, your modern-day papers and effects—to a third party may not mean you lose any Fourth Amendment interest in its contents.").

Although *Carpenter* relied on the *Katz* expectation-of-privacy approach, that test can be inconsistent with the original meaning of the Fourth Amendment. *Carpenter*, 585 U.S. at 391-92 (Gorsuch, J., dissenting). In the digital context, under a property-based approach to extend Fourth Amendment protection to data held by service providers, it is "entirely possible a person's cell-site data could qualify as *his* papers or effects under existing law." *Id.* at 405. According to Justice Gorsuch, the Telecommunications Act supports this view because it prohibits third-party carriers from using or disclosing customer data without permission and requires

carriers to provide the data to customers upon request—thereby conferring a property interest in the data. *Id.* (citing 47 U.S.C. § 222).

Justice Thomas agreed that the *Katz* test lacks a foundation in the text or history of the Fourth Amendment and that it distorts Fourth Amendment jurisprudence. *Carpenter*, 585 U.S. at 343 (Thomas, J., dissenting). He also agreed that a property-based approach could support Fourth Amendment protection of records if Carpenter could establish that the cell-site records were his. *Id.* at 354. However, Justice Thomas found the Telecommunications Act insufficient to establish such a property right. He emphasized that any such property interest could only be derived from Carpenter's contracts with his service providers. *Id.* at 353–54.

Here, unlike in *Carpenter*, Harper's contract with Coinbase explicitly grants him ownership of his records. The contract forbids Coinbase from unauthorized use or disclosure of Harper's data absent a *valid* subpoena or order. By contrast, it grants Harper full access to his transaction records upon request and does not restrict his ability to use or disclose them. This petition presents an opportunity for the Court to recognize Fourth Amendment protection in data held in confidence by a third-party service provider, based on a person's contractual ability to control and exclude others from accessing and using such data.

Harper's contract with Coinbase affords him greater rights to control his financial data than does the Telecommunications Act, which Justice Gorsuch found sufficient to confer a property interest in cell-site records. Just as Justice Thomas noted that

Google's terms of service could establish a property interest in data, Harper's contract could establish that the records held by Coinbase belong to him, demonstrated in part by its repeated use of the possessive pronoun "your" to describe the records.[5] *See Carpenter*, 585 U.S. at 353–54 (Thomas, J., dissenting).

The court's claim below that "Harper makes no effort … to explain the legal source of the [property] interest he asserts," App.20-21a, is contradicted by Harper's consistent assertion of contract rights as the basis of his property interest, *see, e.g.*, Plaintiff-Appellant's Opening Br. at 21–27; Plaintiff's MTD Response ECF32 at 20–21; Amend. Compl. ECF3 at 17–18. The records at issue belonged to someone, and the court below was required to ascertain whom—Harper, Coinbase, or both[6]—by applying principles of

---

[5] The court below claimed in a footnote that Harper raised the contract's repeated use of the possessive pronoun "your" for the first time at oral argument. App.21a n.11. Not so. Harper explicitly made that argument in his opening brief: "The routine use of the possessive pronoun 'your' when service providers, including Coinbase, refer to customers' information illustrates the common understanding that the information is the customers' and protectable by them under the Fourth Amendment[.]" Plaintiff-Appellant's Opening Br. at 27. The court's further suggestion below in the same footnote that "your" merely indicated that the records were *about* Harper rather than *belonging* to him was pure invention and not based on any analysis of the underlying contract. *See* App.21a n.11.

[6] Property interests include a "bundle of rights" that can be allocated by contract among multiple parties. *See Cedar Point Nursery v. Hassid*, 594 U.S. 139, 150 (2021) (citation omitted). Harper's contract with Coinbase grants him the "right to exclude" others from accessing or using his records, which is one

contract interpretation, such as *contra proferentem*. *See Yahoo Inc. v. Nat'l Union Fire Ins. Co. etc.*, 14 Cal.5th 58, 72 (2022).

But the First Circuit did not analyze Harper's contract. Instead, it relied on *Miller*'s rejection of financial records in that case as the suspect's "private papers." App.23a. This approach is misguided, as there was no contractual or legal basis in *Miller* establishing that the bank records belonged to the defendant. As Justice Alito explained, "[t]he defendant did not claim that he owned these documents," and instead argued that "'analysis of ownership, property rights and possessory interests in the determination of Fourth Amendment rights ha[d] been severely impeached' by *Katz* and other recent cases." *Carpenter*, 585 U.S. at 384 (Alito, J., dissenting) (quoting Brief of Respondent in *United States v. Miller*, OT 1975, No. 74-1179, p.6).

There was no occasion in *Miller* to analyze whether the bank records belonged to the defendant; instead, the Court applied *Katz*'s privacy-based analysis: "We must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents." 425 U.S. at 442. Thus, *Miller* is irrelevant to the property-based approach to Fourth Amendment protection and presents no barrier to Harper's possessing a property interest in his cryptocurrency records based on his contract with Coinbase.

---

of the "most treasured" rights within that bundle. *See Id.* at 150-51

This petition provides an ideal opportunity for the Court to recognize that Fourth Amendment protection of data held by third-party service providers can be based on contract rights. At a minimum, the Court should grant the petition to reverse the lower court's misinterpretation of *Miller* and remand for an analysis of Harper's property interest in his records based on his contract with Coinbase. Furthermore, the Court should consider overruling *Miller* to the extent that the decision is interpreted as nullifying property rights in all data transferred to a third party without regard for contractual terms.

B. The Court Should Cabin the Third-Party Doctrine to Its Foundation of Targeted Investigations

This petition also presents the Court with a vital opportunity to reaffirm the Fourth Amendment's protections by making clear that the third-party doctrine has important limits under *Katz's* privacy-based approach. Indeed, *Katz* held that a person retains a reasonable expectation of privacy in the contents of a telephone call made from a public booth, 389 U.S. at 353, even though "[a]t the time *Katz* was decided, [third party] telephone companies had a right to monitor calls." *Warshak*, 631 F.3d at 287. And of course, the contents of a telephone call are always shared with the recipient. But the fact that a conversation involves two parties, or that it is routed through a third-party provider, does not mean that the speaker forfeits his Fourth Amendment protection in the contents of the communication. *Id.*

If *Katz* remains good law—a fact IRS does not dispute—then *Miller* and *Smith* could not have

established an absolute rule that categorically eliminates Fourth Amendment protection for all information shared with third parties. Instead, those cases must be read as establishing a doctrine that is inherently constrained both by the *volume* of information collected and the *scope* of the surveillance conducted. Otherwise, the third-party doctrine would swallow *Katz* whole, rendering its "reasonable expectation of privacy" test meaningless in an era when individuals necessarily rely on third parties to facilitate everything from financial transactions to healthcare, email communication, and internet usage.

Miller and *Smith* emphasized the limited nature of third-party information being collected. *Miller* involved a narrow request, covering just "two financial statements," "three monthly statements," and a few "checks" and "deposit slip[s]" from a single suspect over a brief, four-month period. *Miller*, 425 U.S. at 438. In *Smith*, the government's request was even narrower: it sought only the numbers that a single defendant dialed from his landline over the course of a single day. *Smith*, 442 U.S. at 737. In upholding this collection, the Court emphasized that the data was extremely "limited," revealing neither the contents of any communication nor the identities of the parties involved. *Id.* at 742. Neither case authorized the kind of warrantless, long-term, indiscriminate surveillance underlying the IRS's collection of three years' worth of transaction data from over 14,000 Coinbase customers.

Warrantless public surveillance permitted under *Knotts*, which evolved directly from the third-party doctrine, was similarly constrained. *See* 460 U.S. at 283. *Knotts* upheld the police force's use of a beeper to

track the movements of a suspect's vehicle in public, relying on *Smith* to reason that individuals lack an expectation of privacy in what they voluntarily expose to the public, *i.e.*, many third parties. *Id.* (citing *Smith*, 442 U.S. at 744-45). But the Court also warned against taking that voluntary-exposure logic too far, recognizing that "twenty-four hour surveillance of any citizen of this country['s]" public movements would present an entirely different constitutional question. *Id.* (citation omitted). Hence, *Knotts* recognized that "if such dragnet type law enforcement practices … should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." *Id.* at 284.

The Court heeded that warning in *Carpenter*, rejecting warrantless government access to cell-site location data to track a suspect's public movements. 585 U.S. at 311-12. Two considerations were key to the decision not to follow *Knotts*'s voluntary-exposure allowing warrantless public surveillance. *First*, "the retrospective quality of the [cell-site] data" allows the government to "travel back in time to retrace a person's whereabouts." *Id.* at 312. *Second*, "this newfound tracking capacity runs against everyone," though the case at issue concerned only a single criminal suspect. *Id.* This ability to reconstruct a historical account of many persons' movements was not possible when *Knotts* was decided. The Court wisely declined to extend it to allow warrantless, "dragnet type" of mass surveillance that *Knotts* cautioned against. 460 U.S. at 284; *see also Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 346 (4th Cir. 2021) (en banc) (striking down aerial

surveillance that enables historical tracking of an entire city's public movements).

Carpenter, however, did not place similar guardrails on the third-party doctrine. Instead, the Court rejected the third-party doctrine based on "the unique nature of cell phone location records." *Carpenter*, 585 U.S. at 309. It fashioned an unstructured balancing test based on ill-defined factors, such as the need to avoid "arbitrary power" and "too permeating police surveillance." *Id.* at 395 (Gorsuch, J., dissenting) (citations omitted). The result is open season on Americans' privacy in digital data—lower courts purporting to follow *Carpenter* have applied the third-party doctrine to eviscerate privacy with respect to web histories, email metadata, and medical records. *Supra* at 21-22. Modern technology gives the government the means to aggregate this vast trove of information to gain unprecedented insight into citizens' private lives.

The mismatch between *Carpenter*'s anti-dragnet limitation for warrantless public surveillance under *Knotts* and the lack of concrete guidance for the third-party doctrine is incoherent. Both operate under the same "voluntary exposure" rationale and should be analyzed in the same way. *See Knotts*, 460 U.S. at 283 (citing *Smith*, 442 U.S. at 744-45). It is unclear why a person would retain a greater expectation of privacy for information exposed publicly under the public-surveillance cases than for information shared with a single third-party service provider.

This case offers an ideal vehicle to resolve the doctrinal mismatch in *Carpenter* because IRS's subpoena directly implicates the same two concerns that led the Court not to permit warrantless public

surveillance under *Knotts*: "the retrospective quality of the data" and a "tracking capacity [that] runs against everyone," *Carpenter*, 585 U.S. at 312. The Court should put the same guardrails on the third-party doctrine, which would restore the doctrine to its limited scope as originally applied in *Miller* and *Smith*.

IRS obtained a staggering three full years' worth of detailed financial records from Harper and other affected Coinbase customers. *See Coinbase, Inc.*, 2017 WL 5890052, at *8-9. Not one day, as in *Smith*, 442 U.S. at 737, nor a few months, as in *Miller*, 425 U.S. at 438. In addition to Social Security numbers and home addresses, the government acquired detailed records of every account holder's "account activity," including every financial transaction conducted. *See Coinbase, Inc.*, 2017 WL 5890052, at *8-9. This is no mere collection of telephone numbers or isolated bank statements—it is a complete transaction history encompassing a three-year span and continuing into the future. This is far from the "limited" information that this Court allowed to be collected without a warrant from a third party. *Smith*, 442 U.S. at 742. Even the court below acknowledged that such collection "opens a potentially wide window into that person's financial activity[.]" App.18a.

Also, unlike in *Miller* and *Smith*, IRS did not seek the financial records of a single individual based on particularized suspicion, nor even an identifiable group of individuals. It obtained the financial records of 14,355 Americans, covering nearly nine million transactions. IRS had no individualized suspicion that any of them had violated the law. This was a fishing expedition conducted with the hope that a

retrospective search through years of transaction data would yield some evidence of wrongdoing. But such "dragnet type" surveillance, *Knotts*, 460 U.S. at 284, is precisely the kind of "indiscriminate searches and seizures conducted under the authority of 'general warrants'" that the Fourth Amendment was enacted to prevent. *Payton v. New York*, 445 U.S. 573, 583 (1980).

IRS's approach to data collection represents an overbroad application of the third-party doctrine that fails to distinguish between targeted investigations and indiscriminate dragnet surveillance. This Court must intervene to recalibrate the doctrine, ensuring that Fourth Amendment protections are not eroded by warrantless, mass data collection practices.

C. The Court Should Take Future Activity out of the Third-Party Doctrine's Reach

The nature of cryptocurrency transactions reinforces the need for the Court's review. Blockchain technology records every such transaction on a public ledger while preserving user privacy through pseudonymous addresses. *See United States v. Harmon*, 474 F. Supp. 3d 76, 81 (D.D.C. 2020). Each user has a unique, pseudonymous "wallet address" or "public key" associated with his or her transactions. *See id.* While the address and key are posted on the ledger for anyone to see, no one knows the identity of the parties involved, thus ensuring anonymity.

This anonymity, however, collapses once the government matches an address or key to an individual. Once that occurs, the government can identify every transaction that person has ever made and will make. Even if someone creates a new

address, publicly available software allows the government to connect his new address to his old one. *See United States v. Sterlingov,* 719 F. Supp. 3d 65, 71–72, 84 (D.D.C. 2024) (detailing blockchain analysis and its reliability).

The upshot is that once the government compels the disclosure of an individual's cryptocurrency addresses and keys, it not only obtains the disclosed information but also gains a surveillance mechanism that tracks all of a user's past and future transactions. *See* App.17a n.9. That is exactly what happened here:[7] by seizing records linked to Harper and over 14,000 others, IRS effectively obtained a real-time monitor of their future financial activity.

Whatever reduced expectation of privacy Harper may have had in the transactions he voluntarily shared with Coinbase did not extend to future transactions conducted through entirely different cryptocurrency exchanges or on his own. In *Miller*, government agents were only able to obtain information regarding the suspect's transactions through the bank at issue. Here, by contrast, IRS can monitor Harper's cryptocurrency transactions with *any* person or exchange, even after he stopped using Coinbase in 2016. IRS has effectively put a crypto "ankle monitor" on Harper and over 14,000 of his fellow Coinbase customers, exposing them to perpetual financial monitoring.

---

[7] The court below "agree[d] with Harper and his amici that exposure of [his wallet address and public key] was a reasonably likely consequence of the IRS summons, either directly or by analyzing the transaction data that was included." App.17a n.9.

Despite the heightened privacy concerns associated with cryptocurrency transactions, the court below treated all financial records as indistinguishable. This Court should update the third-party doctrine to modern technologies and to ensure it does not become a tool for *future-looking* surveillance that was inconceivable when *Miller* was decided.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully Submitted,

Sheng Li
Counsel of Record
John J. Vecchione
Mark S. Chenoweth
NEW CIVIL LIBERTIES ALLIANCE
4250 N. Fairfax Drive, Suite 300
Arlington, VA 22203
(202) 869-5210
sheng.li@ncla.legal

Counsel for Petitioner

February 21, 2025