No. 24-922

In the Supreme Court of the United States

JAMES HARPER, PETITIONER

v.

MICHAEL FAULKENDER, ACTING COMMISSIONER OF INTERNAL REVENUE, ET AL.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FIRST CIRCUIT

REPLY BRIEF FOR THE PETITIONER

JOHN J. VECCHIONE
MARK S. CHENOWETH
NEW CIVIL LIBERTIES ALLIANCE
4250 North Fairfax Drive, Suite 300
Arlington, VA 22203

KANNON K. SHANMUGAM
Counsel of Record
WILLIAM T. MARKS
BENJAMIN M. MILLER-GOOTNICK
BRANT J. VERMEER
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
2001 K Street, N.W.
Washington, DC 20006
(202) 223-7300
kshanmugam@paulweiss.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases:

Page

Cases—continued:

Constitution and statute:

In the Supreme Court of the United States

No. 24-922

JAMES HARPER, PETITIONER

v.

MICHAEL FAULKENDER, ACTING COMMISSIONER OF INTERNAL REVENUE, ET AL.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FIRST CIRCUIT

REPLY BRIEF FOR THE PETITIONER

This Court adopted the third-party doctrine before e-mail and text messaging became primary forms of communication; before scanners and cloud storage replaced filing cabinets; and before mobile apps stored intimate details about our finances, health, and habits. The third-party doctrine has always struggled to keep up with evolving technology. And as the numerous amici supporting petitioner have recognized, it is particularly problematic when applied to digital records in which an individual has a contractual property interest. All the more so in the context of a cryptocurrency exchange such as Coinbase, where access to an individual's digital records may allow the government to monitor a user's future financial activity in perpetuity. As the dragnet search blessed by the decision below confirms, the third-party doctrine has now

hollowed out the Fourth Amendment. This case is an excellent vehicle for providing much-needed guidance on the scope of the third-party doctrine in the modern world—or for discarding it entirely.

In the face of compelling arguments for further review, the government offers feeble responses. On the need for guidance: while the government cites the absence of conflicting authority, it disregards the growing discontent among the courts of appeals. Judges from no fewer than seven federal courts of appeals have questioned whether the third-party doctrine remains consistent with Fourth Amendment principles in the digital era.

On the merits: the government fails to come to grips with petitioner's property-based claim, arguing that the claim was inadequately preserved and then relying on decisions that did not consider a property-based theory of the Fourth Amendment. But petitioner's briefing below was replete with assertions that his contract with Coinbase allocated him a property interest in the records the Internal Revenue Service obtained. The government's other arguments merely beg the question of whether the third-party doctrine is adequately protective of Fourth Amendment interests today.

This case presents the Court with an ideal opportunity either to reshape the third-party doctrine for the 21st century or to heed the calls of members of this Court, lower-court judges, scholars, and commentators to overrule the doctrine altogether. The petition for a writ of certiorari should be granted.

A. The Lower Courts Are Badly In Need Of Guidance On The Third-Party Doctrine

The government argues that the Court's review is unwarranted because the courts of appeals have shown "uniformity in applying settled Fourth Amendment principles to new technology." Br. in Opp. 20. That argument fails to capture the reality in the lower courts. Judges from numerous federal courts of appeals have voiced concerns about the continued application of the third-party doctrine in the context of modern technologies.

To begin with, two courts of appeals have specifically questioned the continued validity of the presumption at the heart of the third-party doctrine: namely, that a person who gives his private information to a third party assumes the risk of disclosure. The Fifth Circuit has suggested that, because of the "ubiquity" and "necessity" of divulging personal information to third-party companies today, "the notion that users * * * 'assume[] the risk' of th[eir] information being divulged to law enforcement is dubious." *United States* v. *Smith*, 110 F.4th 817, 834-835 (2024) (citation omitted). The Ninth Circuit has likewise expressed the view that "the assumption-of-risk rationale underlying the [third-party] doctrine is 'ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.'" *United States* v. *Moalin*, 973 F.3d 977, 992 (2020) (quoting *United States* v. *Jones*, 565 U.S. 400, 417 (2011) (Sotomayor, J., concurring)).

In a similar vein, judges from five other courts of appeals have expressed grave concerns regarding the scope of information potentially made available to the government through the confluence of the third-party doctrine and the ubiquity of third-party digital products. The Second Circuit has recognized that it is now "difficult if not

impossible to avoid exposing a wealth of information" to digital third parties, *ACLU* v. *Clapper*, 785 F.3d 787, 826 (2015); one Eleventh Circuit judge has expressed concern over the "slippery slope that would result from a wooden application of the third-party doctrine" in the face of massive "technological change." *United States* v. *Davis*, 785 F.3d 498, 537 (Martin, J., dissenting), cert. denied, 577 U.S. 975 (2015). The Tenth Circuit has cautioned that "unfettered government collection of personal data" could produce an "Orwellian-style surveillance state." *United States* v. *Thompson*, 866 F.3d 1149, 1159 (2017), vacated, 585 U.S. 1029 (2018). A panel of the Fourth Circuit went so far as to call the third-party doctrine the "*Lochner* of search and seizure law." *United States* v. *Graham*, 796 F.3d 332, 360 (citation omitted), reversed en banc, 824 F.3d 421 (2016), cert. denied, 585 U.S. 1029 (2018). And as the Sixth Circuit has urged, "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 (2010).

The lower courts have also expressed deep skepticism that Americans' expectations of privacy have remained the same since the 1970s, when the third-party doctrine was first adopted. With the "total integration of third-party[] technological services into everyday life," courts now face a "steroidal version of the problems" that Justices Marshall and Brennan identified in their dissents in *United States* v. *Miller*, 425 U.S. 435 (1976), and *Smith* v. *Maryland*, 442 U.S. 735 (1979). *Davis*, 785 F.3d at 526 (Rosenbaum, J., concurring). Courts are recognizing that "possible changing societal expectations of privacy," *Thompson*, 866 F.3d at 1159, can no longer be ignored. As lower courts have stressed, it is highly questionable that average Americans expect their entire digital existence, which includes their most highly sensitive information, to

be exposed to the government's "inquisitive eyes." *Leaders of a Beautiful Struggle* v. *Baltimore Police Department*, 2 F.4th 330, 340 (4th Cir. 2021) (en banc) (citation omitted); see *id.* at 341-345.

The erosion of the fundamental underpinnings of the third-party doctrine has created deep uncertainty. The en banc Fourth Circuit's recent attempt to address the constitutionality of a new data-collection method called "geofence warrants," which yielded a staggering nine separate opinions, epitomizes this confusion. See *United States* v. *Chatrie*, 136 F.4th 100 (2025). Although the court ultimately refused to suppress the evidence, six judges joined concurring opinions raising concerns about the operation of the third-party doctrine. Chief Judge Diaz lamented that a "Fourth Amendment fog" has settled over courts struggling to discern "the reach of the Fourth Amendment in the digital age." *Id.* at 108. And Judge Wynn, joined by five of his colleagues, wrote that the third-party doctrine "stems from decisions issued over 45 years ago." *Id.* at 116. Absent this Court's intervention, Judge Wynn predicted, "courts and citizens" will be left to "grope in the dark as to the limits of governmental power." *Id.* at 115.

B. The Decision Below Is Incorrect

Although the merits are ultimately for another day, the government's defense of the decision below falls woefully short.

1. The government fails to come to terms with petitioner's basic contention that he has a protected property interest in his private information arising from both the original understanding of the Fourth Amendment and his contract with Coinbase. See Pet. 25-26. As one amicus has explained, the law has long treated one's private in-

formation, including financial records, as private property. See Macleod Br. 6-8; see also Pet. 14. Digital financial records are the modern equivalent of the private papers this Court has long protected. The government offers no compelling answer to that core principle. As petitioner's contract with Coinbase confirms, the government intruded on his protected property here.

The government argues (Br. in Opp. 16) that petitioner "waived" any argument regarding that property interest by failing to develop it until oral argument. That is demonstrably false. Petitioner's opening brief below included an entire section entitled, "Coinbase's Contract with Harper Guarantees Privacy of His Papers." Pet. C.A. Br. 3-5. The brief proceeded to argue that petitioner's "financial records are his 'papers' " and that, when petitioner "entrusts his property to another for purposes of safekeeping (*i.e.*, to a bailee), he does not thereby surrender any portion of his property rights." *Id.* at 21. Petitioner's property argument is clearly preserved.

The government also contends (Br. in Opp. 16-19) that Coinbase's privacy policy created no property rights merely by referring to its records as "your information." But the government is eliding that petitioner's contract also established his right to access and control his transaction records; limited Coinbase's ability to disclose those records without consent or valid legal process; and repeatedly characterized the records as belonging to petitioner. See Pet. 4-5, 24; Pet. App. 40a. In addition, Coinbase's privacy policy provided express protections from "unauthorized access" and "disclosure," including to law enforcement in the absence of valid legal process. See Pet. App. 40a. Taken together, those provisions create the most fundamental property right of all: "the right to exclude." *Cedar Point Nursery* v. *Hassid*, 594 U.S. 139, 150-151 (2021).

The government repeatedly invokes *Miller* for the proposition that petitioner cannot have a property interest in business records created by a third party. See Br. in Opp. 10-13, 17-19. But the defendant in *Miller* "did not claim that he owned [the] documents" at issue there, *Carpenter* v. *United States*, 585 U.S. 296, 384 (2018) (Alito, J., dissenting), so the Court did not consider a property argument there of the kind petitioner is advancing here.

2. The government argues (Br. in Opp. 11) that the Court's decisions in *Miller*, *Smith*, and *Carpenter* resolve this case in its favor. They do not.

For starters, IRS's acquisition of petitioner's wallet addresses and public keys enable the government to monitor petitioner's future related cryptocurrency transactions in perpetuity. See Pet. App. 17a n.9. As the court of appeals explained, "anyone aware of that information can easily ascertain all transactions the person has made using that address—or track future transactions." *Ibid.*

As a result, petitioner is subject to open-ended financial monitoring that was inconceivable when *Miller* was decided. The government's position would allow it to obtain records from any cryptocurrency exchange and use those records to monitor an individual's financial activities across all platforms indefinitely—transforming the third-party doctrine from a rule about historical disclosures into a license for comprehensive future surveillance. The government offers no limiting principle for its rule.

The government also fails to justify the dragnet nature of its surveillance, noting only that the summons was limited to customers with over $20,000 in annual transactions. See Br. in Opp. 5, 14-15. But the third-party doctrine emerged from cases involving targeted investigations of *specific individuals* based on *particularized* suspicion. *Miller* involved a single suspect's records over four months: namely, "two financial statements," "three

monthly statements," and several "checks" and "deposit slip[s]." 425 U.S. at 438. *Smith* likewise involved records of phone numbers dialed by one defendant over a single day. See 442 U.S. at 737.

That pales in comparison to the records the government collected here. In IRS's single request to Coinbase, it obtained financial records from over *14,000* Americans covering nearly *9 million* transactions over three years—without any individualized suspicion whatsoever. See Pet. 3, 5-6. That is precisely the type of "dragnet type law enforcement practice[]" that this Court has cautioned against. *Knotts* v. *United States*, 460 U.S. 276, 284 (1983). Indeed, under the government's theory, Congress could authorize IRS to demand comprehensive financial records from every bank in the Nation without any individualized suspicion, simply by asserting a general interest in tax compliance. That is decidedly not what the Framers contemplated when they adopted the Fourth Amendment.

3. To the extent *Miller* and *Smith* can be read to foreclose petitioner's position, this case presents an ideal opportunity for the Court to reconsider the third-party doctrine altogether. As Justice Gorsuch recently observed, a scholarly consensus has emerged that the third-party doctrine is "not only wrong, but horribly wrong." *Carpenter*, 585 U.S. at 388 (dissenting opinion) (citation omitted). Justice Sotomayor has likewise noted that the doctrine is "ill suited to the digital age." *Jones*, 565 U.S. at 417 (concurring opinion). Those criticisms, echoed by a chorus of lower-court judges and amici in this case, reflect a growing consensus that a doctrine developed for discrete disclosures in the 1970s does not fit the comprehensive data sharing that characterizes modern life.

The government does not seriously dispute that the historical foundations of the third-party doctrine have eroded. When *Miller* and *Smith* were decided, most

Americans had only limited interactions with third-party service providers. Customers used bank accounts primarily for basic transactions, and telephone records captured only limited information about personal communications. Today, by contrast, third parties hold comprehensive records regarding virtually every aspect of Americans' lives—from their physical movements and social relationships to their financial activities and political preferences.

That transformation has fundamentally altered the assumptions underlying the third-party doctrine. The doctrine rested on the premise that individuals could avoid constitutional exposure by limiting their disclosures to third parties. But when meaningful participation in modern society depends on sharing data with third parties, that choice becomes illusory. In the face of technological change, Fourth Amendment doctrine should not be applied in a way that eviscerates the Amendment's protective purposes. See *Carpenter*, 585 U.S. at 313-314; *Riley* v. *California*, 573 U.S. 373, 403 (2014).

C. The Question Presented Is Important And Warrants Review In This Case

The government does not dispute that the question presented recurs frequently or that questions involving the application of the third-party doctrine in the digital age are of substantial practical and legal importance. Instead, the government contends only that certiorari is not warranted here because "the record is underdeveloped" and "the question presented is not outcome determinative." Br. in Opp. 20. Neither contention withstands scrutiny.

1. The government suggests (Br. in Opp. 20-21) that the civil nature of this case renders it a poor vehicle because the criminal context "generally provides this Court with a clearer record." But the proceedings below have

left no uncertainty regarding the information IRS collected through enforcement of its sweeping summons. "Coinbase produced account holder documents and information[,] * * * including information about [petitioner's] Coinbase account from 2013 and 2015." Pet. App. 44a. Subsequent litigation confirmed that IRS obtained three full years' worth of detailed financial records from petitioner and every account holder's "account activity," including every financial transaction conducted. See *United States* v. *Coinbase, Inc.*, Civ. No. 17-1431, 2017 WL 5890052, at *8-*9 (N.D. Cal. 2017). And discovery on remand confirmed that those records revealed petitioner's "wallet addresses" and "public keys," which enable surveillance of his future cryptocurrency transactions. See Pet. App. 17a n.9. The record is thus replete with detailed evidence on the precise nature of the information IRS collected about petitioner.

Far from posing a problem, the fact this is a civil case allows the Court to address the merits of the Fourth Amendment question without needing to navigate the intricacies of the good-faith exception to the exclusionary rule. And this Court has frequently decided Fourth Amendment questions in the civil context. See *Muehler* v. *Mena*, 544 U.S. 93 (2005); *Chandler* v. *Miller*, 520 U.S. 305 (1997); *Soldal* v. *Cook County*, 506 U.S. 56 (1992). The civil nature of this action is no impediment to review.

2. The government further argues (Br. in Opp. 22) that the question presented would not be outcome-determinative because satisfaction of the statutory standard for producing records to IRS set out in *United States* v. *Powell*, 379 U.S. 48 (1964), would suffice to satisfy the Fourth Amendment. But this Court has never considered whether that is so. The government's meager citation of two appellate decisions, one of which offers support only

in dicta within a footnote, hardly assuages the serious concerns about the constitutionality of the search conducted here.

The government's logic also flips the principle of constitutional supremacy on its head by implying that congressional authorization can cure a constitutional violation. To obtain judicial enforcement of a summons under *Powell*, "[t]he government's burden is a slight one, and may be satisfied by a declaration from the investigating agent that the *Powell* requirements are met." *Coinbase*, 2017 WL 5890052, at *3. But as a constitutional matter, that can be true only if the information obtained does not fall within the ambit of the Fourth Amendment. Deciding the question presented in petitioner's favor would obviously render the summons invalid—not the other way around.

The cases cited by the government do not authorize the type of dragnet search that occurred here. In both of those cases, the courts addressed IRS's attempt to obtain records from fewer than five unique individuals or entities, rather than thousands. See *United States* v. *Allee*, 888 F.2d 208, 209 (1st Cir. 1989); *Pressley* v. *United States*, 895 F.3d 1284, 1287-1288 (11th Cir. 2018). And Congress apparently recognized the threat posed by dragnet searches when it amended Section 7609(f) to require that a John Doe summons be "narrowly tailored to information" about a particular person or ascertainable group. Taxpayer First Act, Pub. L. No. 116- 25, § 1204(a), 133 Stat. 981, 988 (2019).

Finally, the harm suffered by petitioner is redressable by this Court. As plainly stated both in the complaint and in subsequent briefing, the harm asserted is that IRS continues to possess petitioner's sensitive financial information, creating ongoing threats of inadvertent dissemination as well as financial surveillance in perpetuity. See

Pet. 6-7. An injunction requiring IRS to return petitioner's sensitive information, and barring it from obtaining such information without a warrant going forward, would eliminate those threats.

In sum, this case is an excellent vehicle for resolving an exceedingly important constitutional question that has sown confusion and concern throughout the lower courts. The court of appeals' decision violated fundamental principles of the Fourth Amendment. The Court should grant review and, on the merits, reverse the judgment below.

* * * * *

The petition for a writ of certiorari should be granted.

Respectfully submitted.

JOHN J. VECCHIONE
MARK S. CHENOWETH
NEW CIVIL LIBERTIES ALLIANCE
4250 North Fairfax Drive, Suite 300
Arlington, VA 22203

KANNON K. SHANMUGAM
WILLIAM T. MARKS
BENJAMIN M. MILLER-GOOTNICK
BRANT J. VERMEER
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
2001 K Street, N.W.
Washington, DC 20006
(202) 223-7300
kshanmugam@paulweiss.com

JUNE 2025