No. 24-922

In the Supreme Court of the United States

JAMES HARPER,

Petitioner,

v.

DOUGLAS O'DONNELL, ACTING COMMISSIONER OF INTERNAL REVENUE SERVICE, ET AL.,

Respondents.

On Petition for Writ of Certiorari to the United States Court of Appeals for the First Circuit

BRIEF FOR AMICUS CURIAE NETCHOICE IN SUPPORT OF PETITIONER

MARK M. ROTHROCK
LEHOTSKY KELLER COHN LLP
8513 Caldbeck Drive
Raleigh, NC 27615

SCOTT A. KELLER
Counsel of Record
JEREMY EVAN MALTZ
LEHOTSKY KELLER COHN LLP
200 Massachusetts Ave. NW
Suite 700
Washington, DC 20001
(512) 693-8350
scott@lkcfirm.com

Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

INTEREST OF AMICUS CURIAE

NetChoice is a national trade association of online businesses that works to protect free expression and promote free enterprise online.[1] Toward those ends, NetChoice is engaged in litigation, amicus curiae work, and legal advocacy. At both the federal and state level, NetChoice fights to ensure the Internet stays innovative and free.

The Court's third-party doctrine at the heart of this dispute can threaten how users interact with the online services that NetChoice's members provide. It likewise could threaten the level of trust users can place in these services to safeguard their data. A broad interpretation of this doctrine, allowing for unchecked governmental access to user data submitted to those services, could undermine user confidence and chill online activity and commerce. NetChoice's members, including various online marketplaces and services, rely on this user trust to foster innovation and economic growth in the digital space.

This case highlights the need to clarify the application of existing legal frameworks to evolving digital technologies. And it presents an important constitutional question: Whether the Fourth

[1] In accordance with Rule 37.6, no counsel for any party has authored this brief in whole or in part, and no person or entity other than NetChoice, its members, or its counsel made a monetary contribution to the preparation or submission of this brief. In accordance with Rule 37.2, NetChoice timely notified all counsel of record of its intent to file this brief.

Amendment permits the government to engage in warrantless searches of user data held by third-party services. NetChoice and its members have a significant interest in the resolution of this question. NetChoice also has a strong interest in ensuring that legal precedents appropriately protect constitutional rights online, thereby fostering a vibrant and trustworthy internet.

SUMMARY OF ARGUMENT

"[T]he Cyber Age is a revolution of historic proportions." *Packingham v. North Carolina*, 582 U.S. 98, 105 (2017). Powering this revolution is the internet—an innovation that has "caused far-reaching systemic and structural changes" to American life. *Direct Mktg. Ass'n v. Brohl*, 575 U.S. 1, 18 (2015) (Kennedy, J., concurring). While the Framers knew neither the internet nor cryptocurrency, they understood that "[f]ew protections are as essential to individual liberty as the right to be free from unreasonable searches and seizures." *Byrd v. United States*, 584 U.S. 395, 402 (2018).

Yet lower courts have struggled to apply the Fourth Amendment's third-party doctrine in a way that accounts for the realities of modern internet usage and the unique nature of digital data storage. Mechanical application of the decades-old third-party doctrine may be "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. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring). Users

routinely make such information available to third-party services to participate in the modern digital economy and to use important services provided by NetChoice's members.

This Court's decision in *Carpenter v. United States*, 585 U.S. 296 (2018), recognized limitations on the third-party doctrine in the specific context of cell-site location information. But *Carpenter* did not provide comprehensive guidance for the many other forms of digital data that are now regularly stored with online services. And in the years following that decision, lower federal courts have inconsistently applied *Carpenter*'s holding. Pet.20. This case offers an ideal opportunity to clarify the scope and reach of *Carpenter*. Such guidance, in turn, would ensure that the Fourth Amendment remains an effective safeguard for privacy in the digital age, while providing the technology industry with a predictable framework for protecting user information.

ARGUMENT

I. The Fourth Amendment third-party doctrine's application to the digital age requires this Court's guidance.

The Fourth Amendment third-party doctrine arose decades ago, and its application to the modern technological landscape requires this Court's guidance.

The third-party doctrine is rooted in a pair of cases from the 1970s: *Miller* and *Smith*. *United States v. Miller*, 425 U.S. 435 (1976) (establishing the third-party doctrine); *see also Smith v. Maryland*, 442 U.S. 735 (1979) (similar). In those cases, this Court held that individuals lack a reasonable expectation of privacy in information they voluntarily share with third parties.

Over time, however, the types and volume of information that people share with third parties have radically changed. Today, individuals routinely—and often necessarily—entrust vast amounts of personal information to third parties to participate in the digital world. Pet.10. The pervasive integration of the internet and cloud computing into nearly all aspects of modern life have brought about a profound transformation in how individuals create, store, and share information. *See, e.g.*, Neil Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 WASH. U. L. REV. 1441, 1465 (2017). The very functionality of countless online services that people use daily—from social-media networks and collaborative-content-creation tools to e-commerce

marketplaces and cloud-based data storage solutions, many of which are operated by NetChoice's diverse membership—relies on users submitting data to those services. If users choose, this data can encompass a vast spectrum of sensitive information, including personal communications, financial transactions, browsing history, location data, user-generated content such as text, images, and videos, and myriad other digital records reflecting individuals' thoughts, activities, and associations. *See id.*

As the certiorari petition articulates, the volume, sensitivity, and nature of digital data now routinely stored with third-party services far exceeds the limited scope and context of the information at issue in *Smith* and *Miller*. *See Smith*, 442 U.S. at 737 (short-term use of a pen register to record dialed telephone numbers of a single suspect); *Miller*, 425 U.S. at 437-38 (bank records related to a specific investigation into tax violations). This case provides a perfect example: The IRS acquired three years of detailed cryptocurrency transaction records related to over 14,000 Coinbase customers, including petitioner Harper, without a warrant or any showing of individualized suspicion. Pet.5-6. The First Circuit allowed that acquisition, under the third-party doctrine. Pet.App.11-19.

The lower courts' broad and undifferentiated application of the third-party doctrine poses a significant and growing concern for the technology industry and NetChoice's diverse membership. NetChoice members' online services are designed to

facilitate seamless user interaction, content creation, and information sharing. This can require the storage of user-submitted data.

Accordingly, mechanical application of the third-party doctrine to these online services could essentially circumvent the Fourth Amendment's protections. The government's ability to conduct warrantless, dragnet searches of user information, resembles the type of governmental overreach—and the specter of general warrants—that the Fourth Amendment was specifically intended to prevent. *See Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 301 (1967) (explaining that the Fourth Amendment was "a reaction to the evils of the use of the general warrant in England and the writs of assistance in the Colonies"); 3 Joseph Story, *Commentaries on the Constitution of the United States* § 1895 (1833).

II. This case presents an ideal vehicle to clarify the Fourth Amendment's protections for data that users provide to online services.

This case presents an ideal opportunity for the Court to clarify how the Fourth Amendment third-party doctrine should apply to the digital age after *Carpenter*. In particular, the Court should account for three key factors: the unique nature of digital data and implications for further surveillance, the scope of warrantless governmental access to user data plus the prohibition of dragnet surveillance, and contractual property interests in digital records.

A. *Carpenter* began the process of applying Fourth Amendment principles to modern technologies. 585 U.S. at 309-10. Specifically, the Court held that the government's acquisition of historical cell-site location information constituted a search under the Fourth Amendment. *Id.* at 310. And it did so even though a rote application of the third-party doctrine would have permitted the search. *Id.* at 309-10. The Court emphasized the uniquely revealing nature of such data, which provides an intimate window into a person's movements and habits, and the pervasive, near-constant tracking capabilities it afforded law enforcement. *Id.* at 311.

But *Carpenter* had no occasion to expound on this analysis for the multitude of other forms of digital records that are now routinely generated, submitted, and stored with a wide array of online services. Lower courts have struggled to consistently interpret and apply *Carpenter*'s nuanced holding to these other technologies. And many have continued to apply the underlying logic of the third-party doctrine broadly to deny Fourth Amendment protection to various other forms of highly sensitive digital information. Pet.20.

This case is perhaps the best example of this phenomenon. The First Circuit relied heavily on *Miller*'s decades-old precedent to permit an invasive and broad search, implicating petitioner Harper and thousands of others. Pet.App.15-19. The court below held that Harper lacked any reasonable expectation of privacy in his detailed cryptocurrency transaction records held by Coinbase, even though there was a

contractual agreement between Harper and Coinbase expressly limiting disclosure and affirming Harper's ownership of the records. Pet.App.19-21 & n.11; *see* Pet.25 & n.5. That decision starkly highlights this persistent and deeply concerning uncertainty in the application of Fourth Amendment principles to digital data in the lower courts.

B. This Court's evaluation of Fourth Amendment protections in the digital age should focus on three key factors discussed below.

The unique nature of digital data and the implications for future surveillance. This petition allows the Court to analyze whether and how the nature of the requested data affects the Fourth Amendment analysis. This case happens to involve cryptocurrency transaction records. Pet.33. But the Fourth Amendment concerns presented extend far beyond just the cryptocurrency context, as various other forms of digital data can similarly reveal extensive historical information and potentially enable various forms of future tracking and profiling.

Like other forms of digital data, governmental seizure of cryptocurrency transaction records, when linked to an individual's identity, allow for the perpetual tracking of that individual's past and future financial activity. *Id.* This unprecedented capacity for ongoing surveillance, which was inconceivable in the technological context of *Miller* and *Smith*, raises novel and significant Fourth Amendment concerns. This Court should carefully consider how the third-party doctrine, rooted in a pre-digital era, applies to digital

data that possesses inherently far-reaching and continuous monitoring capabilities. The ability of the government to effectively place a digital "ankle monitor" on individuals without a warrant or any suspicion of wrongdoing—as exemplified by the IRS's actions here—represents a significant expansion of governmental power that demands careful scrutiny under the Fourth Amendment. *Id.*

The very functionality of NetChoice members' diverse online services depends on users believing that their data is secure when they submit it to those services. If users harbor a well-founded belief that their personal information is readily accessible to the government without protections afforded by established legal processes and constitutional safeguards, it will inevitably lead to a significant chilling effect on online expression, innovation, and commerce. It is therefore of paramount importance that this Court provide clear and principled guidance on the proper scope and limitations of the third-party doctrine in the digital age. That guidance is essential to safeguard the fundamental privacy rights of all individuals in an increasingly digital society. It is also necessary to foster a vibrant, dynamic, and innovative online ecosystem in which users feel confident and secure in using the services provided by the technology industry.

The scope of warrantless government access to user data and the prohibition of dragnet surveillance. This case will also allow the Court to consider how the scope and scale of records requests affect the Fourth

Amendment analysis. Here, the IRS made a sweeping demand for three full years of detailed financial transaction records from over 14,000 individuals. Pet.3, 5. The IRS did so without obtaining a warrant supported by probable cause or demonstrating any individualized suspicion of wrongdoing, due to the lower courts' application of the third-party doctrine. Pet.3. The scope of the government's demands here looks nothing like the targeted investigations in both *Miller*, 425 U.S. at 437-38, and *Smith*, 442 U.S. at 737.

Contractual property interests in digital records. Finally, this case allows the Court to consider the extent to which contractual and property interests in online data should affect the Fourth Amendment analysis. Here, petitioner Harper's contract with Coinbase's online service expressly established that his financial records belonged to him. Pet.24.

The First Circuit, however, did not analyze Harper's contractual rights. Instead, it relied on *Miller*, a case that did not involve any analysis of contractual or property interests. *See* 425 U.S. at 440-47. The lower court's analysis undermines the security and privacy that users reasonably and justifiably expect when they entrust their data to online services under clear contractual terms. Ignoring such expressly defined contractual rights effectively erodes the very notion of digital ownership and control.

* * *

The Framers could not have envisioned the internet or the digital world it would produce. But "a

central aim of the Framers was 'to place obstacles in the way of a too permeating police surveillance.'" *Carpenter*, 585 U.S. at 305 (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)). This case provides the Court an ideal opportunity to provide much-needed clarity and direction on the application of core Fourth Amendment principles to the vast and ever-growing realm of digital records held by third-party online services. This guidance will benefit both individuals (like petitioner Harper) who have been subjected to potentially unconstitutional government surveillance, as well as the broader technology industry, including NetChoice's members. Both users and industry need a more predictable set of rules about the government's access to user data.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted.

SCOTT A. KELLER
Counsel of Record
JEREMY EVAN MALTZ
LEHOTSKY KELLER COHN LLP
200 Massachusetts Ave. NW
Suite 700
Washington, DC 20001
(512) 693-8350
scott@lkcfirm.com

MARK M. ROTHROCK
LEHOTSKY KELLER COHN LLP
8513 Caldbeck Drive
Raleigh, NC 27615

Counsel for Amicus Curiae

MARCH 2025