No. 24-922

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 United States Court of Appeals for the First Circuit

BRIEF OF THE CATO INSTITUTE AS *AMICUS CURIAE* IN SUPPORT OF PETITIONER

Thomas A. Berry
Counsel of Record
Brent Skorup
Laura A. Bondank
CATO INSTITUTE
1000 Mass. Ave., N.W.
Washington, DC 20001
(443) 254-6330
tberry@cato.org

March 28, 2025

QUESTIONS PRESENTED

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?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

Constitutional Provisions

INTEREST OF *AMICUS CURIAE*[1]

The Cato Institute is a nonpartisan public policy research foundation founded in 1977 and dedicated to advancing the principles of individual liberty, free markets, and limited government. Cato's Robert A. Levy Center for Constitutional Studies was established in 1989 to promote the principles of limited constitutional government that are the foundation of liberty. Toward those ends, Cato publishes books and studies, conducts conferences, produces the annual *Cato Supreme Court Review*, and files *amicus* briefs.

Cato's interest in this case arises from its mission to support the rights that the Constitution guarantees to all citizens. *Amicus* has a particular interest in this case as it concerns the continuing vitality of the Fourth Amendment and protecting Americans from warrantless searches and seizures of their records.

---

[1] Rule 37 statement: All parties were timely notified before the filing of this brief. No part of this brief was authored by any party's counsel, and no person or entity other than *amicus* funded its preparation or submission.

SUMMARY OF ARGUMENT

In this "smart" and digitized world, much of what we do is captured and stored indefinitely. The places we go (using our phone's built-in GPS), the news stories we read, our Google search history, our credit card purchases, the charities we donate to, and even our gossip and spousal communications—often emailed or sent via messaging apps—are routinely collected and stored by commercial companies.[2] Today, digital recordkeeping is the norm and storing our communications and records on servers owned and maintained by third parties is impossible to avoid.

Digital technologies dramatically reduce the cost and inconvenience of record collection and analysis. And this only stokes law enforcement officials' insatiable appetite for information about citizens. Therefore, Congress and many federal agencies believe they've found a "cheat code" for pervasive government surveillance: demand warrantless access to our records on the dubious theory that we have forfeited any property interest or privacy expectation simply by using a digital service like email or the Internet.

Financial surveillance is a massive and growing threat to privacy rights and our constitutional order. In recent years, for instance, regulators and Congress have required regulated companies to track and give the government access to records about Americans'

---

[2] *See*, *e.g.*, Brent Skorup, *Tech Companies' Terms of Service Agreements Could Bring New Vitality to the Fourth Amendment*, HARV. L. REV. BLOG (Sept. 9, 2024), available at https://tinyurl.com/mrshprrt ("An IT professionals' aphorism—'there is no cloud, it's just someone else's computer'—suggests the reality: our digital lives are stored on nondescript server farms and office parks spread around the world.").

stock trades.[3] They have also required Americans to report small payments between individuals.[4] Financial regulators now even target surveillance at residents in particular counties.[5] Without judicial enforcement of Fourth Amendment protections, secretive and suspicionless digital record collection will become a routine tool of government regulation and control.

The facts of this case are sadly consistent with these trends. In 2016, the Internal Revenue Service (IRS) discreetly ordered Coinbase to produce sensitive information and financial records about millions of its customers. Coinbase resisted that initial production order, but eventually the IRS obtained from Coinbase records about more than 14,000 account holders and millions of their cryptocurrency transactions. *See* Pet. Br. 6. One account holder, James Harper, learned that the IRS had seized and searched his Coinbase account records only after the IRS sent him a letter (incorrectly) suggesting he had not paid taxes on his cryptocurrency income. *Id*.

---

[3] *See* Hester Peirce, *This CAT is a Dangerous Dog*, REALCLEAR POL'Y (Oct. 9, 2019), available at https://tinyurl.com/b88464f8 (describing the Security and Exchange Commission's "consolidated audit trail" system).

[4] *See* National Taxpayer Advocate, *If You Resold the Hottest Ticket of Summer 2023, You Likely Didn't Receive a Form 1099-K—But This Won't* Last Forever & Always, NTA BLOG (Feb. 20, 2024) (noting that "[i]n 2021, Congress passed the American Rescue Plan Act of 2021 (ARPA), which substantially lowered the filing threshold . . . . for issuing Form 1099-K" from $20,000 to $600).

[5] *See* Joe Lancaster, *Taking $200 Out of an ATM Should Not Trigger Federal Financial Surveillance*, REASON (Mar. 14, 2025), available at https://tinyurl.com/3ed93a32.

In 2020, Harper sued to protect his privacy and compel the IRS to delete their copies of his Coinbase account records. Those retained copies include records of his "wallet addresses" and "public keys," which give the agency "a permanent means to monitor Harper's historical and future financial activity." *Id.* at 9. Harper asserts that his Coinbase account records are owned by him and, therefore, that the IRS needed a warrant to seize and search his records. However, after a perfunctory review of his arguments, the district court and the appellate court below held that Harper's records are owned by Coinbase and, therefore, are within the third-party exception to the Fourth Amendment's warrant requirement. *See id.* at 7–9.

This case demonstrates that the third-party doctrine is outdated and increasingly unworkable. Since the doctrine's formalization almost 50 years ago, the government has relied on it to circumvent the warrant requirement and obtain Americans' most sensitive records, including emails, Google search histories, financial records, and location histories.[6] Government demands for Americans' most sensitive records increasingly conflict with the Fourth Amendment's central aim, which is "to place obstacles in the way of a too

[6] For instance, the Stored Communications Act allows government officials to obtain electronic communications stored remotely for longer than 180 days with a subpoena instead of a warrant. *See* 18 U.S.C. § 2703(a)–(d). The origination of this threshold is unclear but the "strange '180 day' rule . . . may reflect the Fourth Amendment abandonment doctrine at work." Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).

permeating police surveillance." *United States v. Di Re*, 332 U.S. 581, 595 (1948).

This Court has been clear that the Fourth Amendment protects our property. *Soldal v. Cook County*, 506 U.S. 56, 62 (1992) ("[O]ur cases unmistakably hold that the Amendment protects property as well as privacy."). Courts must determine whether an individual has a property interest in the searched or seized items. If so, a warrant is required. Yet the district court hastily invoked the third-party doctrine to declare Harper's property interest nonexistent, and the First Circuit affirmed.

"[C]ourts are pretty rusty at applying the traditional [property] approach" in Fourth Amendment cases. *Carpenter v. United States*, 585 U.S. 296, 398 (2018) (Gorsuch, J., dissenting). However, judges need not fly blind—many states define digital records as private property, and some service providers grant ownership to customers. Americans are beginning to assert ownership of their digital records in Fourth Amendment cases, and some state courts are agreeing that customers own their digital records. *See People v. Seymour*, 536 P.3d 1260, 1273 (Colo. 2023) (holding that Google "users own their Google content" for Fourth Amendment purposes); *Ziegler v. Sarasota Police Dep't*, No. 2024-CA-001409-NC (Fla. Dist. Ct. App. July 1, 2024).

This Court should grant the petition, reverse the decision below, and clarify that courts cannot mechanically apply the third-party doctrine when someone makes a plausible claim of ownership of digital records seized or searched by the government.

ARGUMENT

I. FAILURE TO DETERMINE OWNERSHIP OF DIGITAL RECORDS CONSTITUTES REVERSIBLE ERROR.

The Fourth Amendment states that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated" and requires that warrants have "probable cause, supported by Oath or affirmation, and particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

This Court has noted "that the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity." *Riley v. California*, 573 U.S. 373, 403 (2014). Further, "[t]he purpose of the Fourth Amendment's requirement of reasonableness is to preserve that degree of respect for the privacy of persons and the inviolability of their property that existed when the provision was adopted—even if a later, less virtuous age should become accustomed to considering all sorts of intrusion 'reasonable.'" *Richards v. Wisconsin*, 520 U.S. 385, 392 n.4 (1997) (cleaned up). Lower courts have not always evaluated Fourth Amendment challenges with that history in mind.

A. Courts Must Evaluate Property Rights in Fourth Amendment Cases.

Prior to Justice Harlan's concurrence in *Katz v. United States*, 389 U.S. 347 (1967), when people challenged the validity of a warrantless search, courts

focused on property interests. This Court acknowledged that "our Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century." *United States v. Jones*, 565 U.S. 400 (2012). *See also Olmstead v. United States*, 277 U.S. 438, 458–66 (1928) (citing cases); *Ex parte Jackson*, 96 U.S. 727, 733 (1878) (establishing that the postal service needs a warrant before examining unopened mail and packages); *Larthet v. Forgay*, 2 La. Ann. 524, 525 (La. 1847) (holding that warrantless entry into a man's shop and apartment to look for stolen jewelry is an unreasonable search).

Then, in the mid-20th century, the Court seemingly "abandoned" the "property regime" and instead adopted *Katz*'s reasonable expectation of privacy test. Peter P. Swire, Katz *Is Dead—Long Live* Katz, 102 MICH. L. REV. 904, 904–05 (2004). The reasonable expectation of privacy test became the "'lodestar' for determining whether a 'search' had occurred" within the meaning of the Fourth Amendment. *Carpenter*, 585 U.S. at 346 (Thomas, J., dissenting). But the limits of *Katz* became apparent as government surveillance technologies and methods advanced. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 808 (2004).

This Court recognized *Katz*'s limited scope in *United States v. Jones*, 565 U.S. 400 (2012). In *Jones*, the suspect challenged the government's warrantless installation of a GPS tracking device on his vehicle as a violation of his Fourth Amendment rights. *Id.* at 403. The Court declined to apply the reasonable expectation of privacy test and instead relied on its traditional property-based analysis—concluding that the officers

violated the Fourth Amendment by intruding upon a constitutionally protected area. *Id.* at 410.

Jones signaled the rebirth of property rights as a touchstone of the Fourth Amendment. Writing for the majority, Justice Scalia explained: "*Katz* did not erode the principle 'that, when the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment.'" *Id.* at 407 (quoting *United States v. Knotts*, 460 U.S. 276, 286 (1983) (Brennan, J., concurring)). To hold otherwise would be to "narrow the Fourth Amendment's scope." *Id.* at 408. The Court reemphasized the importance of analyzing property concepts in Fourth Amendment search cases just one year after *Jones*. In *Florida v. Jardines*, 569 U.S. 1 (2013), the Court again endorsed the property-based approach over *Katz*.

B. Lower Courts Should Not Extend *Katz* and the Third-Party Doctrine to Digital Surveillance Cases.

Although *Jones* and *Jardines* reaffirmed the importance of property rights, lower courts too often resort to the *Katz* test—and the derivative "third party doctrine"—in Fourth Amendment cases involving sensitive records. Decades ago, this Court said that certain information that people turn over to commercial companies can be obtained by the government and searched without a warrant. *See United States v. Miller*, 425 U.S. 435 (1976) (holding that a depositor had no legitimate expectation of privacy concerning certain financial records held by a bank); *Smith v. Maryland*, 442 U.S. 735 (1979) (holding that a suspect had no legitimate expectation of privacy concerning phone

numbers he "conveyed" to a phone company via dialing phone numbers).

But this Court has not upheld a warrantless search or seizure under the third-party doctrine since *Smith* and *Miller*. Further, to the extent that the third-party doctrine is viable, the Court has made clear in recent cases involving searches of digital records that the government's analogies to the pre-digital, "manual" era of government surveillance often do not apply. *See Riley*, 573 U.S. at 386; *Carpenter*, 585 U.S. at 312 ("[T]he retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection . . . . Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years.").

In *Riley*, for instance, the Court prohibited the warrantless search of a digital storage device (both a "smart phone" and, in a companion case, a "flip phone"). In its decision, the Court rejected the government's extrapolation of legal precedents regarding traditional, often physical, records to digital records. *Riley*, 573 U.S. at 386. This Court, notably, cited government searches of years' worth of financial records as the troubling example of the invasive warrantless searches that would follow from the government's impermissible extrapolation from precedent: "The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years." *Id.* at 400.

Setting aside the viability of the third-party doctrine in digital records, the property approach allows courts to "keep easy cases easy." *Jardines*, 569 U.S. at

11. This traditional approach is not "hobbled by *Smith* and *Miller*, for those cases are just limitations on *Katz*, addressing only the question whether individuals have a reasonable expectation of privacy in materials they share with third parties." *Carpenter*, 585 U.S. at 398 (Gorsuch, J., dissenting) (emphasis removed). Instead, under the property-based approach, "Fourth Amendment protections for your papers and effects do not automatically disappear just because you share them with third parties." *Id. See also Ex parte Jackson*, 96 U.S. at 733.

C. The Courts Below Erred in Dismissing Harper's Claim That He Has a Property Interest in His Coinbase Records.

Our right to be secure in our "persons, houses, papers, and effects" does not "rise or fall" with the reasonable expectation of privacy test. *Jones*, 565 U.S. at 406; *see* U.S. CONST. amend. IV. As Justice Gorsuch has pointed out, "*Katz* has yielded an often unpredictable—and sometimes unbelievable—jurisprudence." *Carpenter*, 585 U.S. at 394 (Gorsuch, J., dissenting). There is a better way. Under the property-based approach, courts need only determine whether "a house, paper, or effect was *yours* under the law." *Id.* at 397. If so, the Fourth Amendment is triggered. The lower courts indefensibly ignored these principles and relied on the third-party doctrine to prematurely dismiss Harper's complaint.

Unfortunately, the courts below failed to properly consider Harper's property interests. In his appellate brief and submissions to the district court, Harper repeatedly asserted "contract rights as the basis of his property interest." Pet. Br. 25. Yet, "the First Circuit did not analyze Harper's contract." *Id.* at 26. In

refusing to meaningfully assess Harper's property interest in the digital records, the First Circuit's Fourth Amendment analysis remains incomplete.

The text and history of the Fourth Amendment demonstrates the close relationship between property rights and the right to be secure in one's papers and effects. *Soldal*, 506 U.S. at 62 ("[O]ur cases unmistakably hold that the Amendment protects property as well as privacy."). When a person claims he has a cognizable property interest in something the government has obtained, the courts cannot simply rebut that assertion with citation to the third-party doctrine. Even when someone conveys his personal property or records *to the government*, he may still have a property interest in them, and they cannot be searched without a warrant. *See Ex parte Jackson*, 96 U.S. at 733 ("Letters and sealed packages . . . in the mail are as fully guarded from examination and inspection . . . as if they were retained by the parties forwarding them in their own domiciles.").

While *Katz* "suppl[ies] one way to prove a Fourth Amendment interest," it is not and "has never been the only way"—and "[n]eglecting more traditional approaches may mean failing to vindicate the full protections of the Fourth Amendment." *Carpenter*, 585 U.S. at 405 (Gorsuch, J., dissenting). The courts below erred by shrugging off Harper's claims that he owns his Coinbase records.

The trial court decision made only oblique and brief reference to Coinbase's terms of service, never referencing the state property laws that govern Harper's agreement with Coinbase. Nor, apparently, did the court admit or request testimony from Coinbase representatives concerning who owned the records seized by

the IRS. But such testimony is vital to resolve a dispositive issue like ownership of the records. *See Seymour*, 536 P.3d at 1273 (citing the testimony of a Google employee regarding ambiguous terms of service about ownership of search history records). The district court's cursory property analysis in this case, and the First Circuit's affirmation, is especially confounding considering the court needed to draw all reasonable inferences in Harper's favor. *See Martino v. Forward Air, Inc.*, 609 F.3d 1, 2 (1st Cir. 2010).

Individuals must be afforded the same "degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo v. United States*, 533 U.S. 27, 34 (2001). The lower courts failed to properly analyze Harper's ownership interest based on the terms of the Coinbase agreements.

II. COINBASE USERS HAVE A STRONG ARGUMENT FOR OWNERSHIP OF THEIR DIGITAL RECORDS.

This Court has long recognized that contracts can create constitutionally protected property. *See United States Trust Co. v. New Jersey*, 431 U.S. 1, 19 n.16 (1977). In determining whether a reasonable expectation of privacy exists, this Court has directed lower courts to reference contract law and positive law as "[t]he central inquiry" when determining possession of effects. *See Byrd v. United States*, 584 U.S. 395, 409 (2018) (interpreting a rental car agreement to determine whether a suspect has a reasonable expectation of privacy while operating the vehicle). This Court should likewise make clear that such sources of law

are "central" when evaluating someone's claim of ownership of digital records.

A. Coinbase's User Agreement and Privacy Policy Arguably Recognize Users' Ownership of Their Digital Records.

Like many service providers, Coinbase's terms of service allocate property rights in the data, records, and communications produced by customers in the use of its services. These property interests are allocated and managed pursuant to Coinbase's user agreement and privacy policy, which "explicitly grant[] [the user] ownership of his records." Pet. Br. 24.

This Court recently illustrated how contracts establish property rights for individuals in the context of the Fourth Amendment. In *Byrd v. United States*, the Court rejected the proposition that only drivers listed on a rental agreement are entitled to Fourth Amendment protection when operating a rental car. 584 U.S. at 405. The rental contract gave the renter legal authority to possess and control the vehicle. The Court determined that when she later gave the defendant permission to drive the car, he was given "lawful possession and control and [the] attendant right to exclude." *Id.* at 407. It was based on these contractual rights that the Court found the defendant possessed a reasonable expectation of privacy in the vehicle. *Id.* at 406–07.

Contracts governing digital services likewise convey property interests—thus, Fourth Amendment protections—to users. In *People v. Seymour*, the Colorado Supreme Court held that the defendant owned his Google search history based on the rights afforded to him by Google's terms of service. 536 P.3d at 1273.

Relying on Google's privacy policies and user agreements, the court concluded that the defendant—not Google—owned his search history because the contract terms granted the defendant the right "to exclude and to control the dissemination and use of [his] digital data." *Id.* Thus, the government "interfere[d] with [his] possessory interest" by "infring[ing] on [his] right to exclude and to control" when it obtained copies of his digital records. *Id.*

Seymour and *Byrd* are instructive because in both cases, the contracts governing the defendants' use and possession also afforded them the right to control access to the property. To be sure, both cases implicated third parties—the car in *Byrd* was owned by a rental company but lawfully possessed by the defendant, and the search history in *Seymour* was generated by the defendant but processed, possessed, and stored by Google. But just because a third party lawfully *possesses* property doesn't mean the possessor *owns* the property. *See Carpenter*, 585 U.S. at 400 (Gorsuch, J., dissenting) (discussing bailment concepts and digital records).

Harper seems to have a property interest in his Coinbase records even though he did not possess them. When people use digital financial services, they share and produce personal information that can be sensitive, intimate, and privileged. That is why companies like Coinbase provide user agreements and privacy policies that allocate the bulk of rights to control and use personal data to customers. At any time, Coinbase users may request a copy of their personal information, request the deletion of their data, or withdraw or restrict consent for the processing of their personal information. *Coinbase Global Privacy Policy*,

COINBASE (last updated March 26, 2024).[7] In other words, users have the right to control how and when others access their information. This language leaves the general right to exclude all others from the digital records with the customer.

The contract-based property interests that apply to tangible effects and papers also apply to the storage and dissemination of digital information. Coinbase's terms of service appear to give users ownership over their digital data and records. That means the government cannot seize, store, or otherwise access those records without first obtaining a warrant.

B. Many States—Including Harper's—Expressly Recognize Residents' Ownership of Their Digital Records.

The contractual terms governing user data are not the only independent source of law supporting Harper's assertions of ownership in his Coinbase records. The laws vary, but most states define electronic data and digital records as private property. Many states have enacted laws and policies aimed at protecting users' ability to control how their digital data is stored and used. *See Carpenter*, 585 U.S. at 402 (Gorsuch, J., dissenting).

Positive law has "illuminate[d] the meaning of constitutional provisions" since the Founding. Trevor Burrus & James Knight, Katz *Nipped and* Katz *Cradled:* Carpenter *and the Evolving Fourth Amendment*, 2017–2018 CATO SUP. CT. REV. 79, 106 (2018). In the context of the Takings Clause, the definition of "property" is shaped by "existing rules or understandings

[7] Available at https://www.coinbase.com/legal/privacy.

that stem from an independent source such as state law." *Bd. of Regents of State Colleges v. Roth*, 408 U.S. 564, 577 (1972). The Takings Clause was not meant to be limited to the types of property that existed at the Founding—rather it was meant to protect private property *generally*. *See* William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1843 (2016). By using positive law as a guide, the Court has better preserved the original purpose of the Takings Clause and allowed the definition of property to accord with contemporary understanding.

For the same reasons, positive law is useful in the Fourth Amendment context. *See Carpenter*, 585 U.S. at 354 (Thomas, J., dissenting) (noting that "positive law is potentially relevant" to determining property ownership); *id.* at 403 (Gorsuch, J., dissenting) ("[P]ositive law may help provide detailed guidance on evolving technologies."). States and the federal government are actively working to enact protections for third-party data storage and digital privacy. *See id.* at 402 (Gorsuch, J., dissenting).

It's unclear which state's law governs Coinbase's terms of service obligations because the courts below did not ascertain that. However, Harper is a New Hampshire resident, and the relevant state laws strengthen his property rights argument. In addition to its privacy protection act, New Hampshire's criminal code broadly defines "property" as "anything of value, including . . . tangible and *intangible* personal property." N.H. REV. STAT. § 637:2(I) (2010) (emphasis

added).[8] And its law governing computer crimes explicitly defines "property" to include "[f]inancial instruments [and] computer data." N.H. REV. STAT. § 638:16(XVI)(c) (2022). New Hampshire is not alone. Today, more than half of all states have enacted or amended laws to include digital records and data in their definition of property.[9]

"[I]f state legislators or state courts say that a digital record has the attributes that normally make something property," that provides "a sounder basis for judicial decisionmaking than judicial guesswork." *Carpenter*, 585 U.S. at 402 (Gorsuch, J., dissenting). State laws make it illegal for private actors to access or use another person's digital data. By explicitly defining digital records as "property" and by enacting

---

[8] The New Hampshire law defines "value" as "the highest amount determined by any reasonable standard of property or services." N.H. REV. STAT. § 637:2(V) (2010).

[9] CONN. GEN. STAT. § 53-451(12) (2024); DEL. CODE tit. 11, § 931(15) (2024); GA. CODE § 16-9-92 (2023); HAW. REV. STAT. § 708-890 (2011); 720 ILL. COMP. STAT. 5/15-1 (2006); IOWA CODE § 702.14 (2025); KAN. STAT. § 21-3755 (2011); KEN. REV. STAT. § 514.010 (2005); KEN. REV. STAT. § 434.840 (2002); LA. STAT. § 73.1 (2019); ME. R. CRIM. PROC. 41(d) (2017); MD. CODE, CRIM. LAW § 7-101 (2025); MASS. GEN. LAWS ch. 266, § 30(2) (2025); MINN. STAT. § 609.52(1) (2024); MINN. STAT. § 609.87(6) (2024); MISS. CODE § 97-45-1(u) (2024); MONT. CODE § 45-2-101(65) (2023); NEV. REV. STAT. § 205.4755 (2024); N.J. REV. STAT. § 2C:20-1(g) (2024); N.Y. PENAL LAW § 156.00(3) (2025); N.C. GEN. STAT. § 14-453 (2012); N.D. CENT. CODE § 12.1-06.1-01(3)(h) (2023); OHIO REV. CODE § 2901.01(10)(a) (2023); OR. REV. STAT. § 164.377(j) (2024); S.C. CODE § 16-16-10(f) (2002); TENN. CODE § 39-14-601(17) (2024); TEX. PENAL CODE § 33.01(16) (2023); UTAH CODE § 76-6-702(5) (2023); VT. STAT. tit. 13, § 4101(8) (2024); WIS. STAT. § 943.20(2)(b) (2017); WYO. STAT. § 6-3-501(a)(x) (2024).

digital privacy statutes that give users the right to obtain, control, and delete their personal information, states have embraced the position that users often own their digital records.

It is necessary to rely on "democratically legitimate sources of law" to ensure that judges don't replace sound legal analysis with "their own biases or personal policy preferences." *Id.* at 398 (quoting Todd E. Pettys, *Judicial Discretion in Constitutional Cases*, 26 J.L. & POL. 123, 127 (2011)). Both contract law and state law support the conclusion that Harper owns his Coinbase records. The lower courts' mechanical reliance on the third-party doctrine elevates government officials and gives them the power to search and seize digital records in violation of state law and binding contracts.

CONCLUSION

For these reasons, and those described by the Petitioner, this Court should grant the petition.

Respectfully submitted,

Thomas A. Berry
Counsel of Record
Brent Skorup
Laura A. Bondank
CATO INSTITUTE
1000 Mass. Ave., N.W.
Washington, DC 20001
(443) 254-6330
tberry@cato.org

March 28, 2025