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

AMICUS CURIAE BRIEF OF KANSAS JUSTICE INSTITUTE, GOLDWATER INSTITUTE AND AMERICAN DREAM LEGAL IN SUPPORT OF PETITION FOR A WRIT OF CERTIORARI

TIMOTHY SANDEFUR
SCHARF-NORTON CENTER FOR CONSTITUTIONAL LITIGATION AT THE GOLDWATER INSTITUTE
500 East Coronado Road
Phoenix, AZ 85004

AARON R. RICE
AMERICAN DREAM LEGAL
611 Pear Orchard Rd., Unit 1614
Ridgeland, MS 39157

SAMUEL G. MACROBERTS
Counsel of Record
KANSAS JUSTICE INSTITUTE
12980 Metcalf Avenue, Suite 130
Overland Park, KS 66213
(913) 213-5018
sam.macroberts@kansasjusticeinstitute.org

Counsel for Amici Curiae Kansas Justice Institute, et al.

120364

QUESTIONS PRESENTED

1. 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?

2. If not, does the third-party doctrine need to be discarded or modified to prevent such searches?

TABLE OF CONTENTS

TABLE OF CITED AUTHORITIES

Page

Cases

Cited Authorities

Cited Authorities

Page

Constitutional Provisions

Other Authorities

Page

Cited Authorities

Page

INTEREST OF AMICI CURIAE[1]

Kansas Justice Institute (KJI) is a nonprofit, pro bono, public interest litigation firm committed to upholding constitutional freedoms, protecting individual liberty, and defending against government overreach and abuse. KJI directly litigates in state and federal courts, files amicus briefs, and comments on matters of public concern. KJI is a Kansas limited liability company whose sole member is Kansas Policy Institute, a nonprofit, nonpartisan public policy organization—a think tank—founded in 1996. In particular, KJI believes that the right to be free from warrantless searches and seizures is both a fundamental right and necessary to ensuring individual liberty, safeguarding personal privacy, and protecting against government intrusions of property interests. Since its inception, KJI has engaged in state and federal search and seizure litigation and continues to do so. *See, e.g., Johnson v. Smith*, 104 F.4th 153 (10th Cir. 2024).

The Goldwater Institute (GI) is a nonpartisan public policy and research foundation devoted to advancing the principles of limited government, individual freedom, and constitutional protections through litigation, research, and advocacy. Through its Scharf-Norton Center for Constitutional Litigation, GI litigates and files amicus briefs when its or its clients' objectives are implicated. Among GI's priorities is the enforcement of both state and federal constitutional protections against searches

1. All parties were timely notified of the filing of this brief. Counsel affirms that no counsel for any party authored this brief in whole or in part and that no person or entity other than *amici* made a monetary contribution to its preparation or submission.

and seizures. GI has appeared often in state and federal courts both as an amicus and representing parties in cases involving these concerns. *See, e.g., Mendez v. Chicago*, 228 N.E.3d 774 (Ill. 2023); *State v. Mixton*, 478 P.3d 1227 (Ariz. 2021); *State v. McNeill*, 2019 WL 4793121 (Ariz. Ct. App. Oct. 1, 2019); *State v. Hernandez*, 417 P.3d 207 (Ariz. 2018); *City of Charlestown v. Charlestown Pleasant Ridge Neighborhood Assn. Corp.*, 111 N.E.3d 199 (Ind. 2018). GI scholars have also published important scholarship on state constitutional protections against warrantless searches. *See* Timothy Sandefur, *The Arizona "Private Affairs" Clause*, 51 Ariz. St. L.J. 723 (2019).

American Dream Legal is a nonprofit, public interest law firm that believes in the transcendent power of the American Dream and is committed to extending its promise to people from every walk of life. American Dream Legal represent everyday people—free of charge—when the government obstructs their pursuit of the American Dream. The victories that American Dream Legal wins for its clients set lasting precedents that redeem the Dream's promise for one and all.

Amici believe their litigation experience and policy expertise will aid this Court in considering the petition.

INTRODUCTION AND SUMMARY OF ARGUMENT

Every day, millions of Americans engage in digital transactions through third-party platforms. They purchase stocks online, buy goods on Amazon, and pay the babysitter on Venmo. To do so, they must entrust their personal financial information to digital third-

party platforms. And each transaction is tracked. This reality is inescapable in a digital economy. So, too, for Petitioner James Harper, who entrusted Coinbase with his personal financial information to facilitate cryptocurrency transactions. He was one of 14,355 Coinbase account holders–spanning 8.9 million transactions–whose digital financial records were seized by the IRS without a warrant. Pet. App. 5-6. In effect, the IRS took Mr. Harper's digital wallet and the keys to unlock every transaction Mr. Harper made on Coinbase.

The First Circuit held that the IRS did not violate the Fourth Amendment when it seized the Coinbase records. In their view, Mr. Harper lacked a protectable privacy interest in them under the third-party doctrine. Pet. App. 3a, 13a-14a. In doing so, it relied on *United States v. Miller*, 425 U.S. 435 (1976), in which this Court held a person has no legitimate expectation of privacy in information voluntarily given to third parties, including bank records. *Id*. at 443-45. Applying *Miller*, the First Circuit reasoned that the Coinbase data "is directly analogous to the bank records" and thus "falls squarely within this 'third party doctrine[.]'" Pet. App. 3a.

The First Circuit's mechanical interpretation of *Miller* is ill-suited to the facts here. For one thing, *Miller* was decided in an era before pervasive password protection (or its equivalent)—a distinction that makes all the difference, as discussed below. But more importantly, the Fourth Amendment demands more than what this Court in *Carpenter v. United States*, 585 U.S. 296, 305 (2018), called a "'mechanical interpretation'" of constitutional doctrine that leaves Americans "'at the mercy of advancing technology.'" (quoting *Kyllo v. United*

States, 533 U.S. 27, 34-35 (2001)); *see also United States v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("[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."). Fortunately, state courts have done a good job of developing a better path. That is significant because the constitutional provisions on which those courts have relied are often similar, even identical, to the Fourth Amendment—and in some cases, antedate the Fourth Amendment, making them particularly suited to assist this Court in revisiting the third-party doctrine.

This is an issue that can no longer be avoided. Too many Americans now entrust their information to third parties, which renders them vulnerable to intrusions on their privacy under the *Miller* rule—intrusions that simply are not "reasonable" in the sense the Fourth Amendment intended. The Court should take this case to resolve that issue.

ARGUMENT

Mr. Harper's case is an excellent vehicle to address this incredibly important question. It hardly needs to be said that every day, hundreds of millions of Americans entrust information of the most private sort to third-party conveyors such as Gmail, Microsoft Outlook, or Apple's iCloud. To hold that in doing so, they have abandoned their right to be secure in their papers and effects, or that it is "reasonable" for the government to acquire this information without a warrant, is to elevate formalism over reality in the most extreme of ways.

Fortunately, history provides the answer. The Fourth Amendment was patterned after search and seizure clauses in state constitutions. This Court should therefore look to state constitutional jurisprudence as a persuasive and practical guide. State courts have, in fact, developed a robust body of caselaw—some echoing Justice Brennan's *Miller* dissent, others forging their own path—construing their search and seizure clauses in the context of the digital age and offering helpful guides. This Court should follow their lead and hold that a person has a constitutionally protectable privacy interest in financial records held by third parties, including those in digital form.

I. State Court Interpretations of State Constitutions That Contain Language Paralleling the Fourth Amendment Offers a Better Alternative to the *Miller* Doctrine

"Founding-era understandings" are a vital tool to interpreting and applying the Fourth Amendment in light of modern technology. *Carpenter*, 585 U.S. at 296-297. Indeed, as this Court has emphasized in recent years, the Fourth Amendment must protect, at a minimum, those rights recognized by the Founding-era common law. *See, e.g., Lange v. California*, 594 U.S. 295, 309 (2021); *Jones*, 565 U.S. at 411; *Gonzalez v. United States*, 145 S. Ct. 529, 532 (2025) (Sotomayor, J., respecting denial of certiorari).

Founding-era understandings, however, are informed not only by the experience of the Stuart monarchs or by British colonial practices, but also by state constitutional jurisprudence. *See* Jeffrey S. Sutton, *What Does—and Does Not—Ail State Constitutional Law*, 59 U. Kan. L. Rev. 687, 712 (2011) ("[S]ome state court rulings may help

inform the original meaning of language in the Federal Constitution that first appeared in state constitutions or may provide pragmatic reasons for following or steering clear of an approach embraced by the states."). This Court should consult state court rulings regarding the third-party doctrine.

Many state constitutions antedate the Fourth Amendment, and offer helpful guidance for application of their federal counterpart. Jack L. Landau, *Should State Courts Depart from the Fourth Amendment? Search and Seizure, State Constitutions, and the Oregon Experience*, 77 Miss. L.J. 369, 375–77 (2007). "State-level rights guarantees served as the model for many of the most familiar features of the Bill of Rights and of American constitutional law." Joseph Blocher, *What State Constitutional Law Can Tell Us About the Federal Constitution*, 115 Penn St. L. Rev. 1035, 1036 (2011); *see* William J. Brennan, Jr., *State Constitutions and the Protection of Individual Rights*, 90 Harv. L. Rev. 489, 501 (1977); Clint Bolick, *Principles of State Constitutional Interpretation*, 53 Ariz. St. L.J. 771, 773 (2021).

And "the early state constitutions created a positive right—namely, to be secure in one's person, house, papers, and effects against unreasonable search and seizure." Laura K. Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181, 1264 (2016). The Federal Constitution followed suit. Accordingly, early state constitutions—like Pennsylvania's—help inform the original meaning of the Fourth Amendment. *See id.* at 1267-69 (discussing early states' constitutional influence, including Pennsylvania's, on development of Fourth Amendment).

The Pennsylvania Constitution's search and seizure provision (Article I, § 8), is a good example. It closely resembles, but predates, its federal counterpart. It declares that "The people shall be secure in their persons, houses, papers and possessions from unreasonable searches and seizures," requires that warrants be as precise as possible, and bars warrants absent probable cause and an oath or affirmation.

From the adoption of that language in 1776 until the late twentieth century, Pennsylvania never adopted anything like the third-party doctrine. On the contrary, the Pennsylvania Supreme Court expressly rejected the *Miller* theory in *Com. v. De John*, 403 A.2d 1283, 1291 (Pa. 1979), when it held that a person has a privacy interest under the state constitution in personal records held by a bank. The court reasoned that under Section 8, "'[s]o long as a person seeks to preserve his effects as private, even if they are accessible to . . . others, they are constitutionally protected.'" Id. at 1289 (quoting *Com. v. Platou*, 312 A.2d 29, 34 (Pa. 1973)). Reasonably, a customer expects the records submitted to a bank will remain private. *Id.* at 1289. And practically, it is impossible to participate in modern economic life without a bank account. *Id.*

De John relied heavily on the California Supreme Court's ruling in *Burrows v. Superior Court*, 529 P. 2d 590 (Cal. 1974). That state's constitution also includes language strikingly similar to the Fourth Amendment: "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable seizures and searches may not be violated . . . ." Cal. Const. art. I § 13. The *Burrows* court explained that a bank customer "has a reasonable expectation of privacy in [her] bank

statements," and that this is not defeated by the customer's voluntarily handing over this information to the bank because "[a] bank customer's reasonable expectation is that, absent compulsion by legal process, the matters he reveals to the bank will be utilized by the bank only for internal banking purposes." *Id.* at 593. Thus, the theory—embraced in *Miller*—that by handing over bank records, the individual voluntarily surrenders his or her privacy rights *in toto* is untenable.[2] [3]

Notably, the *Burrows* approach makes better sense of the constitutional *text* than *Miller* does. The Fourth Amendment—like the Pennsylvania and California Constitutions—protects the people's right "to be secure in *their* persons, houses, papers, and effects." U.S. Const. Amend. IV (emphasis added). The possessive is significant because if, as *Carpenter* declared, "Fourth Amendment search doctrine [is] 'tied to common-law trespass,'" 585 U.S. at 304, then the fact that the bank customer *retains* ownership of the information even while giving it to the bank is surely relevant—and more so here, where the individual made a contract explicitly guaranteeing his retention of full ownership rights over the information in question.

---

2. Justice Brennan endorsed *Burrows* in his *Miller* dissent. *See Miller*, 425 U.S. at 447-454 (Brennan, J., dissenting).

3. As Justice Gorsuch asked in his dissent in *Carpenter*, 585 U.S. at 389, "[s]uppose I entrust a friend with a letter and he promises to keep it secret until he delivers it to an intended recipient. In what sense have I agreed to bear the risk that he will turn around, break his promise, and spill its contents to someone else?" This might seem a rhetorical question, but in *United States v. Payner*, 447 U.S. 727, 731–32 (1980), the Court applied *Miller* to permit the introduction of evidence that the government had obtained through a burglary that it organized.

Several other courts have likewise rejected the *Miller* rationale. In *Charnes v. DiGiacomo*, 612 P.2d 1117, 1120 (Colo. 1980), the Colorado Supreme Court held that the government may not obtain personal financial information from an individual's bank on the theory that by sharing that information with the bank, the individual voluntarily gives up his or her right to privacy.

Like the Pennsylvania and California Constitutions, the Colorado Constitution's language is effectively the same as that of the Fourth Amendment: "The people shall be secure in their persons, papers, homes and effects, from unreasonable searches and seizures . . . ." Colo. Const. art. II § 7. The *Charnes* court found that "bank transactions are not completely voluntary because bank accounts are necessary to modern commercial life," and that a customer shares information with a bank, not in order to voluntarily waive privacy rights, but to "facilitat[e] fund transfers." 612 P.2d at 1121.

In *People v. Jackson*, 452 N.E.2d 85 (Ill. App. 1983), too, the Illinois Court of Appeals rejected the *Miller* approach, holding instead that "an individual's reasonable expectation of privacy . . . is not bound by the location and present ownership of the records. Consequently, the right to privacy is not waived by placing these records in the hands of a bank. The individual can still legitimately expect that her financial records will not be subject to disclosure." *Id.* at 88.[4]

4. The Illinois Constitution does differ significantly from the Fourth Amendment in that, along with protecting the individual's "right to be secure in their persons, houses, papers and other possessions against unreasonable searches [and] seizures," it also explicitly protects privacy.

And in *State v. Thompson*, 810 P.2d 415 (Utah 1991), the state obtained defendants' financial information by subpoenaing their bankers, accountants, business associates, and companies with which they were associated. *See id.* at 416. Utah's constitutional warrant requirement uses language identical to the Fourth Amendment. *See* Utah Const. art. I § 14. Yet the court found that a bank customer only surrenders information to a bank "'upon the reasonable assumption that the information would remain confidential,'" *id.* at 418 (quoting *De John*, 403 A.2d at 1290), and that cannot be construed as an assumption of the risk or a waiver of constitutional protections.

More recently, in *State v. McAllister*, 875 A.2d 866 (N.J. 2005), the New Jersey Supreme Court rejected the *Miller* theory. "To be sure," it said, "bank customers voluntarily provide their information to banks, but they do so with the understanding that it will remain confidential." *Id.* at 874. (The New Jersey Constitution's warrant provision is written in language identical to the Fourth Amendment. *See* N.J. Const. art. I § 7.)

There are many more such examples. In fact, at least eleven state supreme courts have rejected the third-party doctrine in part or whole. *See* 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, 376, 396-399 (2006) (listing states and adding that "ten others have given some reason to believe they might reject it").

The reasoning shared by those state courts that have rejected the *Miller* rule applies with greater force to

digital records held by third parties today. As the *Burrows* court presciently observed,

> [T]he totality of bank records provides a virtual current biography. While we are concerned in the present case only with bank statements, the logical extension of the contention that the bank's ownership of records permits free access to … all papers which the customer has supplied to the bank to facilitate the conduct of his financial affairs upon the reasonable assumption that the information would remain confidential.

529 P.2d at 596.

So too in the Bitcoin era. Mr. Harper, and thousands of account holders like him, have a reasonable expectation of privacy in their Coinbase records, which depict a "virtual current biography" of all transactions they have and will make on the platform.

II. The *Miller* Rule Is Obsolete in a World of Ubiquitous Password Protection

The theory behind *Miller* was simple. It concerned the "reasonableness" component of the Fourth Amendment, and concluded that it was not "unreasonable" for the government to obtain the documents in question without a warrant because the accused had surrendered whatever privacy right he had when he let the bank make and keep copies of those documents. "The depositor takes the risk," the Court said, "in revealing his affairs to another, that the information will be conveyed by that

person to the Government." 425 U.S. at 443. In support of that proposition, the Court cited *United States v. White*, 401 U.S. 745 (1971), which said the Fourth Amendment "affords no protection to 'a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.'" *Id.* at 749 (quoting *Hoffa v. United States*, 385 U.S. 293, 302 (1966)).

Many have criticized this assumption-of-risk theory, but even laying that criticism aside, the theory is hard to take seriously 50 years later, in an era in which password protection has become ubiquitous. In 1976, it was plausible to say that a person who "voluntarily confides" in another is assuming the risk of that information being revealed. But in today's society—at least with respect to password-protected smartphones, password-protected online bank accounts, and password-protected email—it is far less plausible to suggest that the users of such technology are assuming the risk of disclosure, betrayal, or revelation.

One reason password protection and similar technological security measures—including those used here—are so relevant is precisely because of the word "their" in the Fourth Amendment. The *Miller* decision hinged almost entirely on the idea that the financial records at issue in that case *belonged to the bank*. The Court emphasized that they "are not respondent's 'private papers,'" and that a bank customer "reveal[s] his affairs to another." 425 U.S. at 440, 443. That is not true in today's environment, where password protection or other precautionary measures—and particularly the ones taken by Mr. Harper and Coinbase—ensure that the records *do* remain the person's private papers, and that the customer is *not* revealing his affairs to another. These technologies

make the information more like the contents of a sealed package than the address on the outside. *Cf. Ex parte Jackson*, 96 U.S. (6 Otto) 727, 735 (1877).

To put it another way, *Kyllo*, *Carpenter,* and *Jones* involved situations in which technology made possible intrusions into privacy that were unimaginable at the time of the Fourth Amendment. But this case shows that technology can also *expand* both the individual's subjective expectation of privacy and the reasonableness of that expectation—that is, society's "prepar[ation] to accept [those expectations] as reasonable." *O'Connor v. Ortega*, 480 U.S. 709, 715 (1987) (plurality opinion). In some ways, social life is less private than in 1973, but in many ways it is far *more* private.

That is manifested by the ubiquity of password protection or its equivalent—in this case, the stringent privacy controls contemplated by Mr. Harper's contract with Coinbase. In 1976, it may have been unreasonable to expect information transferred to a bank as part of a transaction to be kept private, just as it was unreasonable to expect the phone numbers one dialed to be kept private. *See Smith v. Maryland*, 442 U.S. 735 (1979). But in today's world, people have greater, not lesser, expectations of privacy with respect to certain information—particularly financial information—and society is more, not less, prepared to view those expectations as reasonable.

In 1976, a reasonable banking customer would likely know that "in the ordinary course of business," information conveyed to them would be kept and used in a manner that could not be reasonably characterized as "confidential communications." *Miller*, 425 U.S. at 743.

That's no longer the case. Bank customers can manage their finances on password-protected smartphones from the privacy of their own bedrooms, through the use of encrypted internet protocols and computer banks, without the intervention of a single human being. And customers today are more likely to object to the betrayal of such anonymity than they would have been in 1976, when most banking transactions had to be done in person at a bank, or with handwritten, hand-stamped documents that lacked any analog to password protection.

If one factor in considering whether to reevaluate a longstanding rule of law is the occurrence of "major legal or factual changes undermining [the] decision's original basis," *Dobbs v. Jackson Women's Health Org.*, 597 U.S. 215, 293 (2022), then the *Miller* rule is due for reconsideration, given the expansion of privacy options—and the greater use of those options—by Americans like Mr. Harper.

In *Riley v. California*, 573 U.S. 373 (2014), this Court recognized that "[t]he fact that technology now allows an individual to carry [private] information in his hand does not make the information any less worthy of the protection for which the Founders fought." *Id.* at 403. On the contrary, had it been possible for a person in the eighteenth century to carry around such private information, it is likely that the framers would have taken precautions to protect it.[5]

5. Probably the closest founding-era analogue is to the British Post Office, which began operating in the colonies in the 1710s. America's founders were well aware that the colonial branch of the Post Office was opening their letters and reading their mail—and that was one of the reasons why, in 1774, they founded an alternative, the "New American Post," also known as the

They did at least take a precaution to preserve Americans' right to "their" papers, effects, and other private matters. The *Riley* Court endorsed that precaution when it said: "Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant." 573 U.S. at 403.

III. A More Protective Fourth Amendment Jurisprudence Will Not Hinder Legitimate Investigations—But Will Better Preserve Constitutional Rights

State constitutional jurisprudence offers a persuasive alternative whereby the Court can apply the Fourth Amendment's original meaning to the Bitcoin era.

Not only have these state courts demonstrated a better grasp of the original meaning of the Fourth Amendment, but the alternative they offer is also practically compelling. The third-party doctrine "is untenable in a technological age where in the ordinary course of life, individuals will of necessity have disclosed a boundless amount of information to third parties." *State v. Walton*, 324 P.3d 876, 901 (Hawai'i 2014).

"Constitutional Post." *See* David J. Seipp, *The Right to Privacy in American History* 10-11 (Harvard Program on Information Resources Policy, July 1978), http://pirp.harvard.edu/pubs_pdf/seipp/seipp-p78-3.pdf. Unlike the King's Mail, letters in the Constitutional Post were kept "under lock and key, and liable to the inspection of no person but the respective Postmasters to whom directed, who shall be under oath for the faithful discharge of the trust reposed in them." 1 Peter Force, ed., *American Archives* 503 (1837). Many Patriots chose to write in code.

The "laboratories" of state constitutional jurisprudence have shown that the sky does not fall on the government's ability to prosecute crimes—let alone on the constitutional meaning of "reasonableness"—when the government is required to go through the simple process of obtaining a warrant (or its equivalent) to gain access to financial records.

Getting a warrant or its equivalent is not a difficult thing to do when law enforcement has reason to suspect a person of a crime. As Washington's Supreme Court observed—in a case holding that bank records may not be obtained without a warrant or a subpoena—"[o]btaining a judicially issued warrant or subpoena risks neither detection nor delay." *State v. Miles*, 156 P.3d 864, 871 (Wash. 2007). That is particularly true, given that—as Chief Justice Roberts observed in *Missouri v. McNeely*, 569 U.S. 141 (2013), more than half the states allow officers to obtain warrants electronically. "Judges have been known to issue warrants in as little as five minutes." *Id.* at 173 (Roberts, C.J., concurring).

Nor is there any reason to believe that the prosecution of crimes is less efficient due to state courts' rejecting the *Miller* theory. Although it is impossible to chart a precise statistical comparison, it is revealing that, for example, the rate of white-collar crime—presumably an area in which the third-party doctrine is regularly employed—is almost ten times higher in Richmond, Virginia, where the state courts follow the *Miller* doctrine, than in Los Angeles, where the state courts do not. Embezzlement is nearly fourteen times as common in Las Vegas, where state courts follow the doctrine, than in Sacramento, where they do not. Rabin Nabizadeh,

A Look at White Collar Crime in Cities Across the U.S., Summit Defense, Nov. 18, 2019.[6]

In their amicus brief to this Court in *Carpenter*, the National District Attorneys Association claimed that requiring law enforcement officers to obtain warrants before acquiring cellphone location information would "seriously impede[]" crime-fighting efforts. Br. Amicus Curiae of Nat. Dist. Attys. Assn., *Carpenter v. United States of America*, 2017 WL 4417212, at *24 (U.S. 2017). They noted that "[e]mbezzlement prosecutions, which create average losses for business and government agencies of well over one million dollars per year, and disproportionately affect smaller businesses, would also be seriously impeded." *Id.* But New York, which follows the *Miller* doctrine,[7] has 12.9 embezzlement cases per 100,000 population—whereas in Florida, which has rejected the *Miller* doctrine,[8] the rate is 13 per 100,000. Geoffrey G. Nathan, *The States with the Most and Least Embezzlement Cases*, FederalCharges.com.[9] Ohio, which follows the *Miller* doctrine,[10] has a rate of 11.9 per 100,000, while Illinois, which rejects it,[11] has a rate of 12.6 per 100,000. *Id.* There is no reason to believe embezzlement is better combatted under the *Miller* rule than without it.

6. https://summitdefense.com/blog/white-collar-crime-us/.

7. *See People v. Guerra*, 478 N.E.2d 1319, 1321 (N.Y. 1985).

8. *See Shaktman v. State*, 553 So. 2d 148, 151-52 (Fla. 1989).

9. https://www.federalcharges.com/the-states-with-the-most-and-least-embezzlement-cases/ (visited Mar. 19, 2025).

10. *See Ohio Domestic Violence Network v. Pub. Utils. Comm.*, 638 N.E.2d 1012, 1019 n.3 (Ohio 1994).

11. *See Jackson, supra.*

The National District Attorneys Association also pointed to insurance fraud as a crime that would be harder to investigate and prosecute if the *Miller* rule were limited. 2017 WL 4417212, at *24. But in 2022-23, there were 4,094 reports of suspected fraud in California (which rejects the *Miller* rule), *see* Property, Life and Casualty Fraud, Cal. Dept. of Insurance,[12] whereas in 2024, in Michigan—which follows the *Miller* rule—there were 3,789. Mich. Dept. of Ins. & Fin. Svcs., *2024 Fraud Investigation Unit Annual Report* at 5.[13] There is simply no reason to believe that abandonment or limitation of the *Miller* rule has made it harder for states to prosecute insurance fraud.

In short, state court jurisprudence on this question offers a pragmatic path forward, already trod for decades, which harmonizes the original meaning of the Fourth Amendment with the realities of the wealth of personal data created and stored by third parties in the digital age. And there is no reason to believe that a more rigorous enforcement of the search warrant requirement will hinder the authorities in enforcing the law.

12. https://www.insurance.ca.gov/0300-fraud/0100-fraud-division-overview/10-anti-fraud-prog/Property-Life-Casualty.cfm (visited Mar. 19, 2025).

13. https://www.michigan.gov/difs/-/media/Project/Websites/difs/FIU/FIU_Annual_Report_2024.pdf (visited Mar. 19, 2025).

CONCLUSION

As Justice Sotomayor noted in *Jones*, it is not plausible to "assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." 565 U.S. at 418 (Sotomayor, J., concurring). State courts, interpreting constitutional clauses with language identical to the Fourth Amendment—indeed, clauses that sometimes antedate that amendment—have offered a better path, and this Court should choose this opportunity to take it. The petition should be *granted*.

Respectfully submitted,

Timothy Sandefur
Scharf-Norton Center
for Constitutional
Litigation at the
Goldwater Institute
500 East Coronado Road
Phoenix, AZ 85004

Aaron R. Rice
American Dream Legal
611 Pear Orchard Rd.,
Unit 1614
Ridgeland, MS 39157

Samuel G. MacRoberts
Counsel of Record
Kansas Justice Institute
12980 Metcalf Avenue,
Suite 130
Overland Park, KS 66213
(913) 213-5018
sam.macroberts@
kansasjusticeinstitute.org

Counsel for Amici Curiae
Kansas Justice Institute, et al.