No. 24-922

# In the Supreme Court of the United States

JAMES HARPER,

*Petitioner*,

v.

DOUGLAS O'DONNELL, ACTING COMMISSIONER OF THE INTERNAL REVENUE SERVICE,

*Respondent*.

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

## BRIEF OF *AMICI CURIAE* STATES OF WEST VIRGINIA, KANSAS, NEBRASKA, NORTH DAKOTA, AND OHIO IN SUPPORT OF PETITIONER


JOHN B. MCCUSKEY
*Attorney General*

OFFICE OF THE WEST VIRGINIA ATTORNEY GENERAL
State Capitol Complex
Building 1, Room E-26
Charleston, WV 25305
mwilliams@wvago.gov
(304) 558-2021

MICHAEL R. WILLIAMS
*Solicitor General*
*Counsel of Record*

FRANKIE DAME
*Assistant Solicitor General*

*Counsel for* Amicus Curiae *State of West Virginia*
[additional counsel listed after signature page]

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

**Page(s)**

**Cases**

**TABLE OF AUTHORITIES**
(*continued*)

**Page(s)**

**TABLE OF AUTHORITIES**
(*continued*)

**Page(s)**

**TABLE OF AUTHORITIES**
(*continued*)

**Page(s)**



**Constitutional Provisions**

## TABLE OF AUTHORITIES
(*continued*)

**Page(s)**

### Statutes



### Other Authorities

**TABLE OF AUTHORITIES**
(*continued*)

**Page(s)**

**TABLE OF AUTHORITIES**
(*continued*)

**Page(s)**

**TABLE OF AUTHORITIES**
(*continued*)

**Page(s)**

**TABLE OF AUTHORITIES**
(*continued*)

**Page(s)**

**TABLE OF AUTHORITIES**
(*continued*)

**Page(s)**

**TABLE OF AUTHORITIES**
(*continued*)

**Page(s)**

**TABLE OF AUTHORITIES**
(*continued*)

**Page(s)**

## INTRODUCTION AND INTERESTS OF *AMICI CURIAE*[*]

Some governmental powers are so potent that our constitutional system of ordered liberty takes them out of "the hands of the government." *District of Columbia* v. *Heller*, 554 U.S. 570, 634 (2008). A dragnet search of thousands upon thousands of people's intimate financial records, for example. Yes, the search might help investigators solve crimes. But the Founders long ago decided that—whatever an invasive fishing expedition's contribution to order—it isn't worth the corresponding loss of liberty. "The very existence of" such a "tremendous power" "renders it susceptible to abuse and endangers" citizens' "fundamental personal liberties." *Zweibon* v. *Mitchell*, 516 F.2d 594, 604 (D.C. Cir. 1975).

This case shows how such essentials have been too often forgotten. Here, the Internal Revenue Service conducted a warrantless dragnet search of 14,355 Coinbase accounts' registration information. With no court signoff, the government trawled through reams of identifying customer details: "records of account activity including transaction logs or other records identifying the date, amount, and type of transaction," "the post transaction balance, and the names of counterparties to the transaction" (about 9 million transactions total); and account statements and invoices. Pet.App.8a. Everything about this expedition looks like a search. See U.S. CONST. amend. IV. Yet the First Circuit said it wasn't because it fell "squarely within this 'third party doctrine' line of precedent." Pet.App.13a.

---

[*] Under Supreme Court Rule 37, *amici* timely notified counsel of record of their intent to file this brief.

Surely Fourth Amendment protections are not "really so tepid that the government can accidentally-on-purpose gather and scrutinize enormous quantities of" data with only a "perfunctory dismissal under the third party doctrine." Nicole B. Cásarez, *The Synergy of Privacy and Speech*, 18 U. PA. J. CONST. L. 813, 871 (2016). The Fourth Amendment should evenly "balance[]" civil liberty and law enforcement. *Hiibel* v. *Sixth Jud. Dist. Ct.*, 542 U.S. 177, 178 (2004). And that "balance" should "tilt[] in favor of freedom from police interference." *Brown* v. *Texas*, 443 U.S. 47, 52 (1979). After all, solving crimes "occupies a lower place in the American pantheon of noble objectives than the protection of our people from suspicionless law-enforcement searches." *Maryland* v. *King*, 569 U.S. 435, 481 (2013) (Scalia, J., dissenting).

Yet the third-party doctrine as it's applied today—unqualifiedly to financial records, with hardly a nod to major technological innovations—has distorted the Fourth Amendment's delicate balance, elevating order over liberty. And although the third-party doctrine is among today's most "weighty constitutional issues," *ACLU* v. *Clapper*, 785 F.3d 787, 824 (2d Cir. 2015), it has received little attention in recent years from this Court. That position of neutrality has allowed the doctrine to mutate into something else entirely. It thus deserves to be the Court's "central focus" again. Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1331 (2012).

Now, then, is the time to act. Third-party doctrine questions are "aris[ing] with increasing frequency" as our economy relies more on companies storing and aggregating "vast amounts of data." *State* v. *Ghim*, 381 P.3d 789, 795 (Or. 2016). Although these "[r]apid changes in technology," *State* v. *Walton*, 324 P.3d 876, 908 (Haw.

2014), have led to "large aggregat[ions] of personal data," "the law has not progressed in response," Helen Winters, *An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants*, 107 MINN. L. REV. 1369, 1385 (2023). That's led to "gaps" in constitutional protections—and these gaps are growing. *Id.* At the same time, our "technological environment" "can only function by providing information to third parties." Daniel Gelb & Richard Gelb, *Framing the Third-Party Doctrine Around Society's Dependence on the Cloud, Artificial Intelligence, and the Internet of Things*, 48 CHAMPION 30, 39 (Sept. 2024). So it's "inevitable" that this Court "will have to continue to revisit" this issue. *Id.*

The Court should grant the petition and lay at least some of these questions—and abuses—to rest.

## SUMMARY OF ARGUMENT

**I.** The Court should apply *Carpenter*'s reasoning to *Miller* and overturn it.

*Carpenter* exempted cell site location information (or CSLI) from the third-party doctrine because it effectively painted an involuntary but nevertheless comprehensive and revealing picture of a person's life. Financial information does the same. Knowing how a person spends her money reveals everything from her politics to her love life to her doctors. A dozen States have been consistently saying just that for fifty years. Most legal scholars (alongside several of this Court's justices) have agreed. And because people can't participate in society without banking—and online banking in particular—sharing financial details with a financial institution is involuntary.

*Miller* is right that a person loses *some* privacy when she banks. But it was wrong to treat privacy as an all-or-nothing commodity. A person can reveal their financial data to a bank and still reasonably believe that it will be kept private—a reality the Constitution should acknowledge.

**II.** Alternatively, the Court should grant the petition to address the ever-increasing danger of dragnet searches under the third-party doctrine.

This Court has long been sensitive to how the Fourth Amendment interacts with technology. Exponential increases in data collection (internet of things), storage (the cloud), and processing (quantum computing and artificial intelligence) have upended the third-party doctrine. A tech-blind, absolutist third-party doctrine will greenlight dragnet acquisitions and searches of anything from dating-app information to comprehensive consumer data to DNA test results. These activities implicate First Amendment protections, too.

One solution is to ban dragnet searches resting on the third-party doctrine, limiting *Miller* to identified-suspect searches. This cabining is easy to reconcile with *Miller*'s facts, which were nothing like a dragnet search. And it's more consonant with American jurisprudence's dislike of governments' "exploratory rummaging."

## ARGUMENT

Fourth Amendment protections today aren't what the Founders hoped they would be. The provision was largely "a reaction to the evils of the use of the general warrant in England and the writs of assistance in the Colonies." *Warden, Md. Penitentiary* v. *Hayden*, 387 U.S. 294, 301 (1967). British officials used these tools to

indiscriminately and generally search whomever and wherever they wanted. That intrusion then became a "driving force[] behind the Revolution." *Riley* v. *California*, 573 U.S. 373, 403 (2014). Indeed, such measures might have been "perhaps the *most* prominent event which inaugurated" the Revolution. *Boyd* v. *United States*, 116 U.S. 616, 625 (1886) (emphasis added).

The Fourth Amendment's central purpose was partially undermined by *United States* v. *Miller*, 425 U.S. 435 (1976). There, the government accessed without a warrant about three months' worth of Mr. Miller's "savings, checking, loan," and "other[]" records, including "checks, deposit slips," and financial and monthly statements. *Miller*, 425 U.S. at 437-38. Because Miller "voluntarily conveyed" this information to his bank and its employees, the Court said, he lacked a reasonable expectation of privacy in that financial information—even though he shared it "for a limited" commercial "purpose." *Id.* at 442-43. As future courts recognized, *Miller*'s absolute language left little (really, no) room for exceptions.

To many, *Miller* was "dead wrong" from the start. Wayne LaFave, *Examination of financial and other business records*, *in* 1 SEARCH & SEIZURE § 2.7(c) (6th ed., 2024); Nadine Strossen, *Beyond the Fourth Amendment: Additional Constitutional Guarantees That Mass Surveillance Violates*, 63 DRAKE L. REV. 1143, 1150 (2015) (saying it has always "been strongly criticized"). Justices Douglas, Marshall, and Brennan all flagged issues with *Miller* and its underlying rationale. *Cal. Bankers Ass'n* v. *Shultz*, 416 U.S. 21, 71-99 (1974) (dissenting opinions); *Miller*, 425 U.S. at 447-56 (same). Scholarly consensus was that *Miller*'s under-reasoned, sweeping conclusion did "great violence" to Fourth

Amendment Protections. LaFave, *supra*, § 2.7(c). Most everyone saw that "unrestricted government access" to "massive" tranches of financial records "pose[d] a severe threat to civil liberties and privacy." *Id.*

Congress and the States did what they could, responding to *Miller* by passing legislation protecting financial privacy. Those efforts strongly telegraphed that *Miller* took "too narrow a view of societal expectations of privacy." *Everett* v. *State*, 186 A.3d 1224, 1233-34 (Del. 2018) (discussing the Right to Financial Privacy Act); see, *e.g.*, N.H. REV. STAT. § 359-C:8-C:10 (state analog to RFPA). And some States eventually constitutionally protected electronic records. See MICH. CONST. art. I, § 11; MO. CONST. art. I, § 15.

But this Court took perhaps the biggest step forward about seven years ago, in *Carpenter* v. *United States*, 585 U.S. 296 (2018). There, the Court struck a blow to the unqualified third-party doctrine when it held that the doctrine doesn't apply to CSLI. The Court explained that CSLI offers "an intimate window into a person's life, revealing" their "familial, political, professional, religious, and sexual associations" and showing the "privacies of life." *Id.* at 311. And it wasn't fair to say that cellphone users were "voluntarily" giving third parties their location data. *Id.* at 315. *Carpenter* didn't "resolve[]" all "pre-existing [third-party doctrine] confusions." Ayesha K. Rasheed, *Personal Genetic Testing and the Fourth Amendment*, 2020 U. ILL. L. REV. 1249 (2020). But it at least showed that "the third-party doctrine no longer applies automatically," LaFave, *supra*, § 2.7(c).

The Court should grant this petition and make good on *Carpenter*'s promise. It should revisit (and overturn) *Miller* or, at least, limit dragnet searches under *Miller*.

## I. The Court should grant the petition to recognize a reasonable expectation of privacy in financial records.

**A.** This Court should grant certiorari and apply the same factors to financial records that it used in *Carpenter*: the data's (1) "deeply revealing nature"; (2) its "depth, breadth, and comprehensive reach"; and (3) its "inescapable," effectively involuntary collection. And in applying those factors, state jurisprudence can help light the way forward.

First, federal courts can rely on "state courts" to better discern the order-liberty balance. Robert J. Delahunty & John Yoo, *Against Foreign Law*, 29 HARV. J.L. PUB. POL'Y 291, 295 (2005). States handle "the vast majority of criminal prosecutions," giving them "comparative expertise in" criminal law and Fourth Amendment-like issues, *People* v. *McKnight*, 446 P.3d 397, 407 (Colo. 2019) (discussing third-party doctrine). And with non-federal law-enforcement officers outnumbering federal law-enforcement officers by nearly ten-to-one, States have more on-the-ground experience in criminal law, too.

Second, state courts have been much quicker than their federal counterparts to treat *Carpenter* as a meaningful advance in the Court's third-party doctrine. From 2018 to 2021, state courts applying *Carpenter* found searches three times more often than federal courts. Matthew Tokson, *The Aftermath of* Carpenter*: An Empirical Study of Fourth Amendment Law, 2018-2021*, 135 HARV. L. REV. 1790, 1811-12 (2022) (~60% of the time versus ~20%). This variance is, in part, because state courts don't think in terms of *Miller*'s "broad third-party doctrine" alone. Matthew Radford, *Back to the Future: Revisiting State Constitutions to Protect Against New Technological Intrusions*, 81 WASH. & LEE L. REV. 1641,

1661 (2024); see also Tokson, *supra*, at 1814 (agreeing state courts are "less biased in favor of the pre-*Carpenter* status quo").

Third, States have long provided more robust constitutional protections against unreasonable searches and seizures in myriad situations. Radford, *supra*, at 1663-76 (cataloging examples including pole cameras, recording conversations, reverse keyword searches, drug dog sniffs, and others); see also *Commonwealth* v. *Augustine*, 4 N.E.3d 846, 858 (Mass. 2014) (noting it provides "more substantive protection" than the Fourth Amendment). That more robust approach hews closer to the Framers' understanding of the Fourth Amendment. See Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 749 (1999) ("The authentic history shows that framing-era doctrine provided a much stronger notion of a 'right to be secure' in person and house than does modern doctrine.").

Applying those factors, the result becomes clear: *Miller* was wrong to categorically exclude financial records from ordinary Fourth Amendment protections. Indeed, many States reject *Miller* and constitutionally protect financial records from warrantless searches. See generally 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 (2006). "It cannot be gainsaid," many States have recognized, that a person "reasonabl[y]" expects that "the matters he reveals to the bank," including his bank "documents" like checks, will "remain private." *Burrows* v. *Superior Court*, 529 P.2d 590, 593 (Cal. 1974); see also, *e.g.*, *Commonwealth* v. *DeJohn*, 403 A.2d 1283, 1290 (Pa. 1979); *Winfield* v. *Div. of Pari-Mutuel Wagering, Dep't of Bus. Regul.*, 477 So. 2d

544, 548 (Fla. 1985); *In re May 1991 Will Cnty. Grand Jury*, 604 N.E.2d 929, 937 (Ill. 1992); *Schroeder* v. *Utah Att'y Gen.'s Off.*, 358 P.3d 1075, 1081 (Utah 2015); *State* v. *Andrews*, 234 A.3d 1254, 1292 n.7 (N.J. 2020).

State court jurisprudence (and other authorities) shows that *Carpenter*'s "privacy and lack-of-free-choice concerns" apply "equally" to "financial records." Jeremy Connell, *You Can't Teach Old* Katz *New Tricks: It's Time to Revitalize the Fourth Amendment*, 78 U. MIAMI L. REV. 171, 221-22 (2023). The Court should grant the petition and hold the same.

**1.** Take *Carpenter*'s first two factors—whether the information is deeply revealing and how comprehensive it is. State courts say "discrete" financial information—and especially a year's worth of *every* transaction detail—tells a great deal about a person's life. *Samson* v. *State*, 919 P.2d 171, 173 (Alaska Ct. App. 1996); *State* v. *Kluss*, 867 P.2d 247, 254 (Idaho Ct. App. 1993). Financial records may look like a mass of undifferentiated "numbers, symbols, dates, and tables"—"a veritable chronicle of" otherwise "mundane" fees, deposits, interest, and other interactions. *State* v. *McAllister*, 875 A.2d 866, 874 (N.J. 2005). But "compiled and indexed," these "individually trivial transactions take on a far greater significance"—serving as "detailed financial dossiers," thoroughly "memorializ[ing] an individual's affairs." *Id.* (cleaned up). They show what a "citizen buys, how often, and from whom"; "what political, recreational, and religious organizations a citizen supports"; and where the citizen travels, their affiliations, reading materials, television viewing habits, financial condition, and more." *State* v. *Miles*, 156 P.3d 864, 869 (Wash. 2007); see also *State* v. *Domicz*, 907 A.2d 395, 403 (N.J. 2006) (listing many more categories).

Financial records thus "reveal[] many aspects of [a person's] personal affairs, opinions, habits and associations." *Burrows*, 529 P.2d at 596. All told, his "checks, savings, bonds, loan applications, loan guarantees," and other details give the bank a "virtual current biography." *Id.*; accord *Andrews*, 234 A.3d at 1292 n.7 (same); *People* v. *Nesbitt*, 938 N.E.2d 600, 605 (Ill. Ct. App. 2010); *State* v. *Thompson*, 810 P.2d 415, 418 (1991) (same); see also *RDT Constr. Corp.* v. *Contralor I*, 141 D.P.R. 424, 442 (1996) (saying financial records reveal "intimate" "patterns and lifestyles"—including a person's occupation, his haunts and goods, his political party and church, and his reading material and associations). Cryptocurrency financial records reveal the same. Noah Lesiuk, *Ushering in A New Era: Assessing the Reasonable Expectation of Privacy Vis-à-Vis Cryptocurrency and Blockchain Data*, 46 MAN. L.J. 206, 228 (2024) (searching "cryptocurrency storage mediums … quite obviously uncovers the intimate details of one's personal choices and lifestyle").

Several of this Court's justices have agreed. As Justice Kennedy (joined by Justice Thomas and Justice Alito) said in dissent in *Carpenter*, "troves of intimate information" gleanable from "financial records … dwarf[] what can be gathered from cell-site records." *Carpenter*, 585 U.S. at 337. Echoing many state court cases, financial records reveal people's purchases, their salaries, their preferred "political and religious organizations," their doctors (including a potential "psychiatrist, plastic surgeon, abortion clinic, or AIDS treatment center"), and whether they frequent "gay bars or straight ones." *Id.* Decades earlier, Justice Douglas had said the same: financial records show a person's "doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, … and so on ad infinitum." *Cal.*

*Bankers*, 416 U.S. at 85 (Douglas, J., dissenting). Because these financial records "touch upon intimate areas of an individual's personal affairs," including their "activities, associations, and beliefs," at some point it "implicate[s] legitimate expectations of privacy." *Id.* at 78-79 (Powell, J., concurring); see also *Miller*, 425 U.S. at 447-54 (Brennan, J., dissenting) (accepting *Burrows*).

**2.** State courts also say that financial records meet *Carpenter*'s third factor: involuntary sharing. *Carpenter* said CSLI wasn't "truly 'shared'" because having a phone is "indispensable to participation in modern society." *Carpenter*, 585 U.S. at 315. Sharing financial records, too, "is not entirely volitional" because it's "impossible to participate in the economic life of contemporary society without maintaining a bank account." *Burrows*, 529 P.2d at 596; accord *Thompson*, 810 P.2d at 418; *Nesbitt*, 938 N.E.2d at 605. Next to no one could transact all (or even a fraction) of their business in person and with "cash"—making financial institutions "indispensable." *McAllister*, 875 A.2d at 874. Banking is "necessary to modern commercial life." *Charnes* v. *DiGiacomo*, 612 P.2d 1117, 1121 (Col. 1980); cf. *RDT*, 141 D.P.R. at 441 ("resort[ing] to banking institutions" is "practically a necessity … to participate adequately in economic life").

So *Miller* was wrong to call banking "a true disclosure to a third party." *Charnes*, 612 P.2d at 1121; *People* v. *Seymour*, 536 P.3d 1260, 1272 (Colo. 2023). Disclosing financial information to third parties is an "inevitable and inescapable" function of modern society; because there is "no realistic alternative," doing so isn't really "voluntary." *Walton*, 324 P.3d at 906, 908. And if *Miller* impliedly suggests that a person should just disconnect from the grid to shield their privacy interests, then that's too much to ask. The Constitution doesn't require citizens to take

"[extra]ordinary" steps to "veil their affairs in secrecy." *State* v. *Hinton*, 319 P.3d 9, 15 (Wash. 2014); see also Luiza M. Leão, *A Unified Theory of Knowing Exposure: Reconciling* Katz *and* Carpenter, 97 N.Y.U. L. REV. 1669, 1690 (2022) (saying the Fourth Amendment doesn't impose a proactive "duty of secretiveness on individuals").

Banking *online* is inescapable, too. As the Fifth Circuit put it, "[g]iven the ubiquity—and necessity—in the digital age of entrusting corporations" like banks with our data, the third-party doctrine's original voluntary-relinquishment theory is "dubious." *United States* v. *Smith*, 110 F.4th 817, 834-35 (5th Cir. 2024). That we "need to use" the internet "to meaningfully participate in society," Leão, *supra*, at 1690, means we now leave digital financial "third-party trails" everywhere, Cásarez, *supra*, at 871. This widespread digitization of commerce "eviscerat[es]" *Miller*'s "outdated" reasoning. *Id.* Because "communicating and sharing" our financial details "through third parties' technology is a necessary condition of existence," *Miller* is "unsupportable in the big data surveillance era." Avidan Y. Cover, *Corporate Avatars and the Erosion of the Populist Fourth Amendment*, 100 IOWA L. REV. 1441 (2015); cf. Tyler O'Connell, *Two Models of the Fourth Amendment and Hashing to Investigate Child Sexual Abuse Material*, 53 U. PAC. L. REV 293, 323-26 (2021) (because third parties are "the true gatekeepers of" our "personal data," *Miller* "is entirely untenable" and has "lost [its] force in the digital era").

**B.** Other of *Miller*'s assumptions were wrong, too—chiefly that voluntarily disclosing certain information for commercial purposes vitiates *all* other privacy expectations. *Miller*, 425 U.S. at 443. To the contrary, when individuals disclose sensitive information to an

institutional third party, they normally and reasonably expect the "information will not be disclosed to others for [extracurricular] purposes." *Walton*, 324 P.3d at 906. There are "some third-party institutions" that deal with such sensitive information that "sharing private information in" those sacrosanct "spaces does not destroy" but confirms "someone's reasonable expectation of privacy." *State* v. *Leonard*, 943 N.W.2d 149, 159 (Minn. 2020).

Banks and other financial institutions, for example. A bank customer does not intend the act of banking itself to grant permission to reveal the "substance" of his financial affairs to the world. *Charnes*, 612 P.2d at 1121; accord *McAllister*, 875 A.2d at 874. Indeed, "[d]isclosure of personal financial information, … instead of benefiting the industry, would violate the legislatively and judicially recognized right to privacy of personal financial information established by Congress when it enacted the Financial Privacy Act." Laurie Durcan & Bruce K. Riordan, *Banking Disclosures, Financial Privacy, and the Public Interest*, 6 ANN. REV. BANKING L. 391, 403 (1987).

No doubt sharing financial details with a bank somewhat diminishes privacy. But just because someone "has diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely." *Riley*, 573 U.S. at 392. A person may not, for example, be reasonably entitled to "privacy in his backyard" from "parents looking for lost" kids even while he is reasonably entitled to privacy from "policemen making a 'dragnet' search of … a whole neighborhood" hoping to "find some evidence of some crime." *State* v. *Hempele*, 576 A.2d 793, 805 (N.J. 1990). Similarly, even if a bank knows some things about a customer, it doesn't follow that the

customer "is indifferent to having those affairs … disclosed to the government." RICHARD POSNER, THE ECONOMICS OF JUSTICE 342 (1981).

*Miller* justified its all-or-nothing approach by saying governments accessing bank records discover only what "the bank customer expected bank employees to be aware of." LaFave, *supra*, § 2.7(c). But that's wrong. Most often, bank employees see only bits of uncontextualized information for just a moment. They then may see hundreds or thousands of other bits of information before they run across the same account again. That's especially true today, when nearly all transactions happen "remotely" and "without interacting with bank employees at all." Connell, *supra*, at 221. Except in very specific cases involving an expressly consented-to disclosure—like, say, applying for a mortgage—individuals don't expect that anyone at the bank will have reason or occasion to make themselves "aware" of *all* their private financial interests. *Burrows*, 529 P.2d at 593 ("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.").

It only takes a basic exercise to reject *Miller*'s premise in the modern world. Imagine a customer discovering that a random bank employee had plotted out her financial transactions for the past year, including *every* purchase she'd made. She would feel violated—and reasonably so. We do not expect a bank or its employees to map our entire financial history. LaFave, *supra*, § 2.7(c) (saying a customer would be shocked to discover that her financial institution or its employees had comprehensively reviewed her finances to "construct accurate conclusions about [her] lifestyle"). If anything, this expectation has

increased since *Miller*. See Kevin Johnson, *The Use of Clearview AI to Support Warrants Violates the Fourth Amendment*, 34 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 991, 1017 (2024). Indeed, Americans are now "more resistant to law enforcement access to their financial records" than access to their "internet use," "medical records," or facial scans. Aditi A. Prabhu, *Contracting for Financial Privacy: The Rights of Banks and Customers Under the Reauthorized Patriot Act*, 39 LOY. U. CHI. L.J. 51, 84 (2007).

*Miller* has always been wrong; the Court should grant the petition to say so.

## II. Alternatively, the Court should grant the petition to clarify that *Miller* doesn't extend to suspect-less dragnet searches.

**A.** Technology has "[]affected" Fourth Amendment privacy protections. *Kyllo* v. *United States*, 533 U.S. 27, 33-34 (2001). This Court and its justices have warned time and again that Fourth Amendment jurisprudence must be technology sensitive. "[T]ime works changes," Justice Brandeis said, meaning "[s]ubtler and more far-reaching means of invading privacy … become available to the government." *Olmstead* v. *United States*, 277 U.S. 438, 473-74 (1928) (Brandeis, J., dissenting).

The Court therefore "reject[s] … mechanical interpretation[s] of the Fourth Amendment" that "leave" citizens "at the mercy of advancing technology" and "take account of more sophisticated," developing technology. *Kyllo*, 533 U.S. at 36. A "Fourth Amendment jurisprudence … so wooden as to ignore" new "techniques of this electronic age," *Cal. Bankers*, 416 U.S. at 95 (Marshall, J., dissenting), would "embarrass the future," *N.W. Airlines, Inc.* v. *Minnesota*, 322 U.S. 292, 300

(1944)). In *United States* v. *Jones*, for example, the Court distinguished between the "practical" protections of "the precomputer age," and the necessary "constitutional" and "statutory" protections of our digital age—an age for which the third-party doctrine appears "ill-suited." 565 U.S. 400, 417 (2012). As *Riley* predicted, the "gulf between physical practicability and digital capacity" has "continue[d] to widen." 573 U.S. at 394. And *Carpenter* rejected arguments that "fail[ed] to contend with the seismic shifts in digital technology." 585 U.S. at 313.

Today's technology mixed with today's third-party doctrine produces a hazardous cocktail. It exposes citizens to the very real "danger of dragnet-style government mass surveillance." Alex Brown, *Derivative-Consent Doctrine and Open Windows: A New Method to Consider the Fourth Amendment Implications of Mass Surveillance Technology*, 66 CASE W. RES. L. REV. 261, 279 (2015); accord PRINCIPLES OF THE LAW, POLICING § 2.05 (AM. LAW. INST., Tentative Draft No. 3, 2021). In the past, practical impossibilities might've prevented dragnet sweeps at the scale seen here. The burden of conducting one would at least provide a substantial disincentive. No more.

Three socio-technological "advance[ments]" in have increased the danger of abusive dragnets through use of the third-party doctrine, V. Alexander Monteith, *Cell Site Location Information: A Catalyst for Change in Fourth Amendment Jurisprudence*, 27 KAN. J.L. & PUB. POL'Y 82, 102 (2017): pervasive data collection (especially through the internet of things); cloud-based data storage; and data processing through artificial intelligence and quantum computing.

*Data collection.* "Today we use the Internet to do most everything," meaning "[c]ountless Internet companies"

collect our data. *Carpenter*, 585 U.S. at 387 (Gorsuch, J., dissenting). Increasingly, Americans are surrounded by a legion of "helpful" devices: smartphones and their myriad applications, smart watches, smart appliances, smart home fixtures, Alexas, air pods, fitbits, in-car information systems, and on and on. And we deploy this artificial intelligence-driven internet-of-things technology to do everything from exercise to keep our schedule to "us[e] a digitally stored credit card at a store or online." Gelb, *supra*, at 31 (saying in 2020 every second each American generated 1.7 megabytes—or 1,000 text pages—of electronically stores information). Largely "unbeknownst to the user," *id.*, these devices collect "a great deal of information about" users and transmit it "to third parties in the course of carrying out mundane tasks. *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring).

So the data piles up. Even ten years ago, "more data [had] been created in the [previous] two years than in the entire previous history of the human race." Bernard Marr, *Big Data: 20 Mind-Boggling Facts Everyone Must Read*, FORBES (Sept. 30, 2015), https://tinyurl.com/36j7nx6w. And the pace of collection has only been quickening post-pandemic.

*Data storage.* Companies have, of course, maintained "detailed records of individuals' personal information" for decades. Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343, 357 (2008). But as *Riley* recognized, we "now live in the world of the cloud." David A. Harris, Riley *v.* California *and the Beginning of the End for the Third-Party Search Doctrine*, 18 U. PA. J. CONST. L. 895, 898-99 (2016). That allows the storage of formerly unthinkable quantities of data that "is, by its very nature, conveyed to and possessed by third parties." *Id.* Today, people don't keep papers and effects at home

but online; they go to hospitals and doctors' offices rather than receiving home visits; and they use "bank-intermediated transactions" rather than pay directly—all of which generates functionally permanent records in the cloud. LaFave, *supra*, § 2.7(c). Bank records, for example, are now being "stored for longer" and in greater numbers "than ever before." Winters, *supra*, at 1384. Especially as data has become a valuable commodity (and storage has become cheap), companies have every incentive to retain as much data as possible for as long as possible. And they do.

*Data processing.* Even in the 1970s, States were warning that the analytical power of new technology like "computers" had "accelerated" surveillance capabilities, and privacy jurisprudence "must keep pace." *Burrows*, 529 P.2d at 593. And "the advent of high-speed computers" made it "[]conceivable" to conduct dragnet searches with "unimaginable" "potential for invasions of privacy." *Clapper*, 785 F.3d at 824. Today we have "Quantum AI"—which combines the "principles of quantum mechanics," like "superposition," with "the pattern recognition and learning capabilities of artificial intelligence." Bernard Marr, *The Next Breakthrough In Artificial Intelligence: How Quantum AI Will Reshape Our World*, FORBES (Oct. 8, 2024), https://perma.cc/4UJG-KHLM. This "fusion" creates "the ability to analyze vast amounts of data, recognize complex patterns, and make predictions with a level of accuracy and speed that was previously thought impossible." *Id.*

Given these shifts, a tech-blind third-party doctrine like the one the First Circuit used below erases any "meaningful" Fourth Amendment protection. Henderson, *supra*, at 412. Just consider a few categories of

information not yet discussed that governments already have or could acquire under the third-party doctrine:

- Ad network profile databases, Elspeth A. Brotherton, *Big Brother Gets A Makeover: Behavioral Targeting and the Third-Party Doctrine*, 61 EMORY L.J. 555, 571 (2012);
- Dating-app and smart-home-device data, Tokson, *supra*, at 1849;
- "[M]etadata," "internet search history," and "hotel guest registries," Adam Lamparello, City of Los Angeles *v.* Patel*: The Upcoming Supreme Court Case No One Is Talking About*, 20 TEX. J. C.L. & C.R. 135, 138 (2015);
- All "commercial data," Carrie Leonetti, *A Grand Compromise for the Fourth Amendment*, 12 J. BUS. & TECH. L. 1, 10 (2016);
- "[A]pp permissions" data, Michael Gentithes, *App Permissions and the Third-Party Doctrine*, 59 WASHBURN L.J. 35, 42 (2020);
- DNA tests, Catherine Arcabascio, *A Genetic Surveillance State: Are We One Buccal Swab Away from A Total Loss of Genetic Privacy?*, 63 HOW. L.J. 117, 152 (2020); and
- Functionally every form of health data, Rhea Bhatia, *A Loophole in the Fourth Amendment: The Government's Unregulated Purchase of Intimate Health Data*, 98 WASH. L. REV. ONLINE 67, 100 (2024).

Too often, these and other examples of law enforcement "data mining" become a pure "fishing expedition" in which the government casts "a giant net to see what" (or who) they can catch. Solove, *supra*, at 357.

The frequent "positioning of [a] data company as a sort of information processing plant makes it a very attractive source of information for government investigators." Ishan Kumar, *The Fourth Party Doctrine: Regulating Big Data with an Inference-Based Approach*, 105 CORNELL L. REV. ONLINE 94, 108 (2020). And as in *Carpenter*, these "newfound" searching "capacit[ies] run[] against everyone" at once. 585 U.S. at 312. The government "need not even know in advance whether" it wants to investigate "a particular individual." *Id.* So these are variations on the Founding Era's much-hated general warrants. Solove, *supra*, at 357. They're a "sweeping nullification" of the Constitution's promises. Connell, *supra*, at 209.

When governments can freely "circumvent" the Fourth Amendment "and legally conduct … millions of general fishing expeditions," Brotherton, *supra*, at 571, ranging across every conceivable data category, it's difficult to see how the Fourth Amendment stays "[]relevant," Jane R. Bambauer, *Filtered Dragnets and the Anti-Authoritarian Fourth Amendment*, 97 S. CAL. L. REV. 571, 608 (2024); cf. *In re Under Seal*, 749 F.3d 276, 280 (4th Cir. 2014) (affirming government's seizure of encryption keys that exposed "400,000-plus email users").

What's worse, these dragnet searches implicate other constitutional protections. Today, it's "impracticable" to "exchange ideas or information without revealing information to third parties." Deepali Lal, *Criminal Procedure-Technology in the Modern Era*, 43 U. ARK. LITTLE ROCK L. REV. 519, 540 (2021). So the third-party doctrine allows people to be targeted for exercising First Amendment freedoms. Solove, *supra*, at 357-58; Brotherton, *supra*, at 589-90. Recognizing as much, potential targets might "self-censor[] [their] speech and

sometimes forgo[] electronic communications in response to [dragnet] surveillance." *Wikimedia Found.* v. *Nat'l Sec. Agency*, 857 F.3d 193, 211 (4th Cir. 2017). Here, that chilling effect isn't limited to the 14,355 Coinbase users alone. Once the IRS gets "the identity of some wallet owners," it could "use these known nodes in the system to build a 'transaction graph' that tracks each particular" sale, exposing "the identity of owners of unknown wallets with which the known wallets transacted." Omri Marian, *A Conceptual Framework for the Regulation of Cryptocurrencies*, 82 U. CHI. L. REV. DIALOGUE 53, 57 (2015). This six-degrees-of-separation spillover effect is just one of many unintended and constitutionally problematic consequences flowing from digital-age dragnet searches.

**B.** But a partial solution is ripe for the taking: limit *Miller*'s third-party doctrine to suspect-specific searches. No dragnets, no fishing expeditions, no forcing 14,355 citizens to undergo a random digital-financial-records strip search. If law enforcement personnel continue to wield *Miller*'s nigh-boundless investigative power, that power should be limited to identified suspects. Even the third-party doctrine's strongest present advocate, Professor Orin Kerr, agrees that something like this could be a reasonable limitation. See Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 309 (2005).

While such a limitation would depart from *Miller*'s absolutist holding, it would square with *Miller*'s facts, which are nothing like digital dragnets. After all, a crime-less, unparticularized search of a year's worth of comprehensive financial activity for 14,355 people "bears little resemblance to" the crime-specific, single-person search of a few months' worth of some checks and

statements "considered in" *Miller*. *Riley*, 573 U.S. at 386; accord Nathan F. Wessler & Max Behrman, *Challeging the Warrantless Bulk Surveillance of Money Transfer Records*, 47 CHAMPION 42, 45 (May 2023). As *Riley* put it, searching someone's pockets is qualitatively different from "ransacking his house." 573 U.S. at 396. Suspecting someone "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. But this case is even worse than *Riley*'s hypothetical because the IRS doesn't suspect any digital "tucking"; it ran its invasive dragnet search with *zero* identified suspicions. Because these facts are "materially distinguishable from" *Miller* and its progeny, they do not justify "the dragnet communications surveillance now at issue." Strossen, *supra*, at 1150; see also Wessler, *supra*, at 45 (saying there is no justification to "extend[]" the third-party "to the sort of bulk [financial-records] surveillance occurring here").

Finally, forbidding *Miller* dragnet searches would be consistent with the principle that searches must "be as limited as possible." *Coolidge* v. *New Hampshire*, 403 U.S. 443, 467 (1971). A "general, exploratory rummaging in a person's belongings" resurrects the "the specific evil" so "abhorred by the colonists"—the general warrant. *Id.* States detest "general exploratory searches," too. *State* v. *Olsen*, 399 P.3d 1141, 1149-50 (2017) (calling them unconstitutional "fishing expedition[s]"); *State* v. *Clampitt*, 364 S.W.3d 605, 613 (Mo. Ct. App. 2012) (forbidding government "fishing expeditions" into one suspect's text messages); accord *State* v. *Baker*, 903 N.W.2d 469, 479 (Neb. 2017); *State* v. *Biery*, 314 P.3d 900 (Kan. Ct. App. 2013). And while dragnet searches are about as close to general warrants as possible in 2025, general warrants and writs of assistance are "puny instruments" compared to the power of a digital dragnet

search. Brotherton, *supra*, at 599. Under a properly balanced Fourth Amendment jurisprudence, "law enforcement" would not be allowed "to rummage through troves of location data from" thousands of people "without any description of the particular suspect or suspects to be found." *Smith*, 110 F.4th at 837-38; accord Bambauer, *supra*, at 233.

***

The exact "scope of the third-party doctrine in the digital age"—and how far the Court will let it drift towards "limitless" surveillance—has been an "issue lurking underneath the surface." Lamparello, *supra*, at 139. This Court said 40 years ago that there would "be time enough" to address "dragnet type law enforcement practices" whenever they "eventually occur[ed]." *United States* v. *Knotts*, 460 U.S. 276, 284 (1983). That time is now.

The First Circuit's absolutist third-party doctrine would allow "[m]assive," functionally unlimited government fishing expeditions. William S. Fallon, *Imperfect Protection Against Perfect Enforcement: When Procedure Is Not Enough*, 57 CONN. L. REV. 279, 296 (2024). The Court should grant the petition to clarify that *Miller* does not authorize IRS-style, 14,355-person dragnet searches.

## CONCLUSION

The Court should grant the petition.

Respectfully submitted.

JOHN B. MCCUSKEY
*Attorney General*

OFFICE OF THE
WEST VIRGINIA
ATTORNEY GENERAL
State Capitol Complex
Building 1, Room E-26
Charleston, WV 25305
mwilliams@wvago.gov
(304) 558-2021

MICHAEL R. WILLIAMS
*Solicitor General*
*Counsel of Record*

FRANKIE DAME
*Assistant Solicitor General*

*Counsel for* Amicus Curiae *State of West Virginia*

**ADDITIONAL COUNSEL**

KRIS KOBACH
Attorney General
State of Kansas

MICHAEL T. HILGERS
Attorney General
State of Nebraska

DREW WRIGLEY
Attorney General
State of North Dakota

DAVE YOST
Attorney General
State of Ohio