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

BRIEF OF X CORP. AS AMICUS CURIAE IN SUPPORT OF PETITIONER

AMY PEIKOFF
Pacific Legal Foundation
555 Capitol Mall,
Suite 1290
Sacramento, CA 95814
(916) 419-7111
apeikoff@pacificlegal.org

MARK MILLER
Counsel of Record
Pacific Legal Foundation
4440 PGA Blvd.,
Suite 307
Palm Beach Gardens, FL 33410
(561) 691-5000
mmiller@pacificlegal.org

Counsel for Amicus Curiae X Corp.

QUESTION PRESENTED

The Internal Revenue Service used a subpoena to obtain without a warrant from a cryptocurrency exchange three years of transaction records concerning over 14,000 of the exchange's customers, including Petitioner James Harper's records. Mr. Harper's contract with the exchange made clear that the records belonged to him and that the exchange would protect his privacy. The transaction records at issue opened an especially intimate window into Harper's life because they not only revealed his historical cryptocurrency transactions but also enabled tracking of his transactions into the future. The court below relied upon the third-party doctrine to hold that IRS's warrantless search and seizure of Harper's financial records did not violate the Fourth Amendment.

The question presented is:

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

U.S. Constitution

Rules

Other Authorities

IDENTITY AND INTEREST OF AMICUS CURIAE[1]

"Awareness that the government may be watching chills associational and expressive freedoms." *United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring). X Corp., an American technology company headquartered in Bastrop, Texas, strives to protect the associational and expressive freedoms of users of its real-time information-sharing app and associated services. X understands that this means also ensuring its users' Fourth Amendment rights are respected regarding the data X collects and processes.

While providing services to users, X collects, processes, and stores multiple classes of sensitive user data which could be the subject of broad, suspicionless subpoenas by law enforcement or other government agencies, including financial data.[2] X believes contractual promises, like those it makes to its users in its Terms of Service, should be recognized as relevant to the protection their data receives under the Fourth Amendment.

---

[1] Pursuant to Rule 37.2, Amicus Curiae provided timely notice to all parties. Pursuant to Rule 37.6, Amicus Curiae affirms that no counsel for any party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than Amicus Curiae, their members, or their counsel made a monetary contribution to its preparation or submission.

[2] Currently, X collects, stores, and processes financial data pursuant to its sales of advertising, as well as its subscription and advertising revenue-sharing features. And there are plans for its affiliates to launch a range of financial services offerings, including peer-to-peer payments. *See, e.g.*, Kate Conger, *Elon Musk's X Partners With Visa to Provide Financial Services*, NY Times (Jan. 28, 2025), https://tinyurl.com/yrk4y9bx.

INTRODUCTION AND SUMMARY OF ARGUMENT

The First Circuit's opinion, which is the subject of the petition before this Court, exemplifies the confusion about the third-party doctrine that exists in the wake of this Court's ruling in *Carpenter v. United States*, 585 U.S. 296 (2018). By granting Petitioner James Harper a writ of certiorari, this Court can clear up the confusion and restore Fourth Amendment protections for individuals guilty of nothing more than participating in an increasingly specialized and technologically advanced economy.

In its review of the district court's dismissal of Harper's suit, the First Circuit affirmed, holding that Harper had no cognizable Fourth Amendment interest in his Coinbase records. It held that the third-party doctrine applied in this case, and therefore the Fourth Amendment was not implicated when: (1) Harper shared sensitive financial information with "third-party" Coinbase; (2) Harper used Coinbase's exchange to deposit and conduct transactions in Bitcoin; and then (3) Coinbase, after first resisting the IRS's dragnet subpoena, eventually shared Harper's information—along with that of 14,354 other Coinbase customers—with the IRS, after a court ordered it to obey a scaled back version of that subpoena. *Harper v. Werfel,* 118 F.4th 100, 107 (1st Cir. 2024) (relying on *Smith* and *Miller* to conclude "the account information obtained by the [IRS] in this case falls squarely within this 'third party doctrine' line of precedent."). Amicus X Corp. agrees with Petitioner Harper that the First Circuit failed to correctly interpret and apply the limitations of the third-party doctrine established in *Carpenter*.

Nevertheless, disagreements about the application of the third-party doctrine post-*Carpenter* do not surprise. As Justice Gorsuch noted in his dissent, the *Carpenter* majority left lower courts "two amorphous balancing tests, a series of weighty and incommensurable principles to consider in them, and a few illustrative examples." *Carpenter,* 585 U.S. at 397 (Gorsuch, J., dissenting).

The first test is the infamous *Katz* "reasonable expectation of privacy" test. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The second is new, formulated by a majority evidently reluctant to further extend the third-party doctrine—previously extended in the 1970s cases *Smith v. Maryland*, 442 U.S. 735 (1979) and *United States v. Miller*, 425 U.S. 435 (1976)—to its logical extreme. Narrowing those cases' holdings, the *Carpenter* majority established "a *second Katz*-like balancing inquiry, asking whether the fact of disclosure to a third party outweighs privacy interests in the 'category of information' so disclosed." *Carpenter*, 585 U.S. at 397 (Gorsuch, J., dissenting).

As a result, judges are left asking questions such as:

- How long is the "long term" to which data must correspond before an expectation of privacy in it becomes "reasonable"? *See, e.g.*, *Leaders of a Beautiful Struggle v. Balt. Police Dep't,* 2 F.4th 330, 341 (4th Cir. 2021) (interpreting *Carpenter* to "solidif[y] the line between short-term tracking of public movements—akin to what law enforcement could do '[p]rior to the digital age'—and prolonged tracking that can reveal intimate details through habits and patterns.");

- How "sensitive" must the data be? *See, e.g.*, *United States v. Smith*, 110 F.4th 817, 832 (5th Cir. 2024) (quoting *Carpenter* among other precedents noting that location data provides "an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.' ") (citations omitted);
- How "intrusive" is the invasion? *See, e.g.*, *United States v. Chatrie*, 107 F.4th 319, 331 n.18 (4th Cir. 2024) (rejecting Chatrie's argument that "the accuracy with which [Google] Location History can estimate a user's location" made the invasion intrusive enough to outweigh the fact that information about an "individual trip viewed in isolation" does not "reveal intimate details through habits and patterns."). *Cf.*, *Smith*, 110 F.4th at 833 ("While it is true that geofences tend to be limited temporally, the potential intrusiveness of even a snapshot of precise location data should not be understated.") (citations and quotations omitted);
- How "voluntary" must the sharing be to outweigh other "reasonableness" factors? *Chatrie*, 107 F.4th at 319 (finding, after noting that Google's Location History sharing feature was turned off by default, could be reset to that default at any time, and that ample notice of the effect of turning on this feature was given, that "unlike with CSLI [at issue in *Carpenter*], a user knowingly and voluntarily exposes his Location History data to Google."). *Cf. Smith*, 110 F.4th at 835 ("As anyone with a smartphone can attest, electronic opt-in processes are

hardly informed and, in many instances, may not even be voluntary. . . . [In] Google's Location History opt-in process . . . users are bombarded multiple times with requests to opt-in across multiple apps. . . . Even Google's own employees have indicated that deactivating Location History data based on Google's 'limited and partially hidden warnings' is 'difficult enough that people won't figure it out.'") (citations omitted); and

- Should courts focus on "capabilities" of the relevant technology, or look only at "results," the data shared in a given case? *See id.* at 834 n.8 (disagreeing with the Fourth Circuit's interpretation of *Carpenter* in *Chatrie*, that standing to challenge geofencing on Fourth Amendment grounds depends on one "contend[ing] that the warrant revealed his own movements within his own constitutionally protected space," i.e., the results achieved, and noting that, by contrast, the *Carpenter* majority "analyzed the *general capabilities* of CSLI, and asked whether the *ability* for CSLI 'to chronicle a person's past movements through the record of his cell phone signals' created an expectation of privacy") (citation omitted).

And so on. This miasma is, as Gorsuch noted, "where *Katz* inevitably leads." *Carpenter,* 585 U.S. at 397 (Gorsuch, J., dissenting).

Besides causing judicial headaches, the third-party doctrine enables government to gather broad swaths of information without first obtaining a warrant based on probable cause and particularized suspicion. This undermines property rights and privacy—necessary

for enjoyment of associational and expressive freedoms—and contradicts the Founders' understanding of our Fourth Amendment protections. *See* William J. Cuddihy, The Fourth Amendment: Origins and Original Meanings 602-1791 776 (Oxford Univ. Press 2009) ("[Individualized warrants] preponderated as the orthodox protocol of search and seizure in 1791. . . . [W]arrants enjoyed the overriding mandate of established usage" by 1800.) (citation omitted).

Moreover, it prevents "third parties" like Coinbase and X Corp. from acting according to their own judgment in relation to both government and their users. Coinbase and X Corp. should not be coerced into helping governments undermine their users' privacy and property rights through an end run around the Fourth Amendment.

Amicus X Corp. urges this Court to grant Petitioner Harper's Petition for a Writ of Certiorari. This case presents an opportunity for the Court to clarify this area of constitutional law by tethering its decision to the Fourth Amendment's original meaning: all searches of private property require warrants based on probable cause and particularized suspicion, *Jones*, 565 U.S. at 404-10 (holding a search occurred when government obtained information by means of trespass on a constitutionally protected "effect")[3], and a search occurs when government gains access to "houses, papers [or] effects," U.S. Const. amend. IV, that belong to a person under the law. *Byrd v. United*

[3] The First Circuit declined to find for Petitioner Harper based on this rationale, describing such a theory as "novel," and stating, incorrectly, that Harper had "ma[de] no effort in his opening brief to explain the legal source of the interest he asserts." *Harper*, 118 F.4th at 111.

States, 584 U.S. 395, 403-04 (2018) ("[*Katz*] supplements, rather than displaces, the traditional property-based understanding of the Fourth Amendment.") (internal citation and quotation omitted).

On this view—and even on an alternative originalist view centering on the Amendment's promise that all searches and seizures be "reasonable"[4]—this tethering is achieved by recourse to the common law. *See Lange v. California,* 594 U.S. 295, 310 (2021) (noting the common law may be instructive as to what sort of searches the Founders would consider reasonable, and the Fourth Amendment must be interpreted to "provide *at a minimum* the degree of protection it afforded when it was adopted") (internal citations and quotations omitted).

In particular, this case and others involving searches of financial and other sensitive data held by third parties should be viewed through the lens of the common law of contract as understood by our Founders. This approach will provide a clear, bright-line rationale for limiting the third-party doctrine's scope in a manner both consistent with the *Carpenter* result and appropriate for our technological age.

---

[4] *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 Harv. L. Rev. 757 (1994) (presenting and arguing for a "refurbished" Fourth Amendment, with reference to both the amendment's text and extensive analysis of the common law). *But see Carpenter*, 585 U.S. at 355-58 (Thomas, J., dissenting) (comparing "reasonable" as used in the text of the Fourth Amendment to the term's use and significance in the *Katz* test). "Suffice it to say, the Founders would be confused by this Court's transformation of their common-law protection of property into a 'warrant requirement' and a vague inquiry into 'reasonable expectations of privacy.' " *Id.* at 356-57.

ARGUMENT

I. The Third-Party Doctrine Originated In "Secret Agent Cases," Which the Common Law Would Address under the Doctrine of *Illegal Contract.* This Explains Why There Was No "Reasonable Expectation of Privacy" In Those Cases

The third-party doctrine in its pre-*Carpenter* form says the Fourth Amendment is not implicated when: (1) you share information with a third party—for example, your bank, your phone company, Coinbase, or X Corp.—even for a limited purpose; and (2) the third party then shares the information with the government. Orin S. Kerr, *The Case for the Third-Party Doctrine,* 107 Mich. L. Rev. 561, 563 (2009). It is important, however, to recall the historical underpinnings of the doctrine to understand its appropriate scope. The genesis of the doctrine is a series of mid-twentieth century "secret agent" cases involving criminals or criminal organizations. *Id.* at 567-68 (discussing "secret agent" cases heard by the Supreme Court between 1952 and 1971). Think of Tony Soprano divulging information about his illegal businesses to a "business associate" turned government informant, and a prosecutor using the informant's disclosures to indict and convict Soprano. But then, in the 1970s, in *Smith* and *Miller*, the scope of the doctrine was drastically expanded to apply not only to mafia dons, but also to any ordinary, innocent citizen who shares information with third parties, whether while doing business, or simply enjoying life.

Alarm bells did not ring immediately. Back then we shared exponentially less information with third parties than we do today. *See* Note *If These Walls*

Could Talk: The Smart Home and the Fourth Amendment Limits of the Third-Party Doctrine, 130 Harv. L. Rev. 1924, 1925 (2017) ("Our daily activities increasingly involve turning over information to third parties in order to undertake basic transactions, such as online banking, email, internet browsing, and cell phone use."). But the digital age brought about a new set of pernicious consequences the Court could never have anticipated. In 2013 the world learned, for example, that the National Security Agency had continuously collected phone record metadata of *all* Verizon customers for *several years*. *See* Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, The Guardian (June 6, 2013).[5] Attempts to chisel away at the third-party doctrine followed, but without overturning *Smith* and *Miller* outright.

Carpenter, with its additional balancing test, is a prime example. Yes, it's true that *Carpenter*'s result is consistent with the original meaning and protections of the Fourth Amendment. Further, a court that properly applied *Carpenter*'s complex rubric should reach the conclusion that the IRS violated the rights of Harper and 14,354 of his fellow Coinbase customers in this case. But the law in this area is, to be blunt, a mess. Amicus X Corp. believes this Court should grant Petitioner Harper's writ of certiorari to finish what it started in *Carpenter*. This Court, with the benefit of decades of hindsight on the effects of its post-*Katz* expansion of the third-party doctrine, should clarify the law in this area and at the very least continue to narrow or distinguish *Smith* and *Miller*,

[5] https://tinyurl.com/3rehu775.

as both failed to justify the third-party doctrine in its pre-*Carpenter* form.[6]

---

[6] The only justification offered by this Court in *Miller* for extending the doctrine beyond the context of the secret agent cases was that Congress had "assumed" the "lack of any legitimate expectation of privacy concerning the information kept in bank records" in enacting the Bank Secrecy Act, which had "a high degree of usefulness in criminal, tax, and regulatory investigations and proceedings.'" *Miller*, 425 U.S. at 442-43 (citations omitted). Later this Court, in *Smith*, merely applied the *Katz*-mediated extension of the doctrine from *Miller*, without any reference to the questionable rationale provided by the *Miller* Court. This facilitated the *Smith* Court's evasion of the question-begging implications of this "justification," pointed out not only by the dissenting Justices, but also in this Court's own majority opinion:

> Situations can be imagined, of course, in which *Katz'* two-pronged inquiry would provide an inadequate index of Fourth Amendment protection. For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects. . . . In determining whether a "legitimate expectation of privacy" existed in such cases, a normative inquiry would be proper.

Smith, 442 U.S. at 740 n.5.

The mere existence of a statute, even one that is useful in "criminal, tax, and regulatory investigations," *Miller*, 425 U.S. at 442-43 (citations omitted), is not, without persuasive normative argument, enough to vitiate one's "legitimate expectation of privacy"—not to mention a property interest protected by the Fourth Amendment. Especially considering the normative arguments *against* the third-party doctrine that have been raised since the 1970s, including those presented by the instant case, reconsideration of this Court's rulings in *Smith* and *Miller* is appropriate.

Justification is due because, although few would expect to retain a legitimate expectation of privacy when they entrust information to confederates in *criminal* activity, the same cannot be said of ordinary individuals sharing information with service providers in their daily lives. The distinction lies in the common-law doctrine of *illegal contract*, which deems unenforceable any agreement made intentionally to achieve an illegal end. *See* 5 Samuel Williston & Richard A. Lord, A Treatise on the Law of Contracts § 12:1 (4th ed. 2009).

If Tony Soprano makes an "arrangement" with a "business associate," any collateral promises are unenforceable, including promises to keep it a secret. But terms of service agreements between users and Coinbase or X Corp. would not be deemed illegal contracts, merely because some users happened to have also committed crimes or are otherwise properly subject to government investigation. *See generally* Amy L. Peikoff, *Of Third-Party Bathwater: How to Throw Out the Third-Party Doctrine While Preserving Government's Ability to Use Secret Agents*, 88 St. John's L. Rev. 349 (2014). A fortiori, that one user breaks the law does not entitle the government to trample on the rights of other, law-abiding users ensnared by constitutionally insufficient, dragnet subpoenas or similarly unreasonable searches. Accordingly, promises made to users by these companies are enforceable under common law, just as (to use another common law analogy) records entrusted to a bailee still belong to the

bailor. *Carpenter*, 585 U.S. at 399 (Gorsuch, J., dissenting).[7] Both users and bailors retain privacy and property interests entitled to Fourth Amendment protection. Nothing less is "reasonable."[8]

II. The Common Law Of Contract Traditionally Protected Privacy, And So Is A Proper Lens Through Which To Analyze The Third-Party Doctrine

"The Right to Privacy," Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890), written by future Supreme Court justice Louis Brandeis and partner Samuel Warren, has been credited with giving rise to a distinct "right of privacy." *See* John W. Wade et al., Prosser, Wade and Schwartz's Cases and Materials on Torts 947 (The Foundation Press 1994). Their core thesis was that this right of privacy was necessary to prevent or redress the publication, without the subject's permission, of private facts, surreptitiously taken photographs, and the like. Brandeis & Warren, *supra,* at 195-96. Notably, the authors did not argue that the

---

[7] Although Justice Gorsuch wrote in dissent in *Carpenter*, he did so on the narrow ground that Carpenter did not invoke contract- or property-based arguments under the Fourth Amendment. To the extent Justice Gorsuch noted that such arguments could potentially provide alternative bases for a Fourth Amendment violation, the *Carpenter* majority did not reach the issue.

[8] *See generally* Peikoff, *Third-Party, supra. See also* Christina Del Rosso & Carol M. Bast, *Protecting Online Privacy in the Digital Age:* Carpenter v. United States *and the Fourth Amendment's Third-Party Doctrine*, 28 Cath. U. J. L. & Tech. 89, 95-96 (2020) ("[T]he third-party doctrine enables the . . . government to engage in surveillance and monitoring of one's daily life, similar to the general warrant that the Fourth Amendment ultimately intended to prevent.") (citation omitted).

common law left privacy without protection. Rather, they argued, the laws protecting rights to property and contract, or defending against breaches of trust or confidence, did not *adequately* protect privacy when new technologies made possible invasions of another's privacy, without committing physical trespass, without privity of contract, and without any relationship of trust or confidence. *Id.* at 213.

Once courts began recognizing this "right to privacy," however, traditional legal protections for privacy seemed to be gradually eroded or forgotten. This is unfortunate because, unlike common-law rights to property or contract, or against breaches of trust or confidence, this "right to privacy" came packaged with an "amorphous balancing test," *see Carpenter*, 585 U.S. at 397 (Gorsuch, J., dissenting) (Gorsuch using this language), from its very inception. In their article, Brandeis and Warren envisioned this new "right" as one subject to "limitations" to be determined by balancing "the dignity and convenience of the individual" against "the demands of the public welfare or of private justice." Brandeis & Warren, *supra*, at 214. Not surprisingly, by the late 1960s, an individual's enjoyment of privacy vis-à-vis government was determined in *Katz* to depend on a judge's pitting the actual privacy expectations of an individual against various and sundry demands of society, to decide whether one had a "reasonable expectation of privacy." *Katz*, 389 U.S. at 361 (1967) (Harlan, J., concurring).

Decades later Justice Antonin Scalia helped reverse this trend, explaining in *United States v. Jones*, 565 U.S. 400 (2012), that the *Katz* privacy test was "*added to,* not *substituted for*, the common-law trespassory test." *Id.* at 409. We unfortunately cannot know how he would have ruled in *Carpenter*. And

while some Justices searched in *Carpenter* for an interest to justify finding the relevant data was Carpenter's, whether a *contract* might be sufficient did not arise on the facts of that case. Even so, each of the dissenting Justices who believed Carpenter presented no winning Fourth Amendment argument further inquired into whether he possessed a property interest in the data at issue.

Justice Kennedy found Carpenter did not own, create, or control the records at issue and therefore a subpoena sufficed. *Carpenter*, 585 U.S. at 329-30 (Kennedy, J., dissenting). Justice Thomas said the issue was not " 'whether' a search occurred," but rather "*whose* property was searched." *Id.* at 342 (Thomas, J., dissenting). However, he continued, "[n]either the terms of his contracts nor any provision of law makes the records [Carpenter's]." *Ibid.* Thomas noted Carpenter argued based on statute, not "property, tort or contract law[.]" *Id.* at 354. Justice Alito wrote, "Carpenter indisputably lacks any meaningful property-based connection to the cell-site records. . . ." *Id.* at 384 (Alito, J., dissenting).

Justice Gorsuch found a statutory basis for Carpenter's cell-site records to "qualify as *his* papers or effects under existing law." *Id.* at 405 (Gorsuch, J., dissenting). "Those interests[,]" he continued, "might even rise to the level of a property right." *Id.* at 406. Nonetheless, Gorsuch dissented because Carpenter failed to "invoke the law of property, or any analogies to the common law." *Ibid.*; s*ee also id.* at 399 ("Entrusting your stuff to others is a *bailment* [a type of contract]. . . . A bailee normally owes a legal duty [to the bailor] to keep [your stuff] safe, according to the terms of the contract," express or implied.). Fourth

Amendment rights are not extinguished when entrusting your documents to a third party; rather, "[t]hese ancient principles" protect your interests, even in digital records. *Id.* at 400.

This Court should grant certiorari to determine whether Petitioner Harper's rights under his contract with Coinbase are relevant to the Fourth Amendment protection his Coinbase records deserve consistent with both Justices Thomas's and Gorsuch's opinions in *Carpenter*. Were this Court to address the relevance of the doctrine of illegal contract to understanding the third-party doctrine's origins and proper scope, it could clarify this area of the law for the benefit of lower courts and litigants alike. Moreover, doing so would restore and reinforce the baseline of protection that the Fourth Amendment should and was intended to provide, something that is sorely needed in our increasingly digital world. *Lange,* 594 U.S. at 309. *Cf.* Wayne A. Logan & Jake Linford, *Contracting for Fourth Amendment Privacy Online*, 104 M.N. L. Rev. 101, 108 (2020) ("[I]mporting contract tools of interpretation [into data privacy] holds significant promise for providing a reliable analytic rubric for resolving . . . privacy questions in the Internet Age.").

III. This Approach Makes It Possible to Limit the Third-Party Doctrine's Application Without Resorting To "Balancing . . . Weighty or Incommensurable Principles"

When viewed through the lens of this traditional "contract" approach, the third-party doctrine is arguably superfluous, because an illegal contract cannot create an enforceable expectation of privacy, whether via recognition of a property interest, or otherwise.

See Peikoff, *Third-Party*, *supra*, at 374-76. This approach also calls into question the amorphous, pragmatic *Katz* test. For it is seeing the third-party doctrine in the context of *Katz* which invited this Court, in *Smith* and *Miller*, to set aside the doctrine's origins and dramatically expand its scope, without justification and with detrimental consequences for law-abiding individuals. As Justice Thomas noted in *Carpenter*, "[a]fter 50 years, it is still unclear what question the *Katz* test is even asking. This Court has steadfastly declined to elaborate the relevant considerations or identify any meaningful constraints." *Carpenter*, 585 U.S. at 358 (Thomas, J., dissenting) (quotations and citations omitted). "*Katz* has yielded an often unpredictable—and sometimes unbelievable—jurisprudence." *Id.* at 394 (Gorsuch, J., dissenting) (quotations and citations omitted). But to achieve justice for Petitioner Harper and others who suffer unreasonable searches of their "persons, houses, papers, and effects," and to do so in a way which provides clarity for judges deciding such cases in the future, this Court need only recognize that the common law of contract provides a principled reason, rooted in our legal traditions, to return the third-party doctrine to its original scope.

Standard contracts between users and companies like Coinbase and X Corp. are enforceable under common law. When their terms include a company's promise to protect a user's data and keep it confidential, that promise should not be terminable by government fiat. Such contracts should be recognized as a legitimate means for maintaining one's property and privacy. As Justice Sotomayor wrote regarding one "weighty or incommensurate principle[]" courts must

"balance" post-*Carpenter*, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information *voluntarily* disclosed to third parties." *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) (emphasis added).[9] What should matter for Fourth Amendment purposes is not solely whether information is shared with a third party and the sharing is voluntary, but also how the common law views the context in which the voluntary sharing occurs—including whether, as in the case before this Court, the parties' agreement protects the user's right to the information at issue.

---

[9] Justice Sotomayor's provocative concurrence in *Jones* inspired many to question the wisdom of the third-party doctrine, including her future colleague, Justice Gorsuch, who in his *Carpenter* dissent expressed willingness to either abandon the doctrine altogether, or alternatively limit its scope to that for which this brief argues. *See Carpenter*, 585 U.S. at 387-91 (Gorsuch, J., dissenting) (examining various explanations for the third-party doctrine as expanded by *Smith* and *Miller* and concluding, "[i]n the end, what do *Smith* and *Miller* add up to? A doubtful application of *Katz* that lets the government search almost whatever it wants whenever it wants. The Sixth Circuit had to follow that rule and faithfully did just that, but it's not clear why we should."); *and id.* at 390 (alluding to the sort of scenario present in the secret agent cases of the doctrine's origin, and agreeing that one could be seen as consenting to having one's papers searched by the government if the third party to whom one had granted access to those papers happens to be an undercover government agent).

CONCLUSION

The IRS violated Petitioner Harper's Fourth Amendment rights—along with those of 14,354 other Coinbase users—when it obtained a vast quantity of Coinbase records by means of a dragnet subpoena devoid of individualized suspicion. That the First Circuit failed to reach this conclusion demonstrates how muddled the law in this area is in the wake of *Carpenter*.

This Court should grant Harper a writ of certiorari and then consider whether the third-party doctrine, as expanded in *Smith* and *Miller*, can withstand the scrutiny made possible by decades of hindsight. Doing so would help return the doctrine to its original, proper scope by limiting it to circumstances in which an individual has no contractual or property right to the information in question, consistent with the Fourth Amendment's original publicly understood meaning. This would provide clarity to law enforcement seeking in their investigations data held by third parties—but not at the cost of holding either "the king always wins" or "the king always loses." *Carpenter*, 585 U.S. at 390 (Gorsuch, J., dissenting). It would allow individuals to preserve their property and privacy once again, even while enjoying the conveniences and pursuits of happiness our modern life offers. Finally, it would help re-establish the proper relationship between government and companies like Coinbase and X Corp., who would no longer be extrajudicially coerced into helping the government violate their users' Fourth Amendment rights.

Respectfully submitted,

AMY PEIKOFF
Pacific Legal Foundation
555 Capitol Mall,
Suite 1290
Sacramento, CA 95814
(916) 419-7111
apeikoff@pacificlegal.org

MARK MILLER
Counsel of Record
Pacific Legal Foundation
4440 PGA Blvd.,
Suite 307
Palm Beach Gardens, FL
33410
(561) 691-5000
mmiller@pacificlegal.org

Counsel for Amicus Curiae X Corp.

MARCH 2025