No. 25-112

In the Supreme Court of the United States

OKELLO T. CHATRIE,
Petitioner,
v.
UNITED STATES OF AMERICA,
Respondent.

On Writ Of Certiorari
To The United States Court Of Appeals
For The Fourth Circuit

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

AMY PEIKOFF
Pacific Legal Foundation
3100 Clarendon Blvd.,
Suite 1000
Arlington, VA 22201
(202) 888-6881
apeikoff@pacificlegal.org

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

Counsel for Amicus Curiae X Corp.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Regulation

Rule

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, strongly agrees, and 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 necessarily collects, processes, and stores multiple classes of sensitive user data pertaining to millions of innocent individuals, which could be the subject of "reverse searches" by law enforcement or other government agencies, including location information.[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 37.6, 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] X may infer the location of its users using multiple signals, including the user-specified location, the user's IP address, and—for the subset of users who consent—device-provided location data like that at issue in this case. X routinely resists overbroad or otherwise invalid government demands for user data, including through litigation.

INTRODUCTION AND SUMMARY OF ARGUMENT

No one realized it then, but this Court's rulings in the 1970s third-party doctrine cases, *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), ushered in a privacy-prohibition era for the twenty-first century. Henceforth, any attempt to selectively share information with one's service provider would be treated, for Fourth Amendment purposes, as if one had shouted the information through a megaphone, perched upon the highest mountaintop, on worldwide livestream.

To this day, *Miller* and *Smith* remain essentially untouched, in part because legal scholars have argued in justification of the idea that an individual who shares information with a third party, even for a limited purpose, no longer has a "reasonable expectation of privacy" in that information. *See, e.g.*, Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561 (2009) ("Kerr 2009"); H. Brian Holland, *A Third-Party Doctrine for Digital Metadata*, 41 Cardozo L. Rev. 1549 (2020); Orin Kerr, *The Digital Fourth Amendment: Privacy and Policing in Our Online World* 133-62 (Oxford Univ. Press 2025) ("Kerr 2025"); *see also* Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third-Party Doctrine*, 100 Minn. L. Rev. 987 (2016) (arguing for retaining the third-party doctrine as an exception to the Fourth Amendment's warrant requirement). And lower courts have at times leaned on those justifications for support. For example, Judge Wilkinson, concurring with the en banc Fourth Circuit, relied upon some of these normative arguments in concluding, "this case involved a straightforward application of [*Miller* and *Smith*]."

United States v. Chatrie, 136 F.4th 100, 109 (4th Cir. 2025) (Wilkinson, J., concurring) (citations omitted). The normative arguments given in support of the doctrine are not persuasive, however. There is a better way.

X Corp.'s suggestion is straightforward. Using the common law of contract as a lens to analyze the "secret agent" cases in which the third-party doctrine arose, one can see that this Court overextended in *Miller* and *Smith* a doctrine originating in the context of *illegal contract* to the context of *ordinary business contracts* between law-abiding citizens and their service providers. *See* Br. of X Corp. as Amicus Curiae in Supp. of Pet'r at 8-11. Terms of service that promise to protect the privacy of information shared by users with their service providers should be treated as the functional equivalent of "no trespassing" signs on a possession perhaps more valuable than real property—our personal information ("papers" or "effects"). When privacy-protective terms of service are in place, terms that recognize users' rights in the information shared, collected, or stored, government should typically get a warrant based on probable cause before gaining access to that information, including by means of "reverse searches" such as the geofence warrant at issue here.

The adoption of this rule would require, at the very least, that this Court continue to narrow or distinguish *Miller* and *Smith*. This is the right thing to do. With politicians and government agencies continuously devising new ways to collect, store, aggregate,

and search individuals' selectively shared private information,[3] the time for this Court to affirm Fourth Amendment protections is at hand.

ARGUMENT

I. *Miller* and *Smith* Dramatically Expanded the Scope of the Third-Party Doctrine Without Justification

The common law of contract is the key to understanding the third-party doctrine. This is so for two reasons. First, given that the Fourth Amendment arose from concerns about government violating individuals' common-law rights, analysis of Fourth Amendment cases in terms of the common-law rights and interests at stake is the best way to understand the implications of the Amendment's original meaning. Br. of X Corp. as Amicus Curiae in Supp. of Pet'r at 6 (citations omitted). Second, before there was ever a proposal to recognize a distinct "right to privacy," the common law provided legal protection for privacy via "laws protecting rights to property and contract, or defending against breaches of trust or confidence[.]"

---

[3] *See, e.g.*, Joseph Cox, *Inside ICE's Tool to Monitor Phones in Entire Neighborhoods*, 404 Media (Jan. 8, 2026, at 9:00 AM), https://tinyurl.com/bum4h764; Autumn Billings, *Mass Surveillance Is Powering a New Era of Pretextual Traffic Stops*, Reason (Nov. 24, 2025, at 12:37 PM), https://tinyurl.com/bde8h97h; Exec. Order No.14243, 90 Fed. Reg. 13681 (Mar. 20, 2025); Sheera Frenkel & Aaron Krolik, *Trump Taps Palantir to Compile Data on Americans*, The New York Times (May 30, 2025), https://tinyurl.com/5ydt98za; David Kopel, *Turning Credit Cards into Comprehensive Financial Surveillance*, Reason: Volokh Conspiracy (July 14, 2025, at 2:46 PM), https://tinyurl.com/38zfynan; J.D. Tuccille, *The ATF Created a Backdoor Gun Registry. Lawmakers Want an Explanation*, Reason (Feb. 13, 2026, at 7:00 AM), https://tinyurl.com/3dw852ud.

Id. at 12 (citing Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 Harv. L. Rev. 193, 213 (1890)).

In its petition-stage brief, amicus X Corp. argued that this Court, in *Miller* and *Smith*, erroneously expanded the third-party doctrine without justification by unmooring the Fourth Amendment from the common law of contract. *Miller* and *Smith* should at least be narrowed or distinguished, and the third-party doctrine should be returned to its original and proper scope set forth in the "secret agent" cases. Specifically, if a party shares information with a third party subject to an *illegal* agreement to keep the information confidential, then the contract should be no bar to a government search of that information. But if a party shares information with a third party subject to a *legal* confidentiality agreement, that arrangement should preserve Fourth Amendment protections. In other words:

> 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 Google 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.

Br. of X Corp. as Amicus Curiae in Supp. of Pet'r at 11 (citing *Hanover Nat'l Bank of City of New York v. First Nat'l Bank of Burlingame*, 109 F. 421, 425 (8th Cir. 1901) ("The mere fact that a contract the consideration and performance of which are lawful incidentally

assists one in evading a law is no bar to its enforcement.")).

That the common law of contract supplies the key to understanding the third-party doctrine should come as no surprise. Legally enforceable[4] promises made to users by third-party service providers to, e.g., safeguard user data and disclose it in only limited, enumerated circumstances as part of their terms of service, should be recognized as giving rise to privacy and property interests entitled to Fourth Amendment protection. *Ibid.* (citing *Carpenter v. United States*, 585 U.S. 296, 399 (2018) (Gorsuch, J., dissenting) (discussing analogy of common-law bailment); Pet'r's Opening Br. at 15-16 (demonstrating how, per Google's terms of service, "Location History has the key attributes of 'property' as traditionally understood: the right to use, enjoy, dispose, and exclude."); *Id.* at 16-17 (collecting cases in which courts have imposed civil liability for commission of "traditional property torts" involving unauthorized access to data held by third-party service providers).

As X Corp. noted in its petition-stage brief, the "justification" offered for the doctrine in *Miller* was an assumption Congress made in enacting the Bank Secrecy Act, which had "a high degree of usefulness" to law enforcement. Br. of X Corp. as Amicus Curiae in Supp. of Pet'r at 9 n.6 (citation omitted). *Smith* applied the ruling in *Miller* without further explanation, even hinting at *Miller*'s question-begging "justification" in a footnote which read, in part, "[I]f the Government were suddenly to announce on nationwide

[4] An example of terms of service that would *not* be enforceable would be those of a website that predominantly or exclusively sells illegal drugs.

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." *Smith*, 442 U.S. at 740 n.5. *See also* Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 Berkeley Tech. L.J. 1199, 1207 (2009) ("[T]he reasonable expectations that flow from knowledge of the law cannot explain how that law should be configured in the first place."). The mere existence of a statute that law enforcement has found "useful" does not extinguish a "legitimate expectation of privacy." In our constitutional republic, more is required. *Miller*'s ruling was not properly justified, and *Smith* was wrong to rely upon it. Instead, as the *Smith* footnote concluded, "a normative inquiry is proper." *Smith*, 442 U.S. at 740 n.5. As we'll see, the normative justifications for retaining the doctrine in its current form are not convincing.

II. Attempts to Provide Normative Justifications for the Doctrine Fail

In the proceedings below, Judge Wilkinson relied in his concurrence on normative justifications for the third-party doctrine offered by Professor Orin Kerr. Professor Kerr's arguments have been among the most influential in defending the doctrine, and worth special consideration. In 2009, he presented two grounds of support. First, "[w]ithout the doctrine, criminals could use third-party agents to fully enshroud their criminal enterprises in Fourth Amendment protection." Kerr 2009, *supra*, at 576. The doctrine, he argued, would maintain "technological neu-

trality," preserving "roughly the same degree of privacy protection" whether a criminal commits a crime alone, or with third-party assistance. *Id.* at 577.

Kerr's argument fails, however, to account for the latitude the "secret agent" cases provide to law enforcement. Because an agreement between a criminal and his third-party *agent* to enshroud a crime in secrecy would be an illegal contract not subject to Fourth Amendment protection, *see* 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, 374-76 (2014), there is no need to expand the third-party doctrine to *all* contracts with third parties to adequately address Kerr's concern.

Moreover, Kerr's argument itself raises substantial questions. First, "the technologies left exposed by third-party doctrine are not exclusively deployed for illicit purposes," and so the doctrine "dissuad[es] innocent, desirable conduct[.]" Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 Berkeley Tech. L.J. 1239, 1241 (2009); *see also* Epstein, *supra*, at 1226 (explaining the doctrine "creates social inefficiencies with respect to lawful conduct that people naturally wish to keep from the prying eye of the state.").

Second, the mere possibility that lawful confidential arrangements may render crime more difficult to detect without a warrant is not a reason to obliterate the confidentiality of such arrangements. After all, the Constitution "[does] not obliterate privacy protections for the home, for instance," just because the vast majority of many crimes occur there. Murphy, *supra*, at 1244.

Moreover, the use of a third party makes it easier for law enforcement: "Third parties increase the probability that a trail will be left or witnesses will be created, all of which only helps the state in building its case." *Ibid.* By deterring criminals from relying on third parties in the first place, the third-party doctrine's applicability to lawful contractual arrangements may sometimes make it *more* difficult to detect crime, not less. By contrast, if the third-party doctrine were narrowed, although it may be necessary to get a warrant to obtain evidence in the possession of a third party, "that is not a particularly high standard to meet." *Ibid.* Finally, a grand jury subpoena *duces tecum* could continue to be supported by something less than probable cause. *Ibid.*; *see United States v. Dionisio*, 410 U.S. 1, 11-12 (1973) ("The Fourth Amendment provides protection against a grand jury subpoena duces tecum too sweeping in its terms 'to be regarded as reasonable.'" (quoting *Hale v. Henkel*, 201 U.S. 43, 76 (1906))); *Carpenter*, 585 U.S. at 362 (Alito, J., dissenting) (suggesting "upheaval" will result if "every grand jury subpoena *duces tecum* [must] be supported by probable cause"). In short, the notion that the Fourth Amendment must be dispensed with in the context of third-party contracts to allow law enforcement to do their job is difficult to credit.

To commit a crime means, concretely, to initiate force or use fraud against another person or another's property. No matter how one does this, some trail of evidence will exist. Yes, without as broad a third-party doctrine, a warrant may be required to learn, for example, the identity of the person whose IP address is linked to an online theft from a bank account. However, given the occurrence of a theft, and knowledge of which IP address was involved, that warrant should

not be difficult to get. Moreover, as amicus X Corp. has argued, even without the third-party doctrine, government can use undercover agents to investigate criminal activity without violating the Fourth Amendment. *See* Br. of X Corp. as Amicus Curiae in Supp. of Pet'r at 15 (citing Peikoff, *supra*, at 374-76).

Kerr's second defense of the doctrine was based on the need for ex ante clarity, given the high stakes of the exclusionary rule's evidence-suppression remedy. Kerr 2009, *supra*, at 582. *See also* Issacharoff & Wirshba, *supra*, at 987 ("The third party doctrine has the virtue of simplicity and administrability."). Justice Gorsuch has, like Kerr, expressed a desire for a solution that provides ex ante clarity in the application of the Fourth Amendment, but not one that makes it so "the king always wins" or the "king always loses." *Carpenter*, 585 U.S. at 390 (Gorsuch, J., dissenting).

What amicus X Corp. suggests offers exactly the solution Justice Gorsuch desires: whenever legally enforceable terms of service that provide for the confidentiality of user information are in place, those terms should be respected and a warrant based on probable cause should usually be obtained before government gains access to the information held by the service provider. X Corp. is not suggesting that terms of service must (or would) *always* include such privacy-protective terms. Nor is X Corp. suggesting that courts impute such terms when they are absent—particularly when the terms of service state, for example, that a provider may share a user's information with law enforcement, which is often the case. In the absence of privacy-protective terms, no warrant would be required for government to obtain the information from the service provider. Such a rule would both be easy

to apply and accord with users' actual expectations of privacy, because users' expectations would reflect the privacy arrangements to which they actually agreed.

In sum, normative arguments for the third-party doctrine—whether based on "technological neutrality" or ex ante clarity—are not persuasive.

III. Recasting the Third-Party Doctrine as "Consent" or "Disclosure" Only Raises More Questions

The third-party doctrine suffers, not only from a lack of normative justification, but also from a lack of plausibility. It is highly counterintuitive to think that, simply by sharing information with a third-party, even if subject to agreed-upon, stringent privacy protections, we have relinquished a "reasonable expectation of privacy" in it. It is to address this lack of plausibility that Kerr attempted to recast the doctrine in terms of "consent." Kerr 2009, *supra*, at 587. He argued that, in *United States v. White*, 401 U.S. 745 (1971), Justice White "chose the wrong doctrinal prong. Instead of grounding the doctrine in consent principles, he reasoned that use of a secret agent did not violate a reasonable expectation of privacy." Kerr 2009, *supra*, at 589 (footnotes omitted). In other words, even if one's expectation of privacy in the information shared with third parties *is* reasonable, so is a consented-to search, and this, Kerr argued, is what you have in the third-party situation.

Epstein challenged this recasting of the doctrine:

> To be sure, there are many cases where the consent of the party searched meets the standard of individualized consent developed in private law settings. But in

> other cases the nominal consent is presumed on the ground that on balance people are better off from the ex ante perspective if they are forced to submit to some searches against their will.

Epstein, *supra*, at 1206; *see also Carpenter*, 585 U.S. at 390 (Gorsuch, J., dissenting) ("Consenting to give a third party access to private papers that remain my property is not the same thing as consenting to a *search of those papers by the government*."); Murphy, *supra*, at 1241 n.6 (agreeing that the "'consent' model seems to just circle back to the reasonable expectation of privacy test.").

In his 2025 book, Kerr further develops his defense of the third-party doctrine by recasting it in a different way. He no longer grounds the doctrine in consent; instead, he argues it is an instance of the "disclosure rule," which says, in the third-party context, "you have no reasonable expectation of privacy in what you voluntarily disclose to third parties." Kerr 2025, *supra*, at 147. Kerr writes:

> [T]he third-party doctrine is a sensible rule that was accidentally mislabeled. It's really just the traditional idea, going back to the Supreme Court's first major search-and-seizure case in 1878, *Ex parte Jackson*, that concealment is needed to establish Fourth Amendment protection. That makes sense, at least in a lot of cases. When you share information with someone, it becomes their information, too. They can do with it as they please without violating your Fourth Amendment rights. Of course,

> we can debate how far to take this principle. . . . But the foundations of the third-party doctrine have been around in the physical world for about as long as courts have been interpreting the Fourth Amendment.

Ibid. There is a lot to unpack. First, does something qualify as a *principle* when it is unclear how far it should be taken, when it "makes sense" only in "a lot of cases"? Second, given that the Fourth Amendment is a constraint on *government*, does it matter that a private "third party" would not violate your Fourth Amendment rights by doing as he or she pleases with your information? For example, people may also be censored by private third parties such as social media platforms. That does not mean the *government* may constitutionally censor them as well. Similarly here, while sharing information with third parties pursuant to a confidentiality agreement does not preclude the third party from breaching that agreement consistent with the Fourth Amendment, that certainly does not imply the *government* may constitutionally demand access to that information as well.

Leaving aside these flaws in Kerr's reasoning, Kerr's reliance upon *Ex parte Jackson*, 96 U.S. 727 (1877), as the foundation for the third-party doctrine is misplaced. Kerr relies upon *Jackson*, not only as support for the doctrine, but more generally as support for a "content/non-content distinction"—the idea that only the content of communications should be protected by the Fourth Amendment's warrant requirement; "non-content" or "metadata" should not receive such protection. *See* Kerr 2025, *supra*, at 139.

Such a distinction would itself require substantially narrowing the scope of the third-party doctrine in its current form, as one can of course share both content and non-content with third parties. In any event, however, Kerr's argument for the content/non-content distinction starts with the premise that communications conducted remotely, by telephone or computer network, should receive the same protection from government observation as communications via in-person meeting. Just as the government could observe you leaving your home, traveling to another's home, entering to have a conversation, and later returning home, Kerr argues, government should be able to learn, without a warrant, that you sent a communication, something about its length, what time you sent it, to whom you sent it, etc. And similarly for phone calls—who placed the call, to whom, when, for how long, etc. *Id.* at 137-38.

Why should courts provide identical protection in these scenarios? Why shouldn't protection be provided according to an individual's lawful exercise of his or her common-law rights? Kerr does not explain *why* courts should "match protections between the physical world and the networked world." Kerr 2025, *supra*, at 136. He says only, "*If* the goal is to match protections between the physical meeting and the network communication," then the way to do that is to allow "the government [to] collect the network equivalent of what the officer saw in public surveillance in the physical example" without a warrant. *Id.* at 138 (emphasis added). But contractual promises made by today's service providers make it possible for metadata to be private. Why not make those promises relevant to the Fourth Amendment protection metadata receives? In *Jones*, Justice Scalia wrote, "At

bottom, we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *United States v. Jones*, 565 U.S. 400, 406 (2012) (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)) (emphasis added). The degree of privacy against government that existed when the Fourth Amendment was adopted was grounded in the common law, including common law rights of contract. *See Carpenter*, 585 U.S. at 397 (Gorsuch, J., dissenting) ("[T]he traditional approach [to the Fourth Amendment] asked if a house, paper or effect was *yours* under law."); *id.* at 399 (quoting Joseph Story, *Commentaries on the Law of Bailments* § 2, p. 2 (1832)) ("[A] bailment is a delivery of a thing in trust for some special object or purpose, and upon a *contract*, express or implied, to conform to the object or purpose of the trust.") (emphasis added).

Kerr's reliance on *Ex parte Jackson* is misplaced. In *Jackson*, this Court "announced the rules for postal network surveillance." *Id.* at 139. Justice Field distinguished "between different kinds of mail matter,—between what is intended to be kept free from inspection, such as letters, and sealed packages subject to letter postage; and what is open to inspection, such as newspapers, magazines, pamphlets, and other printed matter, purposely left in a condition to be examined." *Jackson*, 96 U.S. at 733. As to the former, "Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, *except as to their outward form and weight*, as if they were retained by the parties forwarding them in their own domiciles." *Ibid.* (emphasis added). Kerr infers that "outward form and weight" includes all postal "metadata," such as names, addresses, and date of

mailing, and chalks up *Jackson* as support for his content/non-content distinction. Kerr 2025, *supra*, at 140.

Suppose it is true that Justice Field meant that all postal metadata was properly subject to warrantless inspection by postal service officials. Even so, Field might not insist that the same content/non-content distinction applied to government postal service inspections must also be applied to private electronic service providers that transport or transmit content subject to confidentiality agreements. It is not at all clear, for example, that a user's expectation of privacy in the "outward form and weight" of an envelope is the same as his or her expectation of privacy in the identity of the recipient of an encrypted Signal message. Caution about applying the same distinction in other contexts is warranted because, as Kerr notes, "*Ex parte Jackson* does not explain why it drew the lines it did." Kerr 2025, *supra*, at 140. *See also* Daniel J. Solove, *Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, 118 Nw. Univ. L. Rev. 1081, 1116-18 (2024) (questioning the value of the content/non-content distinction because metadata can "enable[] highly sensitive inferences" and "be very revealing").

This brings us back to the problem with Kerr relying upon *Jackson* for "the foundations of the third-party doctrine." Kerr 2025, *supra*, at 147. In *Jackson* there is no "third party": the "disclosure" is made by a postal customer *directly to government officials*! *See also Carpenter*, 585 U.S. at 332 (Kennedy, J., dissenting) (citing *Jackson* as limiting, rather than supporting, *Miller* and *Smith*).

Moreover, Kerr must still address the cases in which he admits the doctrine does not "make sense." *Ibid.* Enter "equilibrium adjustment," which Kerr describes as the establishment of new rules "away from the content/metadata line," rules made necessary because "technological change is allowing new and more invasive surveillance on the outside/metadata side of the line." Kerr 2025, *supra*, at 148. It is in terms of equilibrium adjustment that Kerr explains this Court's ruling in *Carpenter*: "New technology [cell sites recording information about cell phones connected to them] had eliminated a reasonable expectation of privacy. The law needed to restore it, adding back the expectation of privacy that technology had taken away." *Id.* at 155. Of course, it is not the technology that had "eliminated a reasonable expectation of privacy"; it is *the third-party doctrine* applied to that technology. The same issue exists here. But this is not the only issue with Kerr's equilibrium adjustment theory.

Before showing how his theory applies to *Carpenter*, Kerr discusses this Court's ruling in *Jones*. He describes the *Jones* majority as "introducing a *new* test: the installation of the GPS device was a search because it was a trespass, regardless of whether its subsequent use infringed on Jones's reasonable expectation of privacy." Kerr 2025, *supra*, at 149 (citing *Jones,* 565 U.S. at 404) (emphasis added). He then relies on language in *Jones* concurrences to characterize the case as an example of "classic equilibrium adjustment." Kerr 2025, *supra*, at 149. However, as Justice Scalia noted, it is the *Katz v. United States*, 389 U.S. 347, 361 (1967), "reasonable expectation of privacy" test that was new—it "has been *added to,* not *substituted for*, the common-law trespassory test."

Jones, 565 U.S. at 409. *Cf. Case v. Montana*, 146 S. Ct. 500, 513 (2026) (Gorsuch, J., concurring) ("For a period, to be sure, the miasma created by this Court's *Katz* era led some to think the scope of the rights guaranteed by the Fourth Amendment depend on nothing more than current judicial instincts about 'reasonable expectations of privacy.' But that confusion cannot last forever, for no one should think the rights of Americans hang on so thin a thread. Instead, and as Justice Story recognized, the Fourth Amendment is made of sturdier stuff, representing 'the affirmance of a great constitutional doctrine of the common law.'") (internal citations omitted).

Kerr describes the "confusion" of lower courts, post-*Carpenter*. "When applying the case to new facts, lower courts often have focused on whether the facts before them resemble those in *Carpenter*." Kerr 2025, *supra*, at 153. True enough, as the fractured reasoning in the en banc Fourth Circuit demonstrates. But Kerr's own theory suffers from the same issue with ex ante clarity. In his discussion of the "privacies of life" prong of his test, Kerr does little more than list examples of the sorts of things that judges have found to be encompassed by this descriptor. *See* Kerr 2025, *supra*, at 158-60. Better to adopt a clear test such as the one X Corp. proposes here.

In a forthcoming article, Kerr applies his model to reverse searches of databases, such as the geofence warrant at issue in the instant case. Orin S. Kerr, *Data Scanning and the Fourth Amendment*, 67 B.C. L. Rev. 431 (2026) (forthcoming) ("Kerr 2026"). However, because his argument starts with the assumption that "data scans do not involve physical intrusion," *id.* at 460, he fails to address arguments like those made in this brief that scanning an account that

a service provider agreed to keep confidential is a Fourth Amendment search, or that "the government, via Google, searched every account" in its Sensorvault at step one, making the geofence warrant a general warrant, Pet'r's Opening Br. at 34. Kerr argues that what's important in determining when a search of a database occurs is when and how much information is "revealed to human observation." Kerr 2026, *supra*, at 443. "For a search to occur, information must be exposed to human observation." *Id.* at 460. But per *Jones*, trespass upon property, including one's "papers" and "effects," is a search, *Jones*, 565 U.S. at 411, and under common law a trespass occurs when a person accesses, without consent, the property of another (or causes an object or instrumentality to gain such access). *See, e.g.*, Restatement (Second) of Torts § 217(e) (1965).

Katz-ian balancing tests were supposed to fill in gaps of privacy protection alleged to have been left by the common law. But in recent decades they have often had the opposite effect and, moreover, have left individuals uncertain about what legal protection their privacy will receive. If Kerr's *Katz*-ian theory is adopted, we will only see more of this.

IV. Coda: What about *Katz*?

Students of legal philosophy may recall Lon Fuller's *The Case of the Speluncean Explorers*, 62 Harv. L. Rev. 616 (1949). It was a set of fictitious legal opinions, written in the year 4300 by Supreme Court Justices of Newgarth, each of whom analyzed the case before the Court using a different theory of jurisprudence. The question presented was whether to uphold convictions for murder of speluncean (cave) explorers

who, after having been stranded for many days without food and, after participating in an (arguably) agreed-upon casting of dice, exercised their "right" to eat their fellow explorers. *Id.* at 616-19. This ghastly and unique set of facts allowed for the opinions to each be a paradigmatic example of a single jurisprudential philosophy. The legal positivist/realist could say "law is law" and chide his colleagues' squeamishness. *Id.* at 631-37. The natural law theorist could declare the situation outside the jurisdiction of his laws and use natural law principles to decide the explorers' fates. *Id.* at 620-26. The pragmatist could appeal to public opinion polls. *Id.* at 637-44. And so on.

The set of opinions written by the en banc Fourth Circuit in this case could be said to resemble The Case of the Speluncean Explorers because, as Judge Gregory observed, "its reasoning is fractured." *Chatrie*, 136 F.4th at 157 (Gregory, J., dissenting). Here, however, the "fractured reasoning" is due, not to any judges disregarding the relevant precedent, but instead because that precedent is so amorphous, so flexible, that a judge's reasoning could be influenced by his or her individual ethical, political, and jurisprudential commitments, and still be within the bounds of what a reasonable, conscientious judge would conclude in this case.

At one extreme, Judge Wilkinson wrote, "There was no search because this case involved a straightforward application of [*Miller* and *Smith*]." *Chatrie*, 136 F.4th at 109 (Wilkinson, J., concurring) (citations omitted). While he made a glancing reference to *Carpenter*'s balancing test, it did not seem to sway him in the slightest. Wilkinson warned, "[P]rivacy is in part a peace of mind. The prospect of criminal malefactors intruding on that peace can only mean our privacy has

been compromised. That the transgression is attributable to private actors does not mean it cannot be part of the calculus of reasonableness." *Id.* at 110. He referred to his colleagues' arguments that geofence warrants violate the Fourth Amendment as an "assault." *Id.* at 109. While some share our Founders' concerns about invasions of privacy by government, Wilkinson wrote, "privacy is not invariably in an adversarial relationship with the state, but something the state can take measured steps to protect and provide." *Id.* at 110. *But see United States v. Smith*, 110 F.4th 817, 834 (5th Cir. 2024) ("*Carpenter*'s application to the third-party doctrine in this case is straightforward."); *id.* at 836 (holding the third-party doctrine does not apply to the geofence warrant at issue).

At the other extreme was Judge Wynn, who urged that "the principles enshrined in the Fourth Amendment . . . . be vigorously protected from ever-expanding methods of government intrusion." *Chatrie*, 136 F.4th at 115 (Wynn, J., concurring). *See also id.* at 117 (discussing the home intrusion in *Kyllo* and the "traditional trespass principles" applied by Justice Scalia in *Jones*); *id.* at 118 (discussing *Riley*'s treatment of an arrestee's cell phone as an "effect" under the Fourth Amendment). He rejected the view that users who share information with service providers like Google or X Corp. for a limited purpose thereby relinquish their Fourth Amendment rights: "Smartphone users might reasonably expect that their deidentified data will be used, in aggregate, to fine-tune targeted advertising. But it would be a grave misjudgment to conflate an individual's limited disclosure to Google with an open invitation to the state." *Id.* at 127 (citations omitted).

Judge Richardson discussed the same "voluntariness" factors from *Carpenter* as Judge Wynn, *id.* at 138-39 (Richardson, J., concurring), but reached a different result. Whereas Wynn focused on the *capacities* of Location History to implicate privacy concerns, *id.* at 126 (Wynn, J., concurring), Richardson focused narrowly on the *results* of the geofence warrant at issue, noting "the two hours' worth of Location History data that law enforcement obtained from Google at Step two" was "far less revealing than that obtained in *Jones*, *Carpenter*, or *Beautiful Struggle* and more like the short-term public movements in *Knotts*, which the Court found were 'voluntarily conveyed to anyone who wanted to look.'" *Id.* at 139 (Richardson, J., concurring) (citations omitted). In addition, Richardson found, contra Wynn, that "a user knowingly and voluntarily exposes his Location History data to Google." *Id.* at 140. "The third-party doctrine," he concluded, "squarely governs this case." *Id.* at 141.

Judge Berner also applied the *Carpenter* majority's balancing tests, but she analyzed the three steps of the Google geofence warrant process separately in terms of an additional factor: whether the information produced was "likely to be traceable to the identities of particular Google users." *Id.* at 143 (Berner, J., concurring). Only if it was traceable to individual users' identities, she argued, was the users' reasonable expectation of privacy in their Location Histories impacted under *Carpenter*. *Id.* at 144. *But see supra* pp. 18-19 (showing that even step one of the geofence warrant effected a trespass on user data and therefore should require a proper warrant). Berner disagreed with the Fifth Circuit's holding in *Smith* that geofence warrants were categorically unconstitu-

tional, *Chatrie*, 136 F.4th at 144 (Berner, J., concurring), but found the geofence warrant in this case was unconstitutional because it lacked probable cause. *Id.* at 153 ("A person's mere proximity to suspected criminal activity 'does not, without more, give rise to probable cause to search that person.'") (citation omitted).

Judge Gregory agreed with Judges Wynn and Berner that the geofence warrant violated the Fourth Amendment under *Carpenter*. *Id.* at 157 (Gregory, J., dissenting). Unlike them, however, he found that conclusion so obvious, he would have excluded the evidence against Petitioner Chatrie: "[A]n officer need not know the judiciary's view on the use of new technology with the Fourth Amendment to know that the information in the warrant was insufficient." *Id.* at 160.

As these varied opinions demonstrate, the amorphous quality of the *Katz* and *Carpenter* balancing tests allow judges and scholars to read into the various factors other values and normative commitments, including them among the demands to be weighed. *See also Carpenter*, 585 U.S. at 343 (Thomas, J., dissenting) ("[The *Katz* test] invites courts to make judgments about policy, not law."); *id.* at 357-58 ("Even Justice Harlan, four years after penning his concurrence in *Katz*, confessed that the test encouraged 'the substitution of words for analysis.'" (citing *White,* 401 U.S. at 745 (Harlan, J., dissenting)); *id.* at 393-94 (Gorsuch, J., dissenting) ("When judges abandon legal judgment for political will we . . . risk decisions where 'reasonable expectations of privacy' come to bear 'an uncanny resemblance to those expectations of privacy' shared by Members of this Court." (quoting *Minnesota v. Carter*, 525 U.S. 83, 97 (1998) (Scalia, J., concurring))).

The third-party doctrine of *Miller* and *Smith*, like any legal doctrine that is put through a *Katz*-ian filter, necessarily lacks ex ante clarity. Most importantly, as in the instant case, balancing demands for "anything under the sun," William James, *The Moral Philosopher and Moral Life*, in *The Will to Believe and Other Essays in Popular Philosophy* 201 (1956), often violates individual rights, the protection of which is a non-negotiable demand of a constitutional republic.[5]

CONCLUSION

The Court-created *Katz* test was "*added to*, not *substituted for*, the common law trespassory test." *Jones*, 565 U.S. at 409. If Justice Scalia were on this Court in 1967 to pen a majority opinion in *Katz*, everyone reading this brief might have better things to do. *See Kyllo*, 533 U.S. at 40 (holding unlawful search occurred when Thermovision imaging used to effect an intrusion into a home). The *Katz* test was intended to afford us more privacy; it was to be applied in cases in which the common law appeared too stingy. Now, thanks to the *Katz*-mediated expansion of the third-party doctrine in *Miller* and *Smith*, individuals lawfully exercise their common-law rights, intending and expecting their property rights and privacy to be protected, only to be told by courts that their expectations are not "reasonable." *See Carpenter*, 585 U.S. at 394-95 (Gorsuch, J., dissenting) (collecting "unbelievable"

---

[5] The history of the "right to privacy" has shown that laws directed specifically at invasions of privacy tend, in their application and proliferation, to erode fundamental rights to liberty and property. *See* Amy L. Peikoff, *Beyond Reductionism: Reconsidering the Right to Privacy*, 3 N.Y.U. J.L. & Liberty 1, 24-45 (2008).

cases in which courts rejected as unreasonable, expectations of privacy based on common-law rights).

This Court can fix this. For all the reasons stated in its briefing, amicus X Corp. urges this Court to find that the Government violated Petitioner Chatrie's Fourth Amendment rights—along with those of other Google users—when it obtained their Location Histories by means of a geofence warrant devoid of individualized suspicion. In so doing, this Court should, at the very least, continue to narrow or distinguish *Miller* and *Smith* from cases in which, as here, enforceable, privacy-protective terms of service are in place, and the user has asserted a right to exclude based on these terms. *See* Pet'r's Opening Br. at 15-16. This would allow individuals to decide for themselves what are "privacies of life" and what are not, and to exercise their common-law rights to liberty, property, and contract, accordingly.[6] Courts would be left with the relatively straightforward task of deciding whether an individual had exercised his or her right as necessary to protect a state of privacy against warrantless, suspicionless searches.

Allowing individuals to protect their privacy in this way would create market incentives for service providers to offer privacy-protective terms of service where none currently exist. Enforcing such terms would reduce barriers to offering more innovative uses of sensitive data that ultimately benefit society, and would also benefit law enforcement by reducing service providers' incentive to employ drastic methods—

---

[6] In those rare cases in which no common-law right has been or conceivably could be exercised to protect against a government agent's unreasonable search or seizure, clearly defined limitations on government power are called for.

such as end-to-end encryption, which Google has now implemented for Location History—that make it so, even with a proper, particularized warrant, third parties hold no data to be searched.

Respectfully submitted,

AMY PEIKOFF
Pacific Legal Foundation
3100 Clarendon Blvd.,
Suite 1000
Arlington, VA 22201
(202) 888-6881
apeikoff@pacificlegal.org

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

Counsel for Amicus Curiae X Corp.

MARCH 2026