No. 25-112

In the Supreme Court of the United States

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

On Petition For A 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.

QUESTIONS PRESENTED

This case concerns the constitutionality of geofence warrants. For cell phone users to use certain services, their cell phones must continuously transmit their exact locations to their service providers. A geofence warrant allows law enforcement to obtain, from the service provider, the identities of users who were in the vicinity of a particular location at a particular time.

In this case, law enforcement obtained, and served on Google, a geofence warrant seeking anonymized location data for every device within 150 meters of the location of a bank robbery within one hour of the robbery. After Google returned an initial list, law enforcement sought—without seeking an additional warrant—information about the movements of certain devices for a longer, two-hour period, and Google complied with that request as well. Then—again without seeking an additional warrant—law enforcement requested de-anonymized subscriber information for three devices. One of those devices belonged to Petitioner Okello Chatrie. Based on the evidence derived from the geofence warrant, Petitioner was convicted of armed robbery.

The questions presented are:

1. Whether the execution of the geofence warrant violated the Fourth Amendment.
2. Whether the exclusionary rule should apply to the evidence derived from the geofence warrant.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

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 necessarily collects, processes, and stores multiple classes of sensitive user data 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 37.2, 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] 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

As Judge Gregory noted below, while a majority of the en banc Fourth Circuit agreed "to affirm the district court's opinion," that is the only thing about which it agreed; "its reasoning is fractured." *United States v. Chatrie*, 136 F.4th 100, 157 (4th Cir. 2025) (Gregory, J., dissenting). The set of opinions exemplifies the division and confusion that exists, not only about geofence warrants, but more generally about the application of the third-party doctrine after this Court's ruling in *Carpenter v. United States*, 585 U.S. 296 (2018). By granting Okello Chatrie's petition, this Court can clear up the confusion about both issues, helping ensure uniform Fourth Amendment protection for sensitive data belonging to users of services which have become integral to our specialized, technologically advanced economy.

At one extreme was Judge Wilkinson, who saw this case as involving a "straightforward application" of this Court's rulings in *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976). *Chatrie*, 136 F.4th at 109 (Wilkinson, J., concurring). At the other extreme was Judge Wynn, who, after applying the *Carpenter* majority's "two amorphous balancing tests," comprised of "a series of weighty and incommensurable principles," *Carpenter*, 585 U.S. at 397 (Gorsuch, J., dissenting), concluded, first, "when the Government accessed Location History data that was traceable to Chatrie, it invaded his reasonable expectation of privacy," *Chatrie*, 136 F.4th at 125 (Wynn, J., concurring), and second, Chatrie's sharing of his Location History with Google was not

"meaningfully voluntary," and so did not undermine that expectation. *Id.* at 127.

Disagreements about the application of multi-factor balancing tests are not surprising. This balancing-test approach in Fourth Amendment jurisprudence stems from the infamous *Katz* "reasonable expectation of privacy" test. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Judge Berner's suggestion below, that a search occurs when government obtains data that is non-anonymous or "likely to be traceable to a particular individual," *Chatrie*, 136 F.4th at 156 (Berner, J., concurring), can be added to the parade of considerations courts must attempt to weigh post-*Carpenter*, including:

- How long is the period of time to which the data corresponds? *See, e.g., Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 341 (4th Cir. 2021) (interpreting *Carpenter* as "solidif[ying] 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" is the data? *See, e.g., United States v. Smith,* 110 F.4th 817, 832 (5th Cir. 2024) (noting 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.*, *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);

- Does the data facilitate retrospective tracking? *See*, *e.g.*, *Chatrie*, 136 F.4th at 121 (Wynn, J., concurring) (noting that the CSLI at issue in *Carpenter* "allowed police to 'travel back in time' to 'reconstruct a person's movements,' unlocking 'a category of information otherwise unknowable.'") (quoting *Carpenter*, 585 U.S. at 312);
- Should courts focus on "capabilities" of the relevant technology, or "results," that is, the data obtained by government in a given case? *See Chatrie*, 136 F.4th at 126 (Wynn, J., dissenting) (noting that Location History has the capacity to "track a person's 'physical presence,'" and therefore "'implicates privacy concerns far beyond those considered in *Smith* and *Miller*.'") *Cf. id.* at 139 (Richardson, J., concurring) (noting that "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
- Was the sharing "meaningfully voluntary"? *See Chatrie*, 136 F.4th at 141 (Richardson, J., concurring) (noting that "unlike CSLI, Location History data is obtained by a user's affirmative act."). *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.") (citations omitted).

And so on. This miasma is, as Justice 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) ("[Particularized warrants were] 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 Google and X Corp. from acting according to their own judgment in relation to both government and their users. Google recently made a major change to its product architecture by no longer collecting Location History in Sensorvault, which was used to store the data at issue in this case; location data is now stored on the user's device, where it is less available to Google to retrieve in response to legal process. Ryan Whitwam, *Oops: Google says it might have deleted your Maps Timeline data*, Ars Technica (Mar. 24, 2025).[3] Was this a decision Google made to avoid being coerced into

[3] https://tinyurl.com/46snw6sa.

helping governments undermine its users' property rights and privacy through an end run around the Fourth Amendment?

Amicus X Corp. urges this Court to grant Petitioner Chatrie's Petition for a Writ of Certiorari. This case presents an opportunity to clarify this area of constitutional law by tethering a decision to the Fourth Amendment's original meaning: all searches of private property require warrants based on particularized probable cause, *Jones*, 565 U.S. at 404-10 (holding a search occurred when government obtained information by means of trespass on a constitutionally protected "effect"), 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 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*

---

[4] *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 Harv. L. Rev. 757, 761 (1994) (presenting and arguing for a "[r]efurbished" Fourth Amendment, through analysis of both the amendment's text and the common law). *But see Carpenter*, 585 U.S. at 355-58 (Thomas, J., dissenting) (comparing "reasonable" as used in the Fourth Amendment's text to the term's 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.

Lange v. California, 594 U.S. 295, 309 (2021) (noting the common law may be instructive regarding what searches the Founders would have considered 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).

Amicus X Corp. agrees that, for Fourth Amendment purposes, Petitioner Chatrie has property rights in his Location History as recognized in Google's terms of service, *Chatrie*, No. 25-112, Brief of Petitioner 31-32, and therefore his Fourth Amendment rights were violated when government obtained his data without a warrant based on particularized probable cause. This case and others involving reverse searches of 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.

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 is what Judge Wynn referred to as a "mechanical appl[ication]" of the doctrine. *Chatrie*, 136 F.4th at

125 (Wynn, J., concurring). It says the Fourth Amendment is not implicated when: (1) you share information with a third party—for example, your bank, your phone company, Google, or X Corp.—even for a limited purpose; and (2) the third party then shares the information with the government. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561, 563 (2009). The doctrine's history, however, is key to understanding 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 this 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 dramatically expanded to apply, not only to mafia dons, but also to ordinary, innocent citizens who share 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[.]"). But the digital age brought about a new set of pernicious consequences this 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, *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 hold that the government violated the rights of Chatrie and other Google users in this case. But the law in this area is, to be blunt, a mess. Amicus X Corp. believes this Court should grant Petitioner Chatrie a 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*, as both failed to justify the third-party doctrine in its pre-*Carpenter* form.[6]

---

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

[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 overt reference to the *Miller* Court's question-begging rationale. The closest the *Smith* majority got to acknowledging the issue was this footnote:

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. *See*, *e.g.*, *Chatrie*, 136 F.4th at 127 (Wynn, J., concurring) ("[I]t would be a grave misjudgment to conflate an individual's limited disclosure to Google with an open invitation to the state."). 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).

> 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), does not extinguish a "legitimate expectation of privacy"—much less a property right protected by the Fourth Amendment. Especially considering arguments raised *against* the third-party doctrine since *Smith* and *Miller*, reconsideration of this Court's rulings in those cases is appropriate.

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. *See, e.g.*, *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."). A fortiori, that one user breaks the law does not entitle the government to trample on the rights of other, law-abiding users who might be ensnared by constitutionally insufficient, dragnet warrants or similarly unreasonable searches. Accordingly, promises made to users by these companies to, e.g., safeguard user data and disclose it in only limited, enumerated circumstances are enforceable under common law according to their terms, just as (to use a pertinent 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]

---

[7] Justice Gorsuch dissented in *Carpenter* on the narrow ground that Carpenter did not invoke contract- or property-based arguments. While he noted such arguments could justify Fourth Amendment protection of Carpenter's cell-site location information ("CSLI"), the *Carpenter* majority did not reach the issue.

[8] *See* Christina Del Rosso & Carol M. Bast, *Protecting Online Privacy in the Digital Age:* Carpenter v. United States *and the*

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 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 a "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

---

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 warrants that the Fourth Amendment ultimately intended to prevent.") (citation omitted).

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) (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 divine whether one had a "reasonable expectation of privacy." *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

Decades later Justice Antonin Scalia helped reverse this trend, explaining in *United States v. Jones*, 565 U.S. at 400, 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.*; *see 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."). Fourth Amendment rights are not automatically 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 Chatrie's rights under his contract with Google are relevant to the Fourth Amendment protection his Location History deserves 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 law for the benefit of

lower courts and litigants—i.e., service providers and users—alike. Moreover, doing so would restore and reinforce the baseline of protection that the Fourth Amendment should and was intended to provide, something 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 Minn. L. Rev. 101, 108 (2020) ("[I]mporting contract tools of interpretation [into data privacy] holds significant promise 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* 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). 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, "[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 Chatrie 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 Google 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, or to allow a user to control or delete it, that promise should be heeded and should not be terminable by government fiat. Such contracts should be recognized as legitimate means for preserving one's property and privacy. As Justice Sotomayor wrote regarding one "weighty or incommensurable 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).[9] What should matter for

[9] Justice Sotomayor inspired many to reconsider 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

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.

---

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."); *and id.* at 390 (alluding to a "secret-agent-case" scenario, 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 happened to be an undercover government agent).

CONCLUSION

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. That a majority of the Fourth Circuit failed to reach this conclusion demonstrates how muddled the law in this area is in the wake of *Carpenter*.

This Court should grant Chatrie 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 experience with this Court-created doctrine.

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.

AUGUST 2025