No. 26-460

In the Supreme Court of the United States

ADAM BLOCKER, *Petitioner,*

v.

UNITED STATES

On Petition for Writ of Certiorari
to the United States Court of Appeals
for the Seventh Circuit

BRIEF OF *AMICUS CURIAE*
PROJECT FOR PRIVACY & SURVEILLANCE ACCOUNTABILITY, INC.
SUPPORTING PETITIONER

GENE C. SCHAERR
Counsel of Record
ERIK S. JAFFE
JUSTIN A. MILLER
SCHAERR | JAFFE LLP
1717 K Street NW, Suite 900
Washington, DC 20006
Telephone: (202) 787-1060
gschaerr@schaerr-jaffe.com

Counsel for Amicus Curiae

NOVEMBER 6, 2026

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

INTRODUCTION, SUMMARY, AND INTEREST OF *AMICUS CURIAE* 1

STATEMENT 3

ADDITIONAL REASONS FOR GRANTING THE PETITION 5

I. *Carpenter* and *Chatrie* confirm that private service agreements do not automatically extinguish reasonable expectations of privacy. 6

II. Dropbox's terms do not objectively authorize a government search. 8

III. The decision below improperly makes Fourth Amendment protection turn on providers' drafting choices, with nationwide consequences. 13

CONCLUSION 15

TABLE OF AUTHORITIES

Cases **Page(s)**

Bumper v. *North Carolina*,
391 U.S. 543 (1968) 12

Carpenter v. *United States*,
585 U.S. 296 (2018) 3, 6, 8, 12, 14

Ex parte Jackson,
96 U.S. (6 Otto) 727 (1877) 2

Florida v. *Jimeno*,
500 U.S. 248 (1991) 2, 9, 10, 12

Riley v. *California*,
573 U.S. 373 (2014) 6

Schneckloth v. *Bustamonte*,
412 U.S. 218 (1973) 9

Stoner v. *California*,
376 U.S. 483 (1964) 2

United States v. *Lowers*,
170 F.4th 134 (4th Cir. 2026) 11

United States v. *Maher*,
120 F.4th 297 (2d Cir. 2024) 11

United States v. *Miller*,
425 U.S. 435 (1976) 6

United States v. *Shelton*,
997 F.3d 749 (7th Cir. 2021) 12

United States v. *Warshak*,
631 F.3d 266 (6th Cir. 2010) 11

United States v. *Young*,
350 F.3d 1302 (11th Cir. 2003) 11

INTRODUCTION, SUMMARY, AND INTEREST OF *AMICUS CURIAE*[1]

This case presents an important Fourth Amendment question: Does accepting a cloud provider's standard-form agreement count as consent to a government search of the user's private files based on contract principles? Or must consent turn on a reasonable expectation of privacy? The circuits are split. And the standard for such consent merits this Court's review.

The Seventh Circuit decision here presents a good vehicle to review this question. The panel below held that Petitioner Adam Blocker consented to the warrantless inspection of files stored in his Dropbox account, even if Dropbox acted as a government agent. It held that, by accepting *Dropbox*'s terms of service, Petitioner consented to the *government*'s search. But the Terms of Service contain no express authorization for a government search. Instead, they begin by assuring users that "Your Stuff is yours," then explain that Dropbox needs limited access to provide features such as previews, sorting, editing, and searching. App.11a-12a. A separate provision permits Dropbox to review content for compliance with its policies. App.12a. But those policies are only visible by hyperlink. *Ibid.* The government-disclosure provisions also appear only in a separately hyperlinked Privacy Policy—which immediately assures users that their

---

[1] This brief was not authored in whole or in part by counsel for any party and no person or entity other than *amicus curiae* or its counsel or members has made a monetary contribution toward the brief's preparation or submission. Counsel of record for all parties received timely notice of *amicus*'s intent to file this brief.

data should receive the same legal protection whether stored in the cloud or on a home computer. App.13a-14a.

On the panel's reasoning, these layered contractual permissions establish consent to a government search. So, when an American in Illinois or Ohio or New York or Florida stores their electronic papers in the same cloud, the Fourth Amendment consequences of those same contractual provisions differ depending on the circuit.

But consent to a government search is measured by what the user's agreement objectively authorized. See *Florida* v. *Jimeno*, 500 U.S. 248, 249-251 (1991). And here, the expressed object of permission a user gives a company to police its own platform is not consent to a government search for evidence. That distinction is deeply rooted in this nation's history. A letter sealed and handed to the Postal Service remained protected as if kept in the sender's own home. See *Ex parte Jackson*, 96 U.S. (6 Otto) 727, 732-733 (1877). And a custodian entrusted with another's property does not thereby gain authority to admit the government to search it. See *Stoner* v. *California*, 376 U.S. 483, 488-490 (1964). Letting a plumber into one's home to fix a sink does not surrender any expectation of privacy when the police come knocking.

As for digital custodians, however, the courts of appeals no longer agree on where that line falls. The Seventh Circuit itself recognized that its own precedent is "incompatible with the approach taken in" the Second, Fourth, and Sixth Circuits and that "[a] conflict among the circuits would persist no matter

what [it] did." App.8a. And it added that "the Supreme Court may eventually need to address the conflict." App.9a.

The disagreement is not academic. Roughly 88% of Americans now keep files in the cloud. Pet.14-15 (citation omitted). And now in the Seventh and Eleventh Circuits, standard-form inspection provisions may establish consent to government searches even though comparable provisions do not have that effect in other circuits. That disagreement cries out for the Court's review.

Resolution of that question consistent with the Fourth Amendment is important to *amicus* Project for Privacy & Surveillance Accountability, Inc. ("PPSA"). PPSA is a nonprofit, nonpartisan organization devoted to keeping Fourth Amendment protection from being left "at the mercy of advancing technology." *Carpenter* v. *United States*, 585 U.S. 296, 304-305 (2018) (citation omitted). PPSA has a particular interest in preventing the terms that Americans must accept to function online from being treated as constitutional consent without examining what reasonable users understand those terms to mean. Private contracts can authorize inspections. But the Fourth Amendment must independently determine whether they establish voluntary consent to a government search.

STATEMENT

Dropbox stores its customers' files and lets them back up data, work across devices, and share files with others. App.1a-2a. Using the service requires accepting Dropbox's terms. The Terms begin by explaining that Dropbox's Privacy Policy governs how

it collects and uses information, while its Acceptable Use Policy outlines users' responsibilities. Both are visible only through hyperlinks. The Terms then assure the customer's ownership: "Your Stuff is yours," and give Dropbox no rights to it "except for the limited rights that enable [Dropbox] to offer the Services." App.11a. To provide those services, the user gives Dropbox permission to "access, store, and scan Your Stuff" to provide features such as thumbnails, previews, sorting, editing, sharing, and searching. App.12a. Separately, under "Your Responsibilities," Dropbox states it "may review your conduct and content for compliance" with its policies, but "ha[s] no obligation to do so." *Ibid.* The hyperlinked Privacy Policy, in turn, permits disclosure when Dropbox "determine[s] that such disclosure is reasonably necessary" for specified purposes, including compliance with legal process and appropriate government requests. App.13a-14a. Immediately after that statement, in the same section it assures users that their "data should receive the same legal protections regardless of whether it's stored on our Services or on your home computer's hard drive." App.14a.

Dropbox also entered agreements with NCMEC concerning the use of PhotoDNA technology to identify apparent child pornography. Under a 2014 agreement, Dropbox received access to the technology to assist NCMEC's mission; a subsequent agreement addressed Dropbox's use of NCMEC's signatures to identify prohibited material. Pet.7-8. The examination here began when Dropbox's automated tool flagged files in Petitioner's account. App.15a. A Dropbox employee

then reviewed those files and reported them to the National Center for Missing & Exploited Children (NCMEC). *Ibid.* NCMEC viewed the files and sent them to the FBI, and the FBI viewed them before obtaining warrants for Petitioner's home and his Dropbox account. App.16a.

The district court denied suppression based on consent, and the Seventh Circuit affirmed. The panel assumed that NCMEC is part of the government and that Dropbox acted as its agent. But even given those assumptions, the panel held that Petitioner's agreement to the terms supplied consent that "eliminates any need for probable cause or a warrant." App.3a-5a. Analogizing to a person who tells police, "You may search my house," the panel reasoned that an option to inspect "remains a consent," App.6a, while acknowledging that Petitioner had "allowed Dropbox (but not Google or T-Mobile) to inspect his files," App.8a. The panel then recognized the resulting "conflict among the circuits." App.8a.

ADDITIONAL REASONS FOR GRANTING THE PETITION

The decision below presents an acknowledged circuit split on how a user's acceptance of a cloud provider's standard-form agreement affects his Fourth Amendment rights. This issue merits this Court's review for three reasons. First, *Carpenter* and *Chatrie* establish that entrusting private information to a digital service provider does not itself extinguish a reasonable expectation of privacy. Neither decision resolves whether accepting the provider's terms is consent to government search. Second, the decision

below treats the user's consent as a contractual issue of unconscionability and adhesion rather than a Fourth Amendment issue of reasonable expectations. Third, the decision threatens to make Fourth Amendment protection depend—improperly—on standard-form contracts that users rarely negotiate and that providers may revise under government pressure. That concern is even more significant now that cloud storage is an ordinary way to keep private papers.

I. *Carpenter* and *Chatrie* confirm that private service agreements do not automatically extinguish reasonable expectations of privacy.

This case offers the Court a good vehicle to address an important question at the intersection of reasonable expectations of privacy and constitutional consent. *Carpenter* rejected the view that sharing information with a third party removes that information from the Fourth Amendment's protection. Disclosure can diminish privacy. But "the fact of 'diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely.'" *Carpenter*, 585 U.S. at 314 (quoting *Riley* v. *California*, 573 U.S. 373, 392 (2014)). And disclosure must be weighed against "the nature of the particular documents sought." *Ibid.* (quoting *United States* v. *Miller*, 425 U.S. 435, 442 (1976)). That inquiry reflects modern life. Using essential digital services frequently requires entrusting sensitive information to private providers. A contractual relationship does not itself resolve whether a user reasonably expects that

information to remain protected against government searches.

Chatrie applied that understanding to data held under a provider's terms, rejecting the contention that a user "los[es] his legitimate expectation of privacy" by "authoriz[ing] Google to collect, retain, and use" his information. 609 U.S. at 632-633 (internal citations omitted); accord Pet.5, 21. It did so even though the government pointed to a privacy policy telling users their data could be shared when "reasonably necessary" to comply with "legal process." Pet.21 (citation omitted).

Those terms are close to Dropbox's here. *Ibid.* A cell-phone user, this Court explained, "is not to be viewed as sharing private information with third parties—which then can be freely passed on to the government—just by doing the ordinary things cell-phone users do." *Chatrie* v. *United States*, 609 U.S. 605, 637 (2026); accord Pet.2. Justice Gorsuch, concurring in the judgment, would have reached the same result on a property rationale, reasoning that the government "conducted a search * * * when it compelled Google to rummage through Mr. Chatrie's data." *Chatrie*, 609 U.S. at 650-651 (Gorsuch, J., concurring in judgment); accord Pet.20-21.

To be sure, the compelled disclosure in *Chatrie* differs from Dropbox's initial voluntary inspection. But *Chatrie* establishes that private contractual disclosures do not automatically determine the constitutional protection afforded digital information. Dropbox's recognition that "Your Stuff is yours," App.11a, reinforces the importance of examining the

user's retained interests rather than treating contractual access permissions as dispositive.

Still, *Carpenter* and *Chatrie* did not decide the question here. Each addressed whether a user keeps a reasonable expectation of privacy in data a provider holds. Neither addressed whether agreeing to the provider's terms supplies consent to a government search.

Nor does a reasonable expectation of privacy preclude valid consent to a particular inspection. The questions are distinct: whether the Fourth Amendment protects the information, and whether the user voluntarily authorized the search actually conducted. But the constitutional analysis cannot permit ordinary contract principles to accomplish through purported consent what *Carpenter* and *Chatrie* reject through the third-party doctrine—automatic loss of protection merely because information was entrusted to a service provider.

The panel below predicted that if *Chatrie* "does not address the validity of consents that permit but do not compel disclosures to public officials," this Court "may eventually need to address the conflict." App.9a. This petition presents a good vehicle to address that conflict. This Court should grant review to clarify the governing standard.

II. Dropbox's terms do not objectively authorize a government search.

Boilerplate Terms of Service like Dropbox's are a flimsy reed on which to base constitutional consent to search. See Pet.26 n.9. Yes, the Fourth Amendment permits a search conducted with consent. See

Schneckloth v. *Bustamonte*, 412 U.S. 218, 227-229 (1973). But consent is measured by "'objective' reasonableness—what would the typical reasonable person have understood." *Florida* v. *Jimeno*, 500 U.S. 248, 249-251 (1991). Its scope is "defined by its expressed object." *Id.* at 251-252. The inquiry asks whether a reasonable user would understand Dropbox's terms to authorize the government search at issue, not merely whether the terms give Dropbox a contractual right to inspect. Contract law may impute assent to hyperlinked provisions. That does not itself establish voluntary consent to a government search. At minimum, the claimed consent must be clear enough that a reasonable user would understand the authorized intrusion.

Those terms present a good vehicle for this Court to consider consent and Terms of Service. Contrary to the Seventh Circuit's decision, the terms do not plainly authorize a government search for evidence. The agreement begins by confirming that the files remain the user's: "Your Stuff is yours," subject only to "the limited rights that enable [Dropbox] to offer the Services." App.11a. The operational permissions that follow are tied to those services—the user lets Dropbox "access, store, and scan Your Stuff" to provide features, and that permission "extends to [Dropbox's] affiliates and trusted third parties we work with." App.12a. Dropbox separately "may review" content "for compliance" with its policies, though it "ha[s] no obligation to do so." *Ibid.*

The distinction between those provisions goes to the objective reasonableness of Petitioner's purported consent to the government's search. See *Jimeno*, 500

U.S. at 249-251. Dropbox's Terms explain its scanning permissions by reference to ordinary service features—thumbnails, document previews, sorting, editing, sharing, and searching. Nothing in those Terms objectively shows Petitioner's consent to a government search.

The disclosure provision appears only in the separately hyperlinked Privacy Policy. That policy permits disclosure whenever Dropbox "determine[s] that such disclosure is reasonably necessary" to comply with law, regulation, legal process, or an "appropriate government request"; to protect a person from death or serious injury; to prevent fraud or abuse; to protect Dropbox's own rights, property, safety, or interest; or to perform a task in the public interest. App.13a-14a. That is a wide grant of authority. But it is a grant of authority to *Dropbox* to decide when to disclose information for those ends. It does not objectively establish the user's agreement that a government agent may search his files for criminal investigation. A provider's discretion to disclose in defined situations differs from a user's blanket consent to government searches.

And that disclosure provision must be read in conjunction with the immediately following statement that a user's "data should receive the same legal protections regardless of whether it's stored on our Services or on your home computer's hard drive." App.14a. Under the objective-reasonableness standard, a user would understand that promise to preserve the protection his files receive at home, not to waive it. Read as a whole, then, the Terms do not clearly communicate a waiver of constitutional

protection against a government search. That distinction is dispositive in the Second, Fourth, and Sixth Circuits. See Pet.11-12 (citing *United States* v. *Maher*, 120 F.4th 297, 302 (2d Cir. 2024); *United States* v. *Lowers*, 170 F.4th 134, 147 (4th Cir. 2026); *United States* v. *Warshak*, 631 F.3d 266, 286-287 (6th Cir. 2010)). The question there is not whether Dropbox had contractual authority to inspect Petitioner's files, but whether that authority objectively communicated the user's consent to the government inspection. But in the Seventh and Eleventh Circuits, those hyperlinked policies are enough to waive the Fourth Amendment's protections. See Pet.13-14 (citing Pet.8a; *United States* v. *Young*, 350 F.3d 1302, 1308-1309 (11th Cir. 2003)).

The Seventh Circuit's house-search analogy illustrates the gap that has opened for consent and storing papers in the cloud. Telling the police "You may search my house" expressly authorizes the government to search. App.6a. But Dropbox's terms do something different. They grant defined permissions to Dropbox and the "trusted third parties" that help it run the service, App.12a, and they let Dropbox disclose information only in specified circumstances, App.13a-14a. The panel itself marked the difference when it observed that Petitioner had allowed "Dropbox (but not Google or T-Mobile) to inspect his files." App.8a. Whether permission framed that way nevertheless authorizes a government search now divides the courts of appeals. See Pet.10-14. But a user's decision to allow some third parties access to data for particular purposes hardly suggests abandonment of a reasonable expectation of privacy as to others—

especially the government. The Seventh Circuit's *United States* v. *Shelton* decision illustrated the difference, holding that permission to enter an office for business purposes did not necessarily extend to entry to gather evidence for the government. 997 F.3d 749, 766-767 (7th Cir. 2021).

Nor does the enforceability of the contract answer the constitutional question. The panel treated the dispute as one of contract interpretation, enforcing the terms unless unconscionable. App.6a. But the scope of Fourth Amendment consent turns on what a reasonable person would understand the agreement to authorize the government to do—not on whether the agreement binds the user and Dropbox as a matter of private law. See *Jimeno*, 500 U.S. at 249-251.

The actual Terms and policies illustrate the difference. Contract law may bind users to provisions incorporated through hyperlinks, even if the user never opens them. But in the Second, Fourth, and Sixth Circuits, constitutional consent cannot be established merely by imputing knowledge of every incorporated provision. The opposite is true in the Seventh and Eleventh Circuits. That split merits review to preserve "that degree of privacy against government that existed when the Fourth Amendment was adopted." *Carpenter*, 585 U.S. at 305 (quoting *Kyllo*, 533 U.S. at 34).

Measuring constitutional consent by the enforceability of a private contract is a question of federal constitutional law. Cf. *Bumper* v. *North Carolina*, 391 U.S. 543, 548-550 (1968) (consent is not shown "by * * * no more than acquiescence to a claim

of lawful authority"). The courts of appeals have resolved this question in conflicting ways. Only this Court can settle it. The Fourth Amendment should not permit constitutional consent to be manufactured through contractual implication. A person may authorize a private cloud provider to inspect files, including1 for violations of its policies, without necessarily authorizing an inspection conducted on the government's behalf. When the government relies on such permission to dispense with the warrant requirement, the constitutional inquiry must demand a clear indication that the user objectively consented to the government intrusion. Nothing in Dropbox's Terms expressly communicates that consequence. Instead, the agreement emphasizes the user's ownership, explains inspection permissions in terms of operating the service and enforcing its policies, and incorporates a Privacy Policy that expressly affirms continued legal protection. Whether those provisions establish consent to a government search is a question this Court should resolve.

III. The decision below improperly makes Fourth Amendment protection turn on providers' drafting choices, with nationwide consequences.

If accepting a provider's terms authorizes a government search, then the protection a user's files receives depends on language the government did not write and that the provider may revise at will. See App.5a; Pet.14. Constitutional protection should not expand and contract with each edit to a company's boilerplate—which few people even read.

Dropbox's Terms illustrate the danger. The agreement assures users that their files remain theirs, explains scanning through ordinary service functions, and places government-disclosure provisions in a separately linked policy. Yet the decision below treats those provisions as sufficient to establish consent to an inspection a government agent conducts. If that is enough, constitutional protection could depend on contractual provisions that users neither meaningfully negotiate nor reasonably understand as waiving Fourth Amendment rights. Those rights should not turn on geography for nearly ubiquitous cloud services necessary to functioning in modern life.

Those consequences are not confined to this prosecution. Americans store their most sensitive records—financial, medical, personal, and expressive—with providers whose contracts reserve the same inspection and disclosure options as Dropbox's. Pet.14-18. The decision below allows those provisions to establish constitutional consent to certain warrantless inspections, even when the provider is assumed to be acting as a government agent.

But, as the petition explains (at Pet.11-14), other circuits have taken a different approach to comparable contractual permissions. That disagreement affects the protection afforded enormous quantities of sensitive information. Those protections of electronic papers should not become the victims "of advancing technology." *Carpenter*, 585 U.S. at 304-305 (quoting *Kyllo*, 533 U.S. at 35). This Court should grant review to address this issue, which affects most Americans and now divides the circuits.

CONCLUSION

The Fourth Amendment requires voluntary consent measured by what a reasonable person would understand the permission to authorize. That standard should not depend—as it does under the decision below—on conflicting interpretations of standard-form agreements governing the electronic papers of millions of Americans. The Court should grant the petition.

Respectfully submitted,

GENE C. SCHAERR
Counsel of Record
ERIK S. JAFFE
JUSTIN A. MILLER
SCHAERR | JAFFE LLP
1717 K Street NW, Suite 900
Washington, DC 20006
Telephone: (202) 787-1060
gschaerr@schaerr-jaffe.com

Counsel for Amicus Curiae

November 6, 2026