

In the
United States Court of Appeals
For the Seventh Circuit

No. 25-1536

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

ADAM BLOCKER,

Defendant-Appellant.

Appeal from the United States District Court for the
Northern District of Illinois, Eastern Division.
No. 20 CR 704 — **Virginia M. Kendall**, *Chief Judge*.

ARGUED FEBRUARY 12, 2026 — DECIDED MAY 5, 2026

Before EASTERBROOK, PRYOR, and MALDONADO, *Circuit Judges*.

EASTERBROOK, *Circuit Judge*. Dropbox stores customers' data on its own servers or space furnished by other firms. People can use Dropbox to synchronize files across multiple devices, back up data, offload data to the cloud and free up local storage, and share files with others.

Access to Dropbox is contingent on agreement to its terms of service. One term provides that “Your Stuff” (the users’ data) belongs to the user: Dropbox disclaims authorship, ownership, or any right to publish the information. Another term provides that Dropbox may examine the data to ensure that it is not being used for illegal purposes, such as fraud, copyright infringement, or obscenity. A third term adds:

We may disclose your information to third parties if we determine that such disclosure is reasonably necessary to: (a) comply with any applicable law, regulation, legal process, or appropriate government request; (b) protect any person from death or serious bodily injury; (c) prevent fraud or abuse of Dropbox or our users; (d) protect Dropbox’s rights, property, safety, or interest; or (e) perform a task carried out in the public interest.

In 2018 Dropbox informed the National Center for Missing and Exploited Children (NCMEC or the Center) that it had found child pornography in files that Adam Blocker was sharing with third persons. It sent the files to the Center, which alerted federal authorities. The FBI obtained a search warrant for Blocker’s computers and storage, including the data at Dropbox. The search located child porn in addition to the images that Dropbox had sent to the Center. Blocker pleaded guilty to two counts related to child pornography, 18 U.S.C. §2252A(a), reserving the right to contest on appeal the district court’s denial of his motion to suppress the evidence. He is serving a term of 120 months’ imprisonment.

Blocker’s main problem is that the Fourth Amendment, on which he relies, applies only to searches and seizures by public officials. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). Private searches and seizures are outside its scope, and Dropbox is a private entity. Blocker observes, however, that the Center holds a charter from the United States, receives public

money, and has been designated as the national clearing-house for reports of child pornography. 18 U.S.C. §2258A. At least one court of appeals has held that this makes the Center part of the government. *United States v. Ackerman*, 831 F.3d 1292, 1296–1300 (10th Cir. 2016) (Gorsuch, J.). Contra, *United States v. Meals*, 21 F.4th 903, 908 (5th Cir. 2021). Our decision in *United States v. Bebris*, 4 F.4th 551, 558 (7th Cir. 2021), assumes that *Ackerman* is correct, and we do the same today (without deciding the point). Blocker observes that Dropbox promised to tell the Center when it detects child porn on its servers. The Center agreed in exchange to furnish Dropbox with software that would assist in detection. This means, Blocker insists, that Dropbox’s acts are fairly attributable to the United States and so are governed by the Fourth Amendment, see *United States v. Hudson*, 86 F.4th 806 (7th Cir. 2023), and are unconstitutional because it searched his files without probable cause or a warrant.

It is far from clear to us that an entity’s practice of sending information to a governmental body makes that entity the equivalent of the government itself. Federal Express routinely tells the DEA when it discovers illegal drugs in parcels, but courts just as routinely hold that searches by FedEx are private activity. *Jacobsen* itself involved a search by FedEx. See also, e.g., *United States v. Koenig*, 856 F.2d 843, 846–50 (7th Cir. 1988); *United States v. Young*, 153 F.3d 1079 (9th Cir. 1998); *United States v. Smith*, 383 F.3d 700, 705–06 (8th Cir. 2004); *United States v. Gonzalez*, 781 F.3d 422, 427–28 (8th Cir. 2015). Why should searches by Dropbox be different? True, federal law requires entities such as Dropbox to report known child pornography, but the statute says that it does not require any service to monitor its customers’ data to produce the knowledge that would trigger a duty to report. 18 U.S.C.

§2258A(f). That leaves in private hands the choice whether to search the files' content.

Potentially it matters *why* Dropbox looked through its users' files and sent child porn images to the Center. Was it to carry out a governmental program imposing duties on Dropbox? If so, perhaps Dropbox acted as a governmental agent. Or was it to implement a policy that Dropbox formulated on its own? The prosecutor insists that Dropbox looks at users' data to avoid distributing unlawful files, which would carry both moral and reputational costs. In response to a motion during discovery, Dropbox explained that it "has a private business interest in enforcing" its prohibition on child pornography and "keeping its platform safe for account holders and others by voluntarily searching for and removing this content." That makes business sense: people might elect not to use Dropbox if it distributes child pornography (as Blocker was using it to do). This private motive makes the search look private. See *Bebris*, 4 F.4th at 554–55 (rejecting a challenge to a district court's conclusion that a search by Facebook of content on its servers was private activity).

As it happens, however, this is not the ground on which the district court denied the motion to suppress. Instead District Judge Lee (as he then was) ruled that Blocker consented to the search. (The case was transferred to Judge Kendall after Judge Lee was appointed to this court.) Voluntary consent eliminates any need for probable cause or a warrant, even when police do the searching. *Schneckloth v. Bustamonte*, 412 U.S. 218 (1973).

Blocker assented to Dropbox's terms of service, which allow Dropbox to review stored data to ensure that its service is being used lawfully. Judge Lee found this enough to reflect

Blocker's consent. Blocker replies that Dropbox's terms of service are just so much fine print that he and many other users accept because they want to use the service, and he asks us to hold that the terms are not clear enough to consent to a search in which a public body such as the Center has an interest. Three courts of appeals appear to have adopted that approach. See *United States v. Lowers*, 170 F.4th 134, 145–48 (4th Cir. 2026); *United States v. Maher*, 120 F.4th 297, 307–09 (2d Cir. 2024); *United States v. Warshak*, 631 F.3d 266, 286–87 (6th Cir. 2010).

We acknowledge that few people pore over consumer contracts or try to grasp how they might work in practice. See Omri Ben-Shahar & Carl E. Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* (2014). Yet the fact that a contract is lengthy and poorly understood does not justify reading it with a thumb on the scale. The language of this contract unambiguously permits Dropbox to scan all files at its option and reveal the contents for five specified purposes—and Blocker does not deny that, having discovered child porn, one or more of these purposes applies.

Neither the language of this contract nor the effect of similar consumer contracts turns on whether a unit of government has a view about what should happen. So if the fine print in a contract to buy a car includes a limited warranty (say, three years or 50,000 miles rather than lifetime), then the manufacturer can reject a request for warranty service if a part fails after four years, even if the reason for doing so turns out to be the urging of a highway-safety agency. If the fine print in a credit-card agreement contains an arbitration clause, then any dispute goes to arbitration whether the Consumer Financial Protection Bureau favors or discourages arbitration.

The law of contracts has one important proviso: unconscionable clauses will not be enforced. *Restatement of Consumer Contracts* §6 comment 1 (2024). But Blocker does not contend that it is unconscionable for a firm such as Dropbox to prevent its service from being used to distribute child porn or to alert public officials when it discovers that its service has been put to illegal use.

Decisions such as *Lowers*, *Maher*, and *Warshak* conclude that language similar to Dropbox’s is insufficient because it says that a service *may* examine and disclose the contents of their files, rather than that they *will* do so. We do not see why this should matter. “You may search my house” authorizes a search by the police, whether or not the police guarantee that they will conduct a search. A consent granting an option to search remains a consent. Perhaps a flat statement that “we inspect all files every day” would do more to alert users—but such a statement may not be honest. The record of this case does not show the probability that any given file on Dropbox will be inspected, or how often. What matters—at least, what ought to matter—is a clear grant of permission to inspect. Similarly, consumers who sign bills of lading permitting FedEx to inspect the contents of their packages do not expect it to open every package in search of liquor or drugs or firearms or poison—inspection is infrequent—but, when FedEx *does* open a package, it can rely on the consent.

This isn’t the first time we have encountered a broadly worded consent found in a consumer contract. *United States v. Adkinson*, 916 F.3d 605 (7th Cir. 2019), enforced a consent in a contract between T-Mobile and a user of its telecom services. T-Mobile supplied some cell-site data to help agents

determine who had robbed one of its stores. We rejected an argument based on the Fourth Amendment, explaining:

Adkinson’s Fourth Amendment rights were ... not violated because Adkinson consented to T-Mobile collecting and sharing his cell-site information. A defendant can voluntarily consent in advance to a search as a condition of receiving contracted services. See *Medlock v. Trustees of Indiana Univ.*, 738 F.3d 867, 872 (7th Cir. 2013). As a condition of using a phone serviced by T-Mobile, Adkinson agreed to T-Mobile’s policy that T-Mobile could disclose information when reasonably necessary to protect its rights, interests, property, or safety, or that of others. And T-Mobile, in accordance with its policy, shared information with law enforcement after one of its stores was robbed at gunpoint.

916 F.3d at 610. Accord, *United States v. Young*, 350 F.3d 1302, 1308–09 (11th Cir. 2003) (enforcing a consent to search in a FedEx bill of lading). See also Orin S. Kerr, *Terms of Service and Fourth Amendment Rights*, 172 U. Pa. L. Rev. 287, 291–304 (2024) (collecting cases). We do not see a material difference between the sort of consent at issue in *Adkinson* and the sort on which Dropbox relied. T-Mobile’s language, like Dropbox’s, gave it an option to discover and reveal information, not an obligation to do so. *Adkinson* is incompatible with the approach taken in *Lowers*, *Maher*, and *Warshak*.

Those decisions ask whether a given consent “extinguishes all expectation of privacy” or something similar. The courts’ negative answer follows from this phrasing, because nothing short of an enforceable obligation to examine and reveal the contents of files to the world could “extinguish” all privacy in them. But that is not how consent works in the law of search and seizure. If a driver tells a police officer that the officer may open the car’s trunk, this does not extinguish all privacy in that space. Both privacy and property interests may be enforced against members of the driver’s family, or the

driver's neighbors, or other law enforcement agencies the next week. Still, the consent to search gives the recipient of that consent an option to act in particular ways. Blocker allowed Dropbox (but not Google or T-Mobile) to inspect his files, and to disclose appropriately in response. Action within the scope of such a consent does not require probable cause or a warrant. That's the point of our decision in *Adkinson*. No more does effective consent require universal disclosure.

Given *Adkinson*, Judge Lee's finding of consent to search cannot be set aside as clearly erroneous. Blocker wants us to reconsider *Adkinson*, but we are not inclined to do so. A conflict among the circuits would persist no matter what we did. *Chatrie v. United States*, No. 25–112 (argued Apr. 27, 2026), which grew out of a consent permitting Google to disclose location data that underlay a geofence warrant, is under advisement at the Supreme Court. The principal question in *Chatrie* is the validity of geofence warrants as a class, but consent may influence the Court's decision. If *Chatrie* does not address the validity of consents that permit but do not compel disclosures to public officials, the Supreme Court may eventually need to address the conflict between decisions such as *Adkinson* and *Young* on one side, and *Lowers*, *Maher*, and *Warshak* on the other. All we need do today is stand by *Adkinson*, which reflects how the law of contract is ordinarily understood when the terms are not unconscionable.

AFFIRMED