

APPENDICES

TABLE OF CONTENTS

Appendix A – Court of appeals decision	1a
Appendix B – District court suppression order	10a

1a

APPENDIX A

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 clearinghouse 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

APPENDIX B

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

	)	
UNITED STATES OF	)	
AMERICA,	)	
	)	
Plaintiff	)	
	)	No. 20 CR 704
v.	)	
	)	Judge John Z. Lee
ADAM BLOCKER,	)	
	)	
Defendant.	)	

ORDER

In October 2020, Defendant Adam Blocker was indicted on six counts related to the transportation, receipt, and possession of child pornography. He filed this motion to suppress evidence, arguing that the source of the investigation against him—the discovery of child pornography files in his personal Dropbox account—violated his Fourth Amendment rights. For the following reasons, his motion is denied.

I. Background¹**A. Blocker's Dropbox Account**

Dropbox is a company that provides cloud-based data storage for users around the world. *See* Def.'s

¹ The following facts are uncontroverted unless otherwise noted.

Mot. Suppress (“Def.’s Mot.”) at 7, ECF No. 73. On May 20, 2018, Blocker became one of those users when he made a storage account with Dropbox. *Id.* at 9.

As part of the sign-up process, Blocker agreed to Dropbox’s Terms of Service and its associated policies in their entirety. Def.’s Mot. at 9. Because Dropbox’s Terms of Service, its Privacy Policy, and Accepted Use Policy are central to this analysis, they are quoted extensively below.

Dropbox’s Terms of Service provided, in relevant part:

These terms of service (“Terms”) cover your use and access to our servers, client software and websites (“Services”). . . . Our Privacy Policy explains how we collect and use your information while our Acceptable Use Policy outlines your responsibilities when using our services. By using our Services, you’re agreeing to be bound by these Terms, our Privacy Policy, and Acceptable Use Policy.

...

Your Stuff & Your Permissions

When you use our Services, you provide us with things like your files, content, messages, contacts, and so on (“**Your Stuff**”). Your Stuff is yours. These Terms don’t give us any rights to Your Stuff except for the limited rights that enable us to offer the Services.

We need your permission to do things like hosting Your Stuff, backing it up, and sharing it when you ask us to. Our Services also provide you with features like photo thumbnails, document previews, commenting, easy sorting, editing, sharing, and searching.

These and other features may require our systems to access, store, and scan Your Stuff. You give us permission to do those things, and this permission extends to our affiliates and trusted third parties we work with.

...

Your Responsibilities

You're responsible for your conduct. Your stuff and you must comply with our Acceptable Use Policy. . . . We may review your conduct and content for compliance with these Terms and our Acceptable Use Policy. With that said, we have no obligation to do so. We aren't responsible for the content people post and share via the Services.

...

You may use our Services only as permitted by applicable law, including export control laws and regulations.

Def.'s Mot. Ex. E, Dropbox's 2018 Terms of Service ("Terms") at 2, ECF No. 72-6 (bolding in original).

The phrases "Privacy Policy" and "Acceptable Use Policy" were hyperlinked each time they were used and connected the user to the Privacy Policy and the Acceptable Use Policy, respectively.

At the time Blocker signed up for Dropbox, its Privacy Policy stated in pertinent part:

Dropbox Privacy Policy

...

Here we describe how we collect, use, and handle your personal information when you

use our websites, software and services (“Services”).

...

What & Why

We collect and use the following information to provide, improve, and protect our Services:

...

Your Stuff. Our Services are designed to make it simple for you to store your files, documents, photos, comments, messages, and so on (“Your Stuff”), collaborate with others, and work across multiple devices. To make that possible, we store, process, and transmit Your Stuff as well as information related to it. This related information includes your profile information that makes it easier to collaborate and share Your Stuff with others, as well as things like the size of the file, the time it was uploaded, collaborators, and usage activity. Our Services provide you with different options for sharing Your Stuff.

...

With Whom

We may share information as discussed below, but we won’t sell it to advertisers or third parties.

...

Law & Order and the Public Interest. 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 users; (d) protect Dropbox's rights, property, safety, or interest; (e) perform a task carried out in the public interest.

Stewardship of your data is critical to us and a responsibility that we embrace. We believe that your data should receive the same legal protections regardless of whether it's stored on our Services or on your home computer's hard drive. We'll abide by the following Government Request Principles when receiving, scrutinizing, and responding to government requests (including national security requests) for your data:

- Be transparent,
- Fight blanket requests,
- Protect all users, and
- Provide trusted services[.]

Gov't Resp. Opp'n Def.'s Mot. Suppress ("Gov't Resp."), Ex. C, Dropbox Privacy Policy ("Privacy Policy") at 1–2, ECF No. 80-3 (bold and italics in original).

Furthermore, at the time that Blocker registered with Dropbox, its Acceptable Use Policy stated:

Dropbox Acceptable Use Policy

...

You agree not to misuse the Dropbox Services ("Services") or help anyone else to do so. For example, you must not even try to do any of the following in connection with the Services:

...

- Publish or share materials that are unlawfully pornographic or indecent, or that contain extreme acts of violence

...

- Violate the law in any way, including storing, publishing or sharing material that's fraudulent, defamatory, or misleading[.]

Gov't Resp., Ex. B, Dropbox Acceptable Use Policy ("Use Policy") at 2, ECF No. 80-2 (bold in original).

B. Dropbox's Review of Blocker's Files

Sometime after Blocker signed up for this account and began storing his files with Dropbox, Dropbox used a software called PhotoDNA to scan the files in Blocker's account for child pornography.² *Id.* at 10. When PhotoDNA detected suspected child pornography in several of Blocker's image files, a Dropbox employee manually reviewed those files, as well as the videos on Blocker's account. *Id.* Based on this review, Dropbox reported its findings to the National Center for Missing and Exploited Children ("NCMEC").³ *Id.*

² PhotoDNA is designed to automatically match the digital characteristics of unknown photo files to the characteristics of known child pornography files. Def.'s Mot. at 6. Blocker contends that it is an imperfect system—that false positives are both possible and documented. *Id.* at 7. For the purposes of this motion, the Court assumes that he is correct and that PhotoDNA has a non-zero error rate.

³ NCMEC is an organization created by Congress to act as a clearinghouse for reports of child pornography. Def.'s Mot. at 5. NCMEC also sublicenses the PhotoDNA software, including to

NCMEC viewed each file, added to the investigation with some of its own research, and sent the report to the FBI. *Id.* at 10–11. The FBI, in turn, viewed each photograph and video to determine whether it constituted child pornography and used this information to obtain two warrants: one for the entirety of Blocker’s Dropbox account and one for his residence. *Id.* at 11. No other information was included in the warrant affidavits. *Id.* See also Def’s Mot., Ex G, Search Warrant Application for Def.’s Home, ECF No. 72-8 and Mot., Ex H, Search Warrant Application for Def.’s Dropbox Account, ECF No. 72-9.

Ultimately, the warrants were issued and executed, and the information obtained under those warrants resulted in the charges against Blocker in this case. Def’s Mot at 11. He now moves to suppress the evidence obtained pursuant to both warrants, arguing that the warrantless reviews of files from his Dropbox account violated his Fourth Amendment rights, and any further evidence constitutes fruit of the poisonous tree.

II. Legal Standard

“Two lines of precedent govern whether officer conduct amounts to a search”: a property-based approach, and a privacy-based approach. *United States v. Lewis*, 38 F.4th 527, 533 (7th Cir. 2022). The

Dropbox. *Id.* at 6. All Internet Service Providers, like Dropbox, who become aware of child pornography are required to report it to NCMEC through a “CyberTipline” program. *Id.* From there, NCMEC reviews the reports and funnels them to the appropriate law enforcement agency. *Id.* Blocker argues that NCMEC’s “substantial budget [and] . . . wide variety of law enforcement powers and responsibilities,” *id.* at 6, make it a government actor for the purposes of the Fourth Amendment. For the sake of argument, the Court also assumes that this is true throughout this order.

former, the property-based approach, is implicated “when an officer enters a constitutionally protected area, such as the home, for the purpose of gathering evidence against the property owner.” *Id.* This line of precedent derives from the common law of trespass. *See United States v. Jones*, 565 U.S. 400, 405 (2012).

The latter test considers whether the defendant had a reasonable expectation of privacy in the place where the evidence was discovered. *Lewis*, 38 F.4th at 534. This is a two-part inquiry: First, the Court asks whether the defendant subjectively exhibited an expectation of privacy in the circumstances at issue; second, it determines whether “the expectation [is] one that society is prepared to recognize as ‘reasonable.’” *Id.* (quoting *Katz v. United States*, 389 U.S. 347, 361 (1964) (Harlan, J., concurring)). But the fact that conduct amounts to a search alone does not make it unconstitutional. Rather, “the Fourth Amendment proscribes searches and seizures only when they are unreasonable.” *United States v. Jackson*, 598 F.3d 340, 346 (7th Cir. 2010).

III. Analysis

Blocker first argues that NCMEC’s particular role in the enforcement of child pornography laws and its creation and funding by Congress together make it a government actor. Next, Blocker contends that NCMEC’s contract with Dropbox for use of the PhotoDNA software makes *Dropbox* a government actor. *See id.* And, because Dropbox did not have a warrant when it scanned and reviewed his files, Blocker reasons, these actions constituted a warrantless search that violated his constitutional rights.

In support of his motion, Blocker advances both privacy- and property-based arguments for why

Dropbox’s review of his files with PhotoDNA software was a search. His principal argument is that he had a reasonable expectation of privacy in his Dropbox account, which Dropbox violated when it used PhotoDNA to scan his file and disclose their contents to NCMEC. In the alternative, Blocker argues that Dropbox violated his property interest by reviewing the files, which belonged to him under the Terms of Use. He compares this to the “physical[] occup[ation] [of] private property for the purpose of obtaining information” that constituted a Fourth Amendment violation in *Jones*. 565 U.S. at 404.

Blocker’s motion raises a number of important (and sometimes befuddling) questions about the application of the Fourth Amendment’s safeguard against warrantless searches and seizures in a digital age. For example, was NCMEC a government actor when it reviewed the Dropbox files? Some courts certainly have concluded so under similar circumstances, while others have disagreed. *See United States v. Ackerman*, 831 F.3d 1292, 1302 (10th Cir. 2016) (Gorsuch, J); *but see United States v. Meals*, 21 F.4th 903, 908 (5th Cir. 2021) (stating that “[c]ontrary to Meals’s supposition, NCMEC is a private, nonprofit corporation, not a government entity”).

Furthermore, if NCMEC is a government actor, does NCMEC’s contract with Dropbox turn Dropbox into a government actor? And, if we assume that Dropbox was a government actor, did its use of PhotoDNA to scan Blocker’s Dropbox folder constitute a trespass onto Blocker’s property? Justice Gorsuch, while he was on Tenth Circuit, observed that the warrantless opening of a person’s digital files may be “exactly the type of trespass to chattels that the framers sought to prevent when they adopted the

Fourth Amendment.” *Ackerman*, 831 F.3d at 1307 (Gorsuch, J.).

This, of course, raises the additional question of whether Blocker can claim a property interest in his Dropbox “account” (as opposed to the photographic files that he kept in his Dropbox account, which Dropbox would refer to as “His Stuff.”). And what if Blocker had created separate file folders in his Dropbox account, named them “Private,” and put the photographic files in them? Could he claim a property interest in these “Private” folders he created? And, as to the photographs themselves, would the fact that Dropbox took those files and gave them to NCMEC constitute a seizure under the Fourth Amendment? These are just examples of some of the questions raised by Blocker in his motion.

Whatever the answers those questions may be, however, the Court need not try to divine them here because the Court finds that, by agreeing to Dropbox’s terms of service, Blocker consented to Dropbox’s search of his files. After all, it is well-settled law that, while a warrantless search is generally per se unreasonable, and therefore unconstitutional, no warrant is required if the defendant consents to the search. *United States v. Jones*, 22 F.4th 667, 675 (7th Cir. 2022). And “[a] defendant can voluntarily consent in advance to a search as a condition of receiving contracted services.” *United States v. Adkinson*, 916 F.3d 605, 610 (7th Cir. 2019). That is exactly what happened here.

In agreeing to Dropbox’s terms and conditions, Blocker gave consent to have his files searched for illegal pornographic content. “The scope of consent is assessed under an objective reasonableness standard that asks what a typical reasonable person would have understood to be within the scope.” *Jones*, 22

F.4th at 678 (cleaned up). And a review of Dropbox’s Terms, its Privacy Policy, and its Acceptable Use Policy would put a reasonable person on notice that their files would be searched for illegal content and that the results of that search could be turned over to third parties, including the government.

At the outset, Dropbox’s Terms of Service emphasize that Dropbox “may review your conduct and content for compliance with these Terms and our Acceptable Use Policy.” Terms at 2. A user need look no further than the Privacy Policy’s “Law & Order” section to see that such a review could result in disclosure of files to law enforcement. In fact, the Privacy Policy clearly states that Dropbox “may disclose your information to third parties if [it] determine[s] that such disclosure is reasonably necessary to: (a) comply with *any applicable law*, regulation, legal process, or *appropriate government request*.” Privacy Policy at 1 (emphasis added). And it is clear that laws regulating child pornography are the type of laws this policy contemplates. As the Acceptable Use Policy explains, a user “must not even try to . . . [p]ublish or share materials that are unlawfully pornographic.” Use Policy at 2.

These documents would put a reasonable person on notice that, by using a Dropbox account, he was acquiescing to a search of his files, which might result in discovery of any illegal pornographic content they contained. *See, e.g., Adkinson*, 916 F.3d at 610 (holding that *ex ante* consent to disclosure of location data to a wireless carrier, which stated that it might disclose that location data to a third party, eliminated any Fourth Amendment search claim as to that data); *United States v. Bohannon*, No. 19-CR-00039-CRB-1, 2020 WL 7319430 (N.D. Cal. Dec. 11, 2020) (finding that a PhotoDNA search by Microsoft of a defendant’s

OneDrive account did not implicate the Fourth Amendment because similarly specific warnings in Microsoft’s terms and conditions reflected the defendant’s consent to Microsoft’s review of his files); *State v. Pauli*, No. A19-1886, 2020 WL 7019328, at *3 (Minn. Ct. App. Nov. 30, 2020), *review granted* (Feb. 24, 2021) (finding that Dropbox’s Terms constituted “clear and unambiguous warnings that such content violated Dropbox’s policies; that Dropbox could review [a defendant]’s conduct and content for compliance; and that Dropbox could report his content to law enforcement”).

For his part, Blocker argues⁴ that Dropbox’s Terms of Use were not definite enough for his agreement to constitute consent. In particular, he points out that the Terms state that Dropbox *may* search his files and did not say it had an affirmative obligation to do so. There is support in other circuits for this view, *see United States v. Warshak*, 631 F.3d 266, 287 (6th Cir. 2010) (finding that where the likelihood of an internet service provider reviewing emails is low, a subscriber maintains a reasonable expectation of privacy with respect to those emails). But the Court finds this line of reasoning unpersuasive here, in light of existing Seventh Circuit precedent.

Indeed, in *Adkinson*, the Seventh Circuit found that a defendant had consented *ex ante* to the disclosure of his location data by T-Mobile because his user agreement stated that “T-Mobile *could* disclose information when reasonably necessary to protect its

⁴ Blocker primarily directs this argument at whether he has a reasonable expectation of privacy in his Dropbox account, but for the sake of completeness, the Court considers it with respect to the consent analysis, as well.

rights, interests, property, or safety, or that of others.” 916 F.3d at 610 (emphasis added). In other words, what matters here is not how likely Blocker thought it might be that Dropbox would search his files, but rather how definite the scope of the consent that Blocker gave to Dropbox was. *Cf. United States v. Irving*, 347 F. Supp. 3d 615, 623 (D. Kan. 2018) (finding that the defendant maintained a reasonable expectation of privacy in Facebook messages because “Facebook’s [Terms of Service] d[id] not have explicit terms about monitoring user’s accounts for illegal activities and reporting those activities to law enforcement”). Accordingly, because Blocker consented in advance to the specific type of review and disclosure of his files that Dropbox conducted in this instance, he has no Fourth Amendment claim. *See Adkinson*, 916 F.3d at 610.

IV. Conclusion

For the foregoing reasons, Blocker’s motion to suppress is denied.

IT IS SO ORDERED.

ENTERED: 7/28/22

[handwritten signature]

John Z. Lee

**United States District
Judge**