COURT OF APPEALS FOR THE FIRST DISTRICT OF TEXAS

# Robert Aaron Rosales v. The State of Texas

Rosales v. State · No. 01-23-00876-CR; 01-23-00877-CR · Decided November 25, 2025

## OPINION

Robert Aaron Rosales v. the State of Texas

PER CURIAM.

Opinion issued November 25, 2025 In The Court of Appeals For The First District of Texas

NOS. 01-23-00876-CR

01-23-00877-CR ROBERT AARON ROSALES, Appellant V. THE STATE OF TEXAS, Appellee On Appeal from the 351st District Court Harris County, Texas Trial Court Case Nos. 1682769 & 1682770

O P I N I O N1

1 A prior panel of the Court previously issued an opinion in this case, but the Court withdrew that opinion. The Court, with a new panel, now issues this new opinion in its stead. The Fourth Amendment of the United States Constitution guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" by the government. U.S. CONST. amend. IV. Fourth Amendment protections generally do not extend to the conduct of private persons who are not acting as government agents. That private search doctrine decides this case. Robert Rosales uploaded several digital files containing child pornography to Dropbox, a cloud storage and file-sharing company. Dropbox discovered these files and submitted a cyber tip to the National Center for Missing and Exploited Children (NCMEC). NCMEC, in turn, notified local law enforcement. Law enforcement later obtained a warrant to search the entirety of Rosales's Dropbox account. After being charged in multiple cases with possessing child pornography, Rosales moved to suppress the evidence. The trial court denied his motion, and Rosales pled guilty to two charges of possession of child pornography.2 On appeal, Rosales makes three arguments as to why, he says, the trial court erred in denying his motion to suppress. None supports reversal. First, Rosales argues that Dropbox was a government agent, and therefore the company's review of his files constituted an unlawful search under the Fourth 2 See TEX. PENAL CODE § 43.26. Rosales originally faced five charges, but he pled guilty in exchange for the dismissal of three charges; this appeal concerns the two charges to which he pled guilty. 2 Amendment.3 Applying the law to this record, however, Dropbox was a private party. Its review of the files fell under the private search doctrine and caused no Fourth Amendment intrusion. Second, Rosales argues that even if Dropbox was a private party, the police's pre-warrant review exceeded the scope of Dropbox's review, in violation of the Fourth Amendment. But this record shows the opposite; Dropbox viewed the "entire contents" of each

file at issue, and the police (pre-warrant) viewed only those files that Dropbox had already viewed. Finally, Rosales argues that the trial court erred in finding that probable cause supported the ultimate issuance of a search warrant for the entirety of Rosales's Dropbox account. He emphasizes three statements that the trial court excised from the warrant affidavit under Franks v. Delaware, 438 U.S. 154 (1978), and he argues that, without them, there was no probable cause. But probable cause still existed without those statements. We affirm the judgments of the trial court. 3 Rosales's arguments focus on the Fourth Amendment to the United States Constitution. Because he does not separately brief an argument under the Texas Constitution, we focus our analysis on the United States Constitution's Fourth Amendment. See TEX. R. APP. P. 38.1(i); Young v. State, 563 S.W.3d 325, 329 n.3 (Tex. App.—Houston [1st Dist.] 2018, pet. ref'd). 3

BACKGROUND

A. The Cyber Tip In May 2019, Dropbox submitted a "cyber tip" to NCMEC that it had identified apparent child pornography on one of its user's accounts. 4 The cyber tip provided identifying information for the account holder, including his screen/user name ("Robert Rosales"), his email address, and his user ID. The cyber tip also identified two IP addresses associated with that user's account: one used to log in to the account in January 2019 and the other in May 2019. The cyber tip included nine different files (four images, four videos, and an upload log). The tip stated that Dropbox "view[ed] [the] entire contents" of each uploaded file. After receiving the cyber tip, a NCMEC analyst viewed the uploaded files and observed apparent child pornography. NCMEC generated geolocation data for the reported user and found that the IP addresses associated with the user's account were in Houston, Texas, and the internet provider was Comcast. Based on the location data, NCMEC sent its report to the Houston Police Department (HPD). 4 The parties do not dispute that Dropbox is an "electronic communication service provider," or ESP, and was therefore required by federal law to report child pornography to NCMEC. See United States v. Miller, 982 F.3d 412, 419 (6th Cir. 2020) (citing 18 U.S.C. §§ 2258A(a), 2258E(6)). 4 HPD then subpoenaed Comcast to produce the subscriber's records for the IP addresses that Dropbox included in its cyber tip. Comcast indicated that it did not have subscriber information for the January 2019 IP address. But Comcast did have subscriber information for the May 2019 IP address; this information led to Rosales. B. The Search Warrant Affidavit On September 6, 2019, HPD Officer M. Wilson obtained a search warrant for the electronic customer data in Rosales's Dropbox account. In his warrant affidavit, which is discussed in more detail below, Officer Wilson averred he had reason to believe evidence "of the offenses of Possession and/or Promotion of Child Pornography" would be found in Rosales's Dropbox account. He detailed the history of the cyber tip and his basis for probable cause. Rosales later argued—and the trial court agreed—that three statements in the warrant affidavit were false and needed to be excised under Franks v. Delaware, 438 U.S. 154 (1978).5 The trial court found that the remaining statements still provided probable cause. 5 The statements concerned the following: (1) the affidavit included two IP addresses for Rosales's Houston service address, when only one of the two was actually connected

to that address, (2) the affidavit said both that Officer Wilson expected Dropbox to preserve the data and that he sent a preservation notice—when Officer Wilson clarified that he did not send a notice but rather expected Dropbox to preserve the data; and (3) the affidavit listed the date Dropbox sent its cyber tip as the date Rosales uploaded the files. 5 After the warrant issued, Dropbox provided approximately 200 media files, some of which reportedly contained images and videos of child pornography. C. Motion to Suppress Hearing Rosales filed a motion to suppress, raising the arguments addressed herein.6 During the hearing, Rosales introduced seven exhibits, including certain agreements between NCMEC and Dropbox. Officer Wilson was the only witness to testify. Officer Wilson testified that he was trained in investigating internet crimes against children and NCMEC cyber tips. He stated that, on July 27, 2019, he received the cyber tip from NCMEC, which in turn had been reported by Dropbox. He stated that Dropbox provided Rosales's username, email address, user ID, and IP addresses, as well as the hash values for the files in its cyber tip. Officer Wilson testified that Dropbox had viewed the files in question before submitting the cyber tip to NCMEC. NCMEC then sent the cyber tip report and files to HPD. Officer Wilson explained that, after receiving NCMEC's report, he viewed the files and confirmed that they showed child pornography. He also testified that he did not look at anything beyond what Dropbox had viewed and provided to NCMEC. He then prepared a warrant affidavit and received a search warrant for Rosales's Dropbox account. 6 Rosales also argued that Dropbox violated criminal laws when it viewed his files. See TEX. CODE CRIM. PROC. art 38.23(a). Rosales does not assert that argument here. 6 Officer Wilson testified that he had no communication with Dropbox or NCMEC and was unaware of any communications between Dropbox and any member of HPD. He stated that, in his experience, ESPs like Dropbox generally conduct these reviews on their own because they do not "want child pornography stored on their servers." He further testified that he had no knowledge of any contractual agreements between NCMEC and Dropbox. D. Findings of Fact and Conclusions of Law The trial court denied the motion to suppress and entered findings of fact and conclusions of law in support of its ruling. Among other things, the trial court determined that Dropbox was a private party that was not acting as an instrument or agent of the government when it identified and reported the files to NCMEC. The trial court also determined that Dropbox viewed each file before sharing the files with NCMEC, and that neither Officer Wilson nor NCMEC exceeded the scope of Dropbox's private search. Further, as noted, the trial court determined that three affidavit statements should be excised as false. But the trial court determined that, even after excising those statements, the affidavit still provided probable cause. 7

DISCUSSION

We first address whether Dropbox was a private entity or agent of the government. We then address the scope of Officer Wilson's initial review of the files. And finally, we address the affidavit supporting the warrant. Standard of Review We review a trial court's ruling on a motion to suppress under a bifurcated standard of review. State v. Pettit, 713 S.W.3d 834, 839 (Tex. Crim.

App. 2025). We afford almost total deference to a trial court's determination of historical facts. Id. In a suppression hearing, the trial court is the sole trier of fact and judge of the credibility of the witnesses and the weight to be given their testimony. Valtierra v. State, 310 S.W.3d 442, 447 (Tex. Crim. App. 2010). If the trial court makes express findings of fact, we view the evidence in the light most favorable to its ruling and determine whether the evidence supports those factual findings. Id. We review a trial court's application of the law to the facts de novo. See Pettit, 713 S.W.3d at 839; Valtierra, 310 S.W.3d at 447. We sustain the ruling if it is reasonably supported by the record and is correct on any theory of law applicable to the case. State v. Ruiz, 577 S.W.3d 543, 545 (Tex. Crim. App. 2019). 8 Analysis A. The pre-warrant actions present no Fourth Amendment violation: Dropbox was a private party, and the government did not exceed the scope of Dropbox's private review. The pre-warrant actions in this record present no Fourth Amendment violation. A search that implicates the Fourth Amendment may occur when the government obtains information either by physically intruding upon a constitutionally protected area (the property-based approach) or by infringing on a person's reasonable expectation of privacy. See State v. Huse, 491 S.W.3d 833, 840 (Tex. Crim. App. 2016). Rosales focuses on his asserted reasonable expectation of privacy.7 7 As an initial matter, the State argues on appeal that Rosales cannot assert his challenge because he did not have a reasonable expectation of privacy in these files. A defendant may challenge a search as unconstitutional on privacy grounds "if
(1) he has a subjective expectation of privacy in the place or object searched, and
(2) society recognizes that expectation as reasonable or legitimate." Pettit, 713
S.W.3d at 839. This doctrine is not jurisdictional; it is part of the Fourth Amendment analysis. See Wells v. State, 714 S.W.3d 614, 620 n.9 (Tex. Crim. App. 2025) ("Because Fourth Amendment standing is subsumed under substantive Fourth Amendment doctrine, it is not a jurisdictional question . . . ." (quoting Byrd v. United States, 584 U.S. 395, 411 (2018))). Unfortunately, the record is not developed on Rosales's privacy expectations. For instance, the record does not show what Dropbox terms of service were in effect when Rosales joined Dropbox, to what Rosales might have agreed, or if the applicable agreement is in the record. For purposes of this appeal, we assume without deciding that Rosales had a legitimate expectation of privacy in the files— and thus that he can assert his challenges, which fail on the merits regardless. See United States v. Reddick, 900 F.3d 636, 638 n.1 (5th Cir. 2018) (assuming without deciding that defendant had legitimate expectation of privacy in digital files containing child pornography that were uploaded to cloud hosting service and sent 9 The Fourth Amendment protects only against the government's unreasonable searches and seizures—not those of private parties. See Ruiz, 577 S.W.3d at 546; see also Burdeau v. McDowell, 256 U.S. 465, 475 (1921). Under the private search doctrine, even "a wrongful search or seizure conducted by a private party does not violate the Fourth Amendment and [ ] such private wrongdoing does not deprive the government of the right to use evidence that it has acquired lawfully." Ruiz, 577 S.W.3d at 546 (quoting Walter v. United States, 447 U.S. 649, 656 (1980)). In a seminal case on this doctrine, discussing expectations of privacy,

the United States Supreme Court stated that: “Once frustration of the original expectation of privacy occurs” by a private party, “the Fourth Amendment does not prohibit governmental use of the now-nonprivate information.” United States v. Jacobsen, 466 U.S. 109, 117 (1984) (emphasis added). This concept is somewhat similar to the plain view doctrine—under which no Fourth Amendment intrusion occurs if an officer is legitimately somewhere and then sees contraband.8 So too here. If a private party “violates a person’s privacy, finds evidence of a crime, and turns over the evidence to the government, the evidence to NCMEC; ESP user agreement was “not in the record”); Miller, 982 F.3d at 426– 27 (assuming defendant had reasonable expectation of privacy in emails). 8 See, e.g., State v. Dobbs, 323 S.W.3d 184, 187–88 (Tex. Crim. App. 2010). 10 can be used to obtain warrants or to prosecute.” United States v. Meals, 21 F.4th 903, 906 (5th Cir. 2021). Applying this doctrine, for example, our Court has concluded that the Fourth Amendment was not implicated by a private search conducted by a computer technician who discovered files containing child pornography on the defendant’s computer that the defendant left at an electronics store for repair. Brackens v. State, 312 S.W.3d 831, 837 (Tex. App.—Houston [1st Dist.] 2009, pet. ref’d); see also State v. Rodriguez, 521 S.W.3d 1, 10–11 (Tex. Crim. App. 2017) (offering examples). There are two instances in which the private search doctrine would not apply in a case like this one. First, the doctrine does not apply if the private party was acting as an agent or instrument of the government. See Meals, 21 F.4th at 906. As precedent explains, a private party cannot violate the Fourth Amendment unless they are “acting under the control of, or at the behest of, law enforcement.” Cobb v. State, 85 S.W.3d 258, 270–71 (Tex. Crim. App. 2002); Ruiz, 577 S.W.3d at 547 (“We reaffirm that the Fourth Amendment is a restraint on government and that it does not apply to private individuals who are acting as such.”); see also Skinner v. Ry. Labor Execs.’ Ass’n, 489 U.S. 602, 614 (1989) (“Although the Fourth Amendment does not apply to a search or seizure, even an arbitrary one, effected by a private party on 11 his own initiative, the Amendment protects against such intrusions if the private party acted as an instrument or agent of the Government.”). Second, the doctrine does not enable the government to exceed the scope of the private search without a warrant or other lawful authority to make its own search. Jacobsen, 466 U.S. at 115, 122; see Brackens, 312 S.W.3d at 837 (“[A]ny subsequent law enforcement search must be limited in scope to the private party’s . . . .”). If, without a warrant, the government exceeds the scope of the private review and “discovers new evidence that it was not substantially certain to discover, the private search doctrine does not apply to the new evidence, and the new evidence may be suppressed.” Meals, 21 F.4th at 906–07. The private search doctrine applies in this case.

1. Rosales did not show that Dropbox acted as a government agent

when it reviewed Rosales’s files. a. Dropbox was a private party. Rosales contends that Dropbox acted as an agent or instrument of the government when it reviewed his files. He argues that Dropbox was acting in coordination with NCMEC, which he contends is “a government agency.” See United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016). Thus, Rosales argues that

Dropbox was required to obtain a warrant before reviewing his account, and its 12 failure to do so renders the fruits of its search inadmissible. But even assuming for these purposes that NCMEC is a government agency,9 on this record, we disagree. Under binding precedent, to determine whether a party is acting on behalf of law enforcement, we look to the following factors:

(1) whether the government knew of, and acquiesced in, the intrusive
conduct, and

(2) whether the party performing the search intended to assist law
enforcement efforts or, instead, to further his own ends. Burwell v. State, 576 S.W.3d 826, 831 (Tex. App.—Houston [1st Dist.] 2019, pet ref'd) (citing Dawson v. State, 106 S.W.3d 388, 392 (Tex. App.—Houston [1st Dist.] 2003, no pet.)).10 We conduct our analysis of this question on a case-by-case basis 9 Our Court confronted a similar argument in Burwell v. State—involving Adobe Systems reporting child pornography to NCMEC—and determined that we did not need to decide NCMEC's status because, "[r]egardless of whether NCMEC was acting as a governmental agency," there was "no evidence that Adobe acted as an agent of either NCMEC, the HPD, or any other governmental entity." 576 S.W.3d 826, 831 (Tex. App.—Houston [1st Dist.] 2019, pet. ref'd). The same is true here. 10 The Court of Criminal Appeals explained this test in Stoker v. State, 788 S.W.2d 1, 11 (Tex. Crim. App. 1989), abrogated in part on other grounds by Horton v. California, 496 U.S. 128 (1990). Both at the time of Stoker and today, to "know" means "to perceive directly: have direct cognition of," or "to have understanding of." Know, WEBSTER'S NEW COLLEGIATE DICTIONARY (1981 ed.); see Know, MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY (11th ed. 2020) (same). "Acquiesce" means "to accept or comply tacitly or passively." Acquiesce, WEBSTER'S NEW COLLEGIATE DICTIONARY (1981 ed.); see Acquiesce, MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY (11th ed. 2020) (similar). The formulation of this test is not before us. 13 in light of all the circumstances. Id. at 831–32. Both factors must be present to convert a private search into a search by a government agent. Id. at 831. Our Court has previously concluded that the "defendant bears the burden of proving that a private party acted as an agent of the government." Id. at 832 (quoting Dawson, 106 S.W.3d at 392). That question is thus settled by precedent here. In Burwell, we found both factors absent—and that the defendant failed to carry his burden on this point—where there was no evidence that either NCMEC or anyone in law enforcement encouraged, "knew of or acquiesced in Adobe's search of [defendant's] files," nor did the record contain anything indicating that Adobe intended to assist law enforcement efforts. Id. There was no evidence that Adobe "acted out of anything other than its own business interests in complying with the law and maintaining the integrity of its services as set out in its Terms of Use." Id. The Sixth Circuit reached a similar conclusion in United States v. Miller, rejecting an argument that Google was a government agent when it detected images of child pornography in the defendant's email and reported them to NCMEC. 982 F.3d 412, 420, 423 (6th Cir. 2020). In concluding that Google was not a government agent, the court determined that Google "sought to rid its virtual spaces of criminal activity for the

same reason that shopkeepers have sought to rid their physical spaces of criminal activity: to protect their businesses." Id. at 425. The court also rejected 14 an argument that the government had "acquiesced" in Google's search; "[p]olice got involved only after Google had performed that scan and uncovered the crime." Id. Similar reasoning applies here. Like in Burwell, Rosales did not carry his burden to show that Dropbox "acted out of anything other than its own business interests in complying with the law and maintaining the integrity of its services." See Burwell, 576 S.W.3d at 832. Officer Wilson testified that, in his experience, ESPs like Dropbox generally conduct these searches on their own because they do not "want child pornography stored on their servers." Consistent with this, Dropbox's terms of service and privacy agreements state that:11 • Dropbox users must not "publish, share, or store materials that constitute child sexually exploitative material" and Dropbox "reserve[s] the right to take appropriate action in response to violations of this policy." • Dropbox will "collect and use personal data for our legitimate business needs," and it uses third parties "for the business purpose of helping us provide, improve, and promote our Services." • Dropbox deploys "automated technologies to detect abusive behavior and content that may harm our Services, you, or other users." • Dropbox will disclose user information to third parties to "comply with any applicable law, regulation, legal process, or appropriate government request," to prevent "abuse of Dropbox or our users," or to "protect Dropbox's rights, property, safety, or interest." 11 These terms appear in Dropbox's 2022 agreements, which are in the record. Although the record is not clear which version of the agreements was in effect when Rosales joined Dropbox (and it is not clear to what Rosales might have agreed), Dropbox's inclusion of these terms in the 2022 agreements may serve as evidence of Dropbox's intent during the relevant period. 15 The fact that Dropbox's business interests may intersect with the government's interests in investigating criminal activity does not turn Dropbox into a government agent. See, e.g., United States v. Ringland, 966 F.3d 731, 736 (8th Cir. 2020) ("Google did not become a government agent merely because it had a mutual interest in eradicating child pornography from its platform."). Moreover, in determining that Rosales failed to establish that Dropbox was acting as an instrument or agent of the government, the trial court found that "Dropbox identified the files from Rosales' account as suspected child pornography before sharing them with NCMEC and [the] Houston Police Department." We give deference to the trial court's findings of fact. See Valtierra, 310 S.W.3d at 447. The trial court also found that Rosales did not prove that Dropbox actually used NCMEC's (Microsoft's) software to search his account. Additionally, Officer Wilson testified that he had no communication with Dropbox or NCMEC and was unaware of any communications between Dropbox and any member of HPD. Congress has expressly stated that ESPs—such as Dropbox—need not affirmatively search for child pornography (the law simply requires that they report child pornography when they find it). See 18 U.S.C. § 2258A(f)(3) ("Nothing in this section shall be construed to require a provider to . . . affirmatively search, screen, or scan for facts or circumstances described in sections (a) and (b)."). And—as 16 discussed in detail below—none of the agreements between Dropbox and

NCMEC here show that Dropbox acted as an agent of the government. In sum, this record does not show both that (1) Dropbox intended to assist law enforcement, and (2) NCMEC knew of and acquiesced in Dropbox's search, rather than just generally providing a tool for Dropbox to use when it chose to do so. Yet both elements are required for Rosales to prevail. See Burwell, 576 S.W.3d at 831. In so holding, we join (and are persuaded by) the courts across the country that have found in similar circumstances that ESPs, including Dropbox, are not government agents when reporting child pornography to NCMEC. See, e.g., United States v. Guard, 152 F.4th 375, 389–90 (2d Cir. 2025) (mobile app Kik is not a government agent); United States v. Rosenschein, 136 F.4th 1247, 1254–56 (10th Cir. 2025) (same for Microsoft and Chatstep); United States v. Sykes, 65 F.4th 867, 876–77 (6th Cir. 2023) (same for Facebook); United States v. Rosenow, 50 F.4th 715, 731–35 (9th Cir. 2022) (same for Yahoo and Facebook); Meals, 21 F.4th at 907–08 (same for Facebook); United States v. Bebris, 4 F.4th 551, 562 (7th Cir. 2021) (same for Facebook).12 12 See also, e.g., Ringland, 966 F.3d at 736 (Google); United States v. Stevenson, 727 F.3d 826, 830 (8th Cir. 2013) (AOL); United States v. Cameron, 699 F.3d 621, 636– 38 (1st Cir. 2012) (Yahoo); United States v. Richardson, 607 F.3d 357, 364–67 (4th Cir. 2010) (AOL); United States v. Ambrose, No. 23-CR-13-KKM-CPT, 2025 WL 3153495, at *6–8 (M.D. Fla. Nov. 12, 2025) (Snapchat and Instagram); United States v. Orne, No. 2:21-CR-133-JDL, 2022 WL 1997216, at *3 n.2 (D. Me. June 6, 2022) (Dropbox). 17 b. The agreements between Dropbox and NCMEC do not change this conclusion. Rosales argues that this case is different from Burwell and the many others cited above because of the agreements in the record between NCMEC and Dropbox. Rosales asserts that these agreements transformed Dropbox into a government agent. They did not. One such agreement is a sublicense agreement, which states that Microsoft developed PhotoDNA and licensed it to NCMEC. NCMEC, in turn, agreed to sublicense it to Dropbox for use in identifying child pornography on its servers. Others are agreements allowing Dropbox to access a hash-sharing database between various "nonprofit organizations worldwide" and "industry companies" in sharing hash values for known child pornography. The last (on which Rosales focuses) is a "Memorandum of Understanding" (MOU) allowing Dropbox to access NCMEC's electronic list of hash signatures called "NCMEC PhotoDNA Signatures," and agreeing generally that Dropbox will use NCMEC's signatures, in conjunction with PhotoDNA, in an attempt to identify apparent child pornography on its servers. Specifically, Rosales focuses on the following language from the MOU: NCMEC agrees to give Dropbox a non-exclusive, non-transferrable, royalty-free right and license to use the NCMEC PhotoDNA Signatures as contemplated in this Agreement. **** 18 Dropbox is a cloud storage and sharing company that has agreed to receive PhotoDNA Signatures from NCMEC and to use the PhotoDNA Signatures in connection with the PhotoDNA sublicensed from NCMEC to attempt to identify Apparent Child Pornography on its servers. **** Dropbox . . . will use the NCMEC PhotoDNA signatures, in conjunction with the PhotoDNA, in an attempt to identify Apparent Child Pornography on its servers. Rosales relatedly argues that Dropbox agreed to report its progress in using PhotoDNA

and the signatures to NCMEC “no less than semi-annually.” And he argues that NCMEC reports to Dropbox about arrests resulting from submitted cyber tips. Viewed as a whole, however, the agreements (and record) do not show the government both knew of and acquiesced in Dropbox’s review of Rosales’s account for child pornography. None of the agreements says how often or when Dropbox would use the technology at issue, where or what it would review, or otherwise sets parameters as to what Dropbox would do with the technology. (Moreover, as noted above, the trial court found that Rosales did not prove that Dropbox actually even used NCMEC’s (Microsoft’s) software to search his account here). And critically, even if we were to assume the knowledge and acquiescence element, none of these agreements offers evidence that Dropbox acted on NCMEC’s behalf to assist NCMEC. 19 To begin, the MOU specifically refutes any agency relationship between Dropbox and NCMEC: Dropbox and NCMEC agree that they are dealing with each other as independent contractors. Nothing contained in this MOU shall be construed as creating or constituting an employee/employer relationship, a partnership, a joint venture, or an agency between Dropbox and NCMEC. Additionally, although the agreements enabled Dropbox to use the technology, which it then agreed to do, it is clear from the text of these agreements that NCMEC had no involvement in Dropbox’s actual use of the technology or the database. There is nothing in the agreements on how or when Dropbox would use the technology on its servers—much less for what reason Dropbox would use it (and certainly not that it would use it for NCMEC’s benefit rather than its own). To the contrary, NCMEC explicitly stated that it was “not responsible for instructing, directing, or making any recommendations regarding how [Dropbox] will utilize the PhotoDNA Signatures and/or Hashes they download from the Nonprofit Database.” (emphasis added). NCMEC also stated that “NCMEC does not submit and is not responsible for information submitted to the Nonprofit Database by Participating Nonprofits.” And NCMEC was clear that it “does not categorize, solicit, remove, review, approve, create, vet or make any recommendations regarding any PhotoDNA Signatures and/or Hashes submitted to the Nonprofit Database by Participating Nonprofits.” 20 The agreements additionally show that Dropbox’s participation was voluntary. The database agreements say that Dropbox “is authorized, but not obligated, to access the Nonprofit Database and/or download any PhotoDNA Signatures and/or Hashes contained in the Nonprofit Database.” (emphasis added). Those agreements are also clear that Dropbox was not permitted to use any information from the database “for any purpose other than to perform its voluntary functions under” the agreements. (emphasis added).13 And again, although Dropbox elected (in the MOU) to agree to use PhotoDNA signatures in conjunction with PhotoDNA, the law did not compel this, and nothing requires Dropbox to use the technology in any particular manner—let alone for any particular purpose—beyond what it voluntarily chooses.14 In total, these agreements show that NCMEC makes a database available to Dropbox and allows Dropbox to use (subject to restrictions) its technology (which 13 The same is true for the industry hash-sharing database agreement, which states that NCMEC “is not responsible for content contained within the Database,” and that

Dropbox "is authorized, but not obligated to, access the Database." (emphasis added). Dropbox also acknowledged that "if it voluntarily submits Signatures and Hashes to the Database, it grants to all Registrants" the right to use the information. 14 This is not like Skinner v. Railway Labor Executives Association, 489 U.S. 602, 614–15 (1989), in which features of the regulatory scheme at issue there led the Court to conclude that private railroad actions qualified as governmental actions. See Miller, 982 F.3d at 423–24 (distinguishing Skinner, in which "regulations preempted conflicting state laws and collective-bargaining terms, conferred on the government a right to receive test results, barred railroads from contracting away their testing rights, and prohibited employees from refusing to take tests"). 21 is owned by Microsoft) to detect child pornography on its servers—to whatever extent that Dropbox chooses to do so, and for whatever reasons it may want to do so. Nothing here shows that NCMEC "knew of and acquiesced in" the search of Rosales's files. See Burwell, 576 S.W.3d at 831–32; Miller, 982 F.3d at 425. And critically, nothing shows that Dropbox undertook the actions at issue for the purpose of assisting NCMEC, instead of solely to further its own ends. See Burwell, 576 S.W.3d at 832; Miller, 982 F.3d at 425. On this record, Rosales failed to carry his burden of showing that Dropbox acted as a government agent when it reviewed his files for child pornography or sent its tip to NCMEC (as was required by law once Dropbox found child pornography). See Burwell, 576 S.W.3d at 832.

2. Officer Wilson did not exceed the scope of Dropbox's private

action. Rosales next argues that Officer Wilson's pre-warrant review of the files was an unlawful warrantless search, because, Rosales argues, Officer Wilson exceeded the scope of Dropbox's private action. The record refutes this argument. Under the private search doctrine, a subsequent government action does not intrude on one's Fourth Amendment rights if the government merely replicates prior private action and does not "exceed the scope of the private search." See Jacobsen, 466 U.S. at 115–16, 119–20 (government's "viewing of what a private party had 22 freely made available" did not infringe Fourth Amendment rights); see also Rodriguez, 521 S.W.3d at 11 (similar). The government exceeds the scope when its review goes beyond that of the private party, and it learns or discovers "anything more" than what the private review already showed. See Jacobsen, 466 U.S. at 119–20. But under settled law, the government may replicate a private search without a warrant when there is "virtual certainty" that its actions will disclose nothing more than what a private party's earlier review has revealed. See id. at 119 (private search doctrine authorizes warrantless search only when there is "virtual certainty" latter will "not tell [police] anything more than" already revealed by private search); see also Miller, 982 F.3d at 428 (similar). If the government discovers new evidence that it was not substantially certain to find based on the private search, the private search doctrine does not apply to the new evidence, and the new evidence may be suppressed. See Meals, 21 F.4th at 906–07. The parties dispute who has the burden to prove whether Officer Wilson's pre-warrant review of the materials was within or exceeded the scope of Dropbox's search. But we need not reach that issue. Even if we assume for these purposes the State had the burden to prove that it did not exceed the scope of Dropbox's

private search, it has carried its burden. As the trial court found, the record supports that Officer Wilson viewed the same files that Dropbox viewed, nothing more. 23 Dropbox's cyber tip in this case unequivocally states that Dropbox viewed the "entire contents" of each of the nine uploaded files and then reported the files as child pornography. "Cyber tips have 'significant indicia of reliability,' and the information contained in such tips is per se substantially certain." Meals, 21 F.4th at 908 (quoting United States v. Landreneau, 967 F.3d 443, 453 (5th Cir. 2020)). And there is no dispute that, in his initial review, Officer Wilson viewed only those same nine files that Dropbox sent. That resolves this issue. The record shows that Dropbox viewed the entire contents of each of the nine files at issue. On this record, Officer Wilson's review of those same nine files did not exceed Dropbox's private review. Despite this, Rosales takes aim at the fact that Officer Wilson, in his testimony, said that he was uncertain of how much of the videos were watched by Dropbox. Specifically, he testified that the cyber tip indicated that someone at Dropbox "physically [laid] eyes on [the] file[s]" and "physically saw the video[s]," but he could not affirmatively answer (he did not know) whether that person watched the entire videos. Not only is the trial court's role to assess credibility, see Valtierra, 310 S.W.3d at 447, but this record contained clear evidence in the cyber tip itself that Dropbox viewed the "entire contents" of the files at issue that were later viewed by the police. 24 The trial court was free to believe that evidence. See id. That Officer Wilson did not know all the details of what was viewed does not call this evidence into question.15 Officer Wilson's pre-warrant review did not exceed the scope of Dropbox's private action. This record presents no Fourth Amendment violation. See Jacobsen, 466 U.S. at 119–20. B. As to the ultimate search warrant, the supporting affidavit established probable cause, even with the challenged statements excised. Having determined that the pre-warrant actions at issue did not violate Rosales's Fourth Amendment rights, we turn to Rosales's argument that the trial court erred in concluding that probable cause supported the later issuance of a search 15 Rosales relatedly argues that the record does not specify who at Dropbox viewed the files "or if only the hash values were reviewed" by a computer. Federal appellate courts are divided as to whether the government exceeds the scope of a private search when an investigator views a file after a computer-based hash match. The Fifth and Sixth Circuits say no. See Reddick, 900 F.3d at 639 ("When Detective Ilse first received Reddick's files, he already knew that their hash values matched the hash values of child pornography images known to NCMEC. . . . Accordingly, when Detective Ilse opened the files, there was no significant expansion of the search that had been conducted previously by a private party sufficient to constitute a separate search." (cleaned up)); Miller, 982 F.3d at 426–31 (similar). The Second and Ninth Circuits say yes. See United States v. Maher, 120 F.4th 297, 318 (2d Cir. 2024) ("[T]he private search doctrine does not permit police to conduct a warrantless visual examination of a digital file that a private party has not itself viewed but only computer hash matched to the contents of another digital file previously determined to contain child pornography."); United States v. Wilson, 13 F.4th 961, 964, 974–76 (9th Cir. 2021) (similar). But we need not reach that legal dispute here because the cyber

tip itself was clear that Dropbox viewed the entire contents of the files; Officer Wilson also testified that someone at Dropbox viewed the files (and there was no evidence to the contrary). See Valtierra, 310 S.W.3d at 447. 25 warrant for Rosales's entire Dropbox account. We agree with the trial court. After the challenged statements were excised, the remaining statements in the affidavit establish probable cause.

1. In a case like this one, Texas law asks whether the non-excised

statements in the affidavit establish probable cause. A search warrant must be based on probable cause. Diaz v. State, 632 S.W.3d 889, 892 (Tex. Crim. App. 2021). "Probable cause exists if there is a fair probability that evidence of a crime will be found at a specified location." Id. Under Franks v. Delaware, 438 U.S. 154 (1978), defendants may attack "the truthfulness of factual statements made in a search warrant affidavit." Diaz, 632 S.W.3d at 892 (citing Franks, 438 U.S. at 171–72). The defendant "bears the burden to show by a preponderance of the evidence a material misstatement that was made intentionally or knowingly or with reckless disregard for the truth." Id. (citing Franks at 155–56). If the defendant meets his burden and establishes that a material misstatement was made, the affidavit's false material is set aside. Hyland v. State, 574 S.W.3d 904, 911 (Tex. Crim. App. 2019). The reviewing court then determines whether probable cause still exists without the excised statements. Id. "If the remaining content of the affidavit does not then still establish sufficient probable cause, the search warrant must be voided and the evidence resulting from that search excluded." Harris v. State, 227 S.W.3d 83, 85 (Tex. Crim. App. 2007); see also Hyland, 574 S.W.3d at 911. 26 The "question for the reviewing court becomes the same as it would be for a magistrate conducting an initial review of a search warrant affidavit: Whether the remaining statements in the affidavit establish probable cause." Hyland, 574 S.W.3d at 911. "In resolving that question, reviewing courts are still required to read the purged affidavit in accordance with Illinois v. Gates, [462 U.S. 213 (1983)] and must therefore undertake a totality-of-the-circumstances approach." Id. (cleaned up); see Gates, 462 U.S. at 238 ("The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place."). The reviewing court's probable cause analysis is confined to the four corners of the search warrant affidavit, as well as to logical inferences the magistrate might draw based on the facts contained in the affidavit. Hyland, 574 S.W.3d at 907 n.4, 910–11.

2. The warrant affidavit here included the following information.

Remaining/Non-excised statements In the non-excised portions of the affidavit—the portion that we examine to determine if it shows probable cause—Officer Wilson attested that he had reason to believe evidence "of the offenses of Possession and/or Promotion of Child 27 Pornography" would be found in Rosales's Dropbox account. Officer Wilson averred the following: The tip. • On July 27, 2019, your Affiant received Cybertip number 49956945. • The tip came from NCMEC and showed "a possible Internet child exploitation crime has been observed and reported." •

Officer Wilson reviewed the tip "and learned that the reporting party was Dropbox, Inc." • Officer Wilson knew "from his training and experience that Dropbox is a 'cloud storage' site and file hosting service" that allows users to share files. The files. • Officer Wilson attested that "[t]he representative of Dropbox, Inc., provided eight digital media files with the Cybertip, and your Affiant personally reviewed each of those files provided." • Officer Wilson provided the file names for two of the video files and described how each video depicts a prepubescent girl (approximately 8-11 years of age) exposing her genitals. Rosales. • Officer Wilson stated that Dropbox identified the suspect user under the screen/user name "Robert Rosales" and provided the email address and user ID. • Officer Wilson attested that Dropbox provided an IP address that the user utilized to access his Dropbox account (Officer Wilson included two IP addresses, but one of them was excised; the correct one, however, remains).16 16 According to the affidavit, Dropbox reported two IP addresses that had logged in to the account: 2601:2c1:c100:5d0:6c4f:605b:fc52:d2f3 and 2601:2c1:c100:5d0:115f: 34d4:994e:ca6a. 28 • According to Officer Wilson, Comcast assigned that IP address, which was the IP address Dropbox indicated that the user utilized to access his account on "May 23, 2019 at 09:59:20 UTC." • An officer issued Comcast a subpoena for the subscriber information for that IP address. • Comcast provided subscriber information, which belonged to a subscriber at a Houston service address. • Officer Wilson learned through a police database search that someone named Rosales lived at that Houston service address. Preservation. • Officer Wilson "knows from training and experience that Dropbox, Inc., preserves the contents of customer or individual subscriber/user account(s) as well as the content of the account after reporting a Cybertip." • "[Y]our Affiant can reasonably expect Dropbox, Inc., to currently possess the data requested in this Affidavit." Excised statements Apart from all of this, Officer Wilson made three statements that the trial court excised under Franks. First, the trial court excised the affidavit's discussion of a superfluous (and as the trial court found, not material) IP address—but the trial court did not disturb the discussion of the correct IP address, as explained above. Specifically, in the affidavit, Officer Wilson identified two IP addresses and stated that Comcast "indicated that the subscriber, service address, and billing address" for both belonged to a subscriber at a Houston service address. But the trial court found that Comcast responded to the 29 subpoena with subscriber information for only one of the two listed IP addresses (the non-excised IP address), not both.17 So the trial court excised the discussion of the second, superfluous IP address. Second, the trial court excised a statement about a preservation notice. In addition to discussing his expectation that Dropbox would preserve the files, Officer Wilson asserted that he had "provided notice to Dropbox, Inc. to preserve the contents of the customer or individual subscriber/user account(s)." The trial court found this preservation notice statement to be false—and thus excised it—because Officer Wilson testified that he did not actually notify Dropbox to maintain files. Instead, he testified—consistent with his separate assertion in his affidavit—that, based on his experience, he expected that Dropbox would preserve its files. Finally, the court excised a statement in the affidavit about the upload date of the

materials at issue. The affidavit stated: “In Cybertip 49956945, a representative of Dropbox, Inc., reported that a Dropbox, Inc., user had uploaded approximately eight sexually explicit files which depicted suspected child pornography to the Dropbox, Inc., servers on May 27, 2019.” (emphasis added). But it appears that the May 27 date was the date the files were identified by Dropbox—not the date the files 17 Officer Wilson admitted during the hearing that only one of the IP addresses was actually linked to that service address, and the inclusion of both IP addresses in the affidavit was an “oversight” or “clerical error.” 30 were uploaded.18 The trial court found that no files were uploaded to Dropbox on that date, and it excised that upload date statement.

3. The remaining facts in the affidavit established probable cause.

The non-excised facts, standing on their own, are sufficient to establish probable cause that evidence of child pornography would be found in Rosales’s Dropbox account. Again, the probable cause inquiry asks “if there is a fair probability that evidence of a crime will be found at a specified location,” which here would be Dropbox’s servers. Diaz, 632 S.W.3d at 892. On this record, the answer is yes. See, e.g., Bordelon v. State, 673 S.W.3d 775, 787–92 (Tex. App.—Dallas 2023, no pet.) (warrant affidavit provided probable cause that evidence of child pornography would be found at defendant’s residence by linking his IP address to his physical address and noting that collectors of such material typically retain it for long periods); see also United States v. Bosyk, 933 F.3d 319, 325–30 (4th Cir. 2019) (warrant affidavit provided probable cause to search defendant’s house for child pornography; affidavit showed that, when post advertising child pornography appeared on forum, IP address linked to defendant’s home accessed posted link). 18 The trial court found that the records from Dropbox showed the files in question were uploaded in January 2018 and January 2019. During the hearing, Officer Wilson said that he had made “a clerical error”; he stated that May 27, 2019, was the date reflected in the cyber tip as the offense date for when the files were discovered by Dropbox—not the date the files were uploaded to Dropbox’s servers. 31 Rosales’s arguments to the contrary do not change this analysis. Although in considering probable cause we review the entire remaining affidavit as a whole, in explaining why Rosales’s arguments do not change the result, we take each in turn. Rosales’s IP address argument Rosales contends that, without the second IP address (i.e., with it excised), the affidavit does not link his Dropbox account to a Texas location. Not so. The remaining facts show a valid IP address that was connected in May 2019 to a Houston service address—and to Rosales. The removal of an extra and unnecessary IP address did not erase the affidavit’s identification of the other IP address, which linked to Rosales’s Houston service address. Rosales’s notice argument Contrary to Rosales’s assertion, nor does the removal of the notice statement change the analysis. The affidavit includes Officer Wilson’s statement that he expected Dropbox to preserve the files: that preservation was what companies like Dropbox automatically do (which, we note, is consistent with legal requirements).19 Thus, without the statement that Officer Wilson told Dropbox to keep the files, the 19 Indeed, Dropbox was legally required to preserve the digital files provided in the cyber tip in a secure location for at least one

year after submission of the tip. See 18 U.S.C. § 2258A(h); Ackerman, 831 F.3d at 1297 (ESP must preserve records after submitting cyber tip). 32 affidavit supports a reasonable inference that Dropbox would retain the files after sending its tip. Rosasles's date information argument The excision of the purported upload date likewise does not eliminate probable cause. Probable cause exists in the remaining portions of the affidavit. On this point, Rosales argues that the factual basis for probable cause grew "stale" because, although the court has the date HPD received the cyber tip from NCMEC (among all the other facts), it does not have the specific date when the child pornography was uploaded, when Dropbox discovered the files, or a specific timeline for how long Dropbox would retain the data. Staleness turns on "common sense" and the likelihood that the evidence sought will still be available in the same place. Crider v. State, 352 S.W.3d 704, 707–08 (Tex. Crim. App. 2011). In evaluating staleness, we consider "the details of the case, including the nature of the offense and the evidence sought, especially whether the evidence is of the sort that can reasonably be expected to be kept for long periods of time in the place to be searched." Veal v. State, 682 S.W.3d 577, 582–83 (Tex. App.—Houston [1st Dist.] 2023, pet. ref'd) (internal quotation marks omitted). Here, given the remaining affidavit's inclusion of the date HPD received the cyber tip, coupled with the nature and details of the offense and related information 33 in the remaining portions of the affidavit (including preservation information), as well as the legal framework, the facts were not stale. To begin, certain dates anchor this analysis. Officer Wilson sought the warrant in September 2019. So the question is: Was the information stale at that point? Next, the affidavit states that HPD (and Officer Wilson) received the cyber tip from NCMEC in July 2019. In addition, the affidavit states that Dropbox's tip, which provided the user's IP address, included a date stamp showing the user accessed the account in May 2019. Because Dropbox's tip could not possibly have referenced a May 2019 access date prior to May 2019 (Dropbox could not have included in its tip an access date that had not yet occurred), a court could reasonably infer that Dropbox submitted its tip to NCMEC during or after May 2019. And moreover, because NCMEC, in turn, sent its tip to HPD in July 2019, a court could also reasonably infer that Dropbox must have sent its tip to NCMEC during or before July 2019 (NCMEC's tip was in response to Dropbox's). So, the affidavit supports a reasonable inference that Dropbox sent its tip to NCMEC between May and July 2019 (then NCMEC sent its tip to HPD in July 2019). Moreover, a court could reasonably infer here that Dropbox detected the files in question near the date of its cyber tip to NCMEC. We note that, once Dropbox identified the child pornography, it was subject to federal reporting obligations with 34 severe penalties for noncompliance. See Ackerman, 831 F.3d at 1296 (citing 18 U.S.C. § 2258A(a)(1), (e)) (explaining that ESPs who fail to comply with their obligation to report child pornography "face substantial (and apparently criminal) penalties payable to the federal government"). Despite all of this, Rosales argues that, without the "preservation notice" language that was excised (discussed above), the affidavit lacks any indication of how long Dropbox would retain the data from the account. But as explained, Officer Wilson attested in the affidavit (in the non-excised portion) that

he “reasonably expect[ed]” Dropbox to have possession of this evidence because he knew, based on his training and experience, that Dropbox preserves the contents of a user’s account after reporting a cyber tip. (As noted, this testimony is consistent with Dropbox’s legal requirements). The affidavit thus supports a reasonable inference that, in September 2019, Dropbox would still possess Rosales’s data containing evidence of the child pornography. Under the circumstances, a magistrate could reasonably infer that a search of Rosales’s Dropbox account in September 2019 (when the warrant was issued) would still yield evidence of child pornography. See Bordelon, 673 S.W.3d at 787–92 (where Microsoft sent cyber tip to NCMEC in January, and police sought warrant in June, probable cause did not grow stale despite affidavit not connecting owner of IP address to date of incriminating uploads). 35 Moreover, Texas courts have explained that child pornography cases often involve continuous criminal endeavors where collectors tend to retain the contraband indefinitely; thus, courts “have repeatedly rejected claims that the passage of months or even more than a year between the alleged activity and issuance of the warrant renders the information within an affidavit stale.” Id. at 792 (cleaned up) (citing Ex Parte Jones, 473 S.W.3d 850, 857 (Tex. App.—Houston [14th Dist.] 2015, pet. ref’d) (collecting cases)); see also Steele v. State, 355 S.W.3d 746, 750–52 (Tex. App.—Houston [1st Dist.] 2011, pet. ref’d) (affidavit provided probable cause despite its omission of dates related to child pornography investigation; magistrate could infer ongoing possession of child pornography based on affiant’s expert testimony and continuous nature of activity). Those principles apply readily here. See Bordelon, 673 S.W.3d at 792; United States v. Evans, 171 F. App’x. 694, 696–97 (9th Cir. 2006) (affidavit that did not specify date that images of child pornography were uploaded to defendant’s Yahoo account was not impermissibly stale); see also, e.g., McKissick v. State, 209 S.W.3d 205, 214–15 (Tex. App.—Houston [1st Dist.] 2006, pet ref’d) (facts alleging defendant possessed child pornography were not stale because conduct was of continual nature and officer averred such images tend to be preserved on personal computers over protracted period); Jones, 473 S.W.3d at 856–57 (facts in affidavit had not become stale when magistrate could conclude defendant still possessed child 36 pornography although his last purchase of membership in child-pornography website occurred over two years before; he made purchases on four occasions over time, and officer averred that persons who have sexual interest in children rarely dispose of sexually-explicit materials). Considering the totality of the remaining facts in Officer Wilson’s search warrant affidavit, we conclude that the facts were not stale, and the affidavit demonstrated the existence of probable cause with the Franks statements excised.

CONCLUSION

We affirm the trial court’s judgments. Jennifer Caughey Justice Panel consists of Justices Gunn, Caughey, and Dokupil. Publish. TEX. R. APP. P. 47.2(b). 37