the Jasuta / Schulman report

Volume 33, Number 44 ~ Monday, December 1, 2025 (Report No. 1,589)

TIBA's Case of the Week

Houston / First Court of Criminal Appeals

Case Name: ***Robert Aaron Rosales v. The State of Texas***

- **OFFENSE**: Possession or Promotion of Child Pornography
- **COUNTY**: Harris
- **C/A CASE No**. 01-23-00876-CR and 01-23-00877-CR
- **DATE OF OPINION**: November 25, 2025 **OPINION**: Justice Jennifer Caughey
- **DISPOSITION**: Trial Court Affirmed
- **TRIAL COURT**: 351st D/C; Hon. Natalia Cornelio
- **LAWYERS**: Jonathan Landers & Coby DuBose (Defense); Heather Hudson (State)

Ed Note (**Procedural History**): A prior panel of the Court previously issued an opinion affirming the conviction in this case (see G&S, Vol. 33, No. 29; 08/04/2025). Defense counsel filed a motion to recuse Justice Clint Morgan, who authored the previous opinion, based on his involvement in the case while he worked at the District Attorney's office. The Court withdrew the original opinion on September 25th and indicated that the case would be submitted to a different panel. This opinion follows.

(**Background Facts**): Appellant uploaded several digital files containing child pornography to Dropbox, a cloud storage and file-sharing company. Dropbox discovered these files and, in May of 2019, submitted a "cyber tip" to the National Center for Missing and Exploited Children ("NCMEC") indicating that it had identified apparent child pornography on one of its user's accounts. The cyber tip provided identifying information for the account holder, including his screen/user name, 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). The police 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 Appellant. 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. After the warrant issued, Dropbox provided approximately 200 media files, some of which reportedly contained images and videos of child pornography. A grand jury indicted Appellant for five charges of possession of child pornography.

Ed Note (**Court Proceedings**): Appellant moved to suppress the State's evidence based on a claim that it was obtained illegally. After a hearing, the trial court denied that motion. Appellant then entered a plea bargain where he pleaded guilty to two charges in return for the State dismissing three charges and recommending that he be placed on deferred adjudication community supervision for four years. The trial court accepted the plea bargain, entered orders of deferred adjudication community supervision, and certified Appellant's right to appeal his written motion to suppress.

[**31.02 Search & Seizure / Warrantless Searches**]: Appellant argues that Dropbox was a government agent, and therefore the company's review of his files constituted an unlawful search under the Fourth Amendment.

Holding: The Fourth Amendment protects only against the government's unreasonable searches and seizures -- not those of private parties. ***State v. Ruiz***, 577 S.W.3d 543 (Tex.Cr.App. 2019)(see , Vol. 27, No. 25; 07/08/2019); see also ***Burdeau v. McDowell***, 256 U.S. 465 (1921). Under the private search doctrine, even "a wrongful search or seizure conducted by a private party does not violate the Fourth Amendment and that such private wrongdoing does not deprive the government of the right to use evidence that it has acquired lawfully." ***Ruiz***, (quoting ***Walter v. United States***, 447 U.S. 649, 656 (1980)). *** 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 [see, e.g., ***State v. Dobbs***, 323 S.W.3d 184 (Tex.App. -(Tex.Cr.App. 2010)(see , Vol. 18, No. 41; October 25, 2010)]. 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 can be used to obtain warrants or to prosecute." ***United States v. Meals***, 21 F.4th 903 (5th Cir. 2021). *** The private search doctrine applies in this case.

Sidebars

(David A. Schulman) If you still believe that "cloud" storage sites don't look at your files, you better become more cynical. I once again strongly suggest that lawyers refrain from putting confidential files on **any** cloud storage site.

(**John G. Jasuta**) I agree with David as to lawyers. Don't put confidential files on the internet even if it is called "cloud" storage. As to all you perverts out there, go ahead, dumbass.

[32.01 Search & Seizure / Reasonable Expectation of Privacy (On-Line Services -- Search Warrants)]: Appellant 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. He contends that Dropbox acted as an agent or instrument of the government when it reviewed his files.

Holding: [Appellant] 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, [Appellant] argues that Dropbox was required to obtain a warrant before reviewing his account, and its failure to do so renders the fruits of its search inadmissible. But even assuming for these purposes that NCMEC is a government agency, 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. We conduct our analysis of this question on a case-by-case basis in light of all the circumstances. Both factors must be present to convert a private search into a search by a government agent. Our Court has previously concluded that the "defendant bears the burden of proving that a private party acted as an agent of the government." ***Burwell v. State***, 576 S.W.3d 826 (Tex.App. - Houston [1st] 2019)(see , Vol. 27, No. 19; 05/27/2019)(citing ***Dawson v. State***, 106 S.W.3d 388 (Tex.App. - Houston [1st] 2003)(see , Vol. 11, No. 20; 05/26/2003). That question is thus settled by precedent here. *** 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 [Appellant] to prevail.

Sidebars

(**John G. Jasuta**) See above.

(**David A. Schulman**) To demonstrate the strength of its holding, the Court of Appeals listed several other cases pertaining to several other big Internet based companies. This isn't new law.

[32.01 Search & Seizure / Reasonable Expectation of Privacy (On-Line Services -- Search Warrants)]: Appellant 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.

Holding: [Appellant] 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. *** Viewed as a whole, however, the agreements (and record) do not show the government both knew of and acquiesced in Dropbox's review of [Appellant]'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 [Appellant] 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. *** In total, these agreements show that NCMEC makes a database available to Dropbox and allows Dropbox to use (subject to restrictions) its technology (which 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 [Appellant]'s files. *** On this record, [Appellant] 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).

Sidebars

(**David A. Schulman**) No matter how these arguments are rehashed, I think they're too complicated to overcome the initial holding --- Dropbox is a private entity.

(**John G. Jasuta**) See above.

[31.02 **Search & Seizure / Warrantless Searches**]: Dropbox's tip included the eight files, which the affiant, Officer Wilson, viewed and confirmed at least two files contained child pornography. Appellant argues Wilson's pre-warrant review of the files was an unlawful warrantless search, because Wilson exceeded the scope of Dropbox's private action.

Holding: 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." ***United States v. Jacobsen***, 466 U.S. 109 (1984). *** 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. *** 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. *** 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 . . . 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. *** Officer Wilson's pre-warrant review did not exceed the scope of Dropbox's private action. This record presents no Fourth Amendment violation.

[**31.01 Search & Seizure / Search Warrants (Omissions & Misrepresentations)**]: Appellant argues that the trial court erred in finding that probable cause supported the ultimate issuance of a search warrant for the entirety of his 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.

Holding: Under ***Franks***, defendants may attack "the truthfulness of factual statements made in a search warrant affidavit." *** 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." *** 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 (Tex.Cr.App. 2019)(see , Vol. 27, No. 21; 06/10/2019). *** 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 Pornography" would be found in [Appellant]'s Dropbox account. *** The non-excised facts, standing on their own, are sufficient to establish probable cause that evidence of child pornography would be found in [Appellant]'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. *** On this record, the answer is yes. *** 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 in the remaining portions of the affidavit (including preservation information), as well as the legal framework, the facts were not stale. *** Under the circumstances, a magistrate could reasonably infer that a search of [Appellant]'s Dropbox account in September 2019 (when the warrant was issued) would still yield evidence of child pornography. *** 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.

Sidebars

(**David A. Schulman**) Although this opinion is correct in all or most of aspects, I find it quite interesting that although **more** than twice as long as Justice Morgan's opinion on original submission, this opinion doesn't say anything that wasn't covered in the original opinion. Was this an effort to make the public forget the original opinion? In any event, it shows me that, although he probably never should have participated in the case at the Court of Appeals, Justice Morgan's handling of the case was not in and of itself problematic.