STATE OF MINNESOTA

IN SUPREME COURT

A19-1886

Court of Appeals McKeig, J.

State of Minnesota,

Respondent,

vs.

Filed: August 24, 2022
Office of Appellate Courts

Tyler Ray Pauli,

Appellant.

Keith Ellison, Attorney General, Peter Magnuson, Assistant Attorney General, Saint Paul, Minnesota; and

Mark Rubin, Saint Louis County Attorney, Duluth, Minnesota, for respondent.

Cathryn Middlebrook, Chief Appellate Public Defender, Laura Heinrich, Assistant Public Defender, Saint Paul, Minnesota, for appellant.

Scott M. Flaherty, Taft, Stettinius & Hollister LLP, Minneapolis, Minnesota; and

Jennifer Lynch, Electronic Frontier Foundation, San Francisco, California; and

Teresa Nelson, American Civil Liberties Union of Minnesota, Minneapolis, Minnesota; and

Jennifer S. Granick, American Civil Liberties Union Foundation, San Francisco, California; for amici curiae Electronic Frontier Foundation, American Civil Liberties Union, and American Civil Liberties Union of Minnesota.

S Y L L A B U S

1. When a defendant moves to suppress the evidence obtained from a warrantless search and the State proves that the private search doctrine applies, the burden to show that the private party was acting on behalf of the government falls on the party seeking suppression of the evidence.

2. The Minnesota Rules of Evidence do not apply with full force during suppression hearings.

3. The warrantless search of defendant's personal online cloud storage account did not violate the Fourth Amendment because the search by law enforcement officers did not exceed the scope of the private search performed by an employee of the online cloud storage account company.

Affirmed.

O P I N I O N

MCKEIG, Justice.

Appellant Tyler Ray Pauli was charged with four counts of possession of pornographic work involving minors in violation of Minn. Stat. § 617.247, subd. 4(a) (2020), after law enforcement officers discovered digital child pornography files stored in his personal online cloud storage account.[1] Pauli filed a motion to suppress, arguing that the warrantless search of his online cloud storage account was unconstitutional under both

[1] "Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself." *Riley v. California*, 573 U.S. 373, 397 (2014).

the U.S. and Minnesota constitutions. The district court denied Pauli's suppression motion. Pauli waived his right to a jury trial and proceeded with a stipulated facts trial under Minn. R. Crim. P. 26.01, subd. 4. The district court found him guilty. In an unpublished decision, the court of appeals affirmed his convictions, finding that Pauli did not have an objectively reasonable expectation of privacy in his online cloud storage account. *State v. Pauli*, No. A19-1886, 2020 WL 7019328, at *3 (Minn. App. Nov. 30, 2020). We conclude that, even assuming that Pauli had a reasonable expectation of privacy in his cloud storage account, the government's search of his account was lawful under the private search doctrine. In reaching this conclusion, we further hold that Pauli, as the party seeking to suppress the evidence, bore the burden to show that the private party was acting on behalf of the government, and further hold that the Minnesota Rule of Evidence do not apply with full force during suppression hearings. Thus, we affirm the court of appeals decision, but on different grounds.

FACTS

Appellant Tyler Ray Pauli had a personal online cloud storage account with Dropbox. Dropbox is a private company that provides online accounts for individuals and businesses for the storage and sharing of electronic files, including photos, documents, and videos. Dropbox's terms of service contain a warning that the private company "may disclose your information to third parties if we determine that such disclosure is reasonably necessary to (a) comply with the law; (b) protect any person from death or serious bodily injury; (c) prevent fraud or abuse of Dropbox or our users; or (d) protect Dropbox's property rights." Dropbox's acceptable use policy states:

> [Y]ou 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.

Dropbox's privacy policy states: "[s]tewardship of your data is critical to us and a responsibility that we embrace. We believe that our users' data should receive the same legal protections regardless of whether it's stored on our services or on their home computer's hard drive."

On October 24, 2016, the National Center for Missing & Exploited Children (the Center) received a report of suspected child pornography possession through their CyberTipline.[2] A report submitted by an employee of Dropbox contained 63 images of suspected child pornography found in an account registered to a Yahoo e-mail address. A representative from the Center reviewed 2 of the 63 images and determined that the uploaded files contained child pornography. The Center representative then forwarded its findings and report to the Minnesota Bureau of Criminal Apprehension (BCA) for further investigation and possible criminal charges.

On November 17, 2016, the BCA received the Center's report of suspected child pornography on a Dropbox account and assigned Special Agent John Nordberg to

[2] The Center is a private, nonprofit organization that operates a centralized reporting system for the online exploitation of children, including child pornography, called the CyberTipline. *See* 18 U.S.C. § 2258A(a); 34 U.S.C. § 11293(b). When an electronic communication service provider learns of child pornography on its servers, it must make a report to the Center's CyberTipline. 18 U.S.C. § 2258A(a)(1). The Center is then responsible for forwarding substantiated reports on to the appropriate law enforcement agencies. 18 U.S.C. § 2258A(c).

investigate. Special Agent Nordberg confirmed that the files from Dropbox contained child pornography and connected the Yahoo e-mail address associated with the Dropbox account to Pauli.

On January 18, 2017, Special Agent Nordberg applied for a warrant to search other data and files stored in Pauli's Dropbox account. In the search warrant application, Special Agent Nordberg provided summaries of some of the child pornography files and requested to search the entirety of Pauli's Dropbox account to look for any additional child pornography stored there. A district court judge authorized the warrant, which was subsequently served on Dropbox.

On April 20, 2017, Special Agent Nordberg went to Pauli's residence to execute another search warrant for Pauli's electronic devices and ask Pauli questions about his Dropbox account. When questioned, Pauli admitted to Special Agent Nordberg that he used his Dropbox account to store child pornography images. Special Agent Nordberg seized a cell phone, laptop computer, and tablet from Pauli's residence.

On May 19, 2017, Special Agent Nordberg reviewed 866 files received from Dropbox in response to the search warrant issued in January. Special Agent Nordberg concluded that 156 of the files contained child pornography videos and submitted the files to the Center's Child Victim Identification Program. On June 27, 2017, Special Agent Nordberg received a report from the Center indicating that 21 of the files contained identified child victims.

Based on the BCA's investigation, the State charged Pauli with four counts of possession of pornographic work involving minors in violation of Minn. Stat. § 617.247,

subd. 4(a). On December 19, 2017, Pauli moved to suppress the evidence acquired from his Dropbox account. Pauli argued that the Center is a government actor and its review of the data files provided by Dropbox was an unlawful warrantless search. He also argued that the Dropbox terms of service did not make his expectation of privacy unreasonable. The State argued that the Fourth Amendment does not apply because Pauli does not have a reasonable expectation of privacy in the child pornography files stored in his Dropbox account. In the alternative, the State contended that the private search doctrine applied to the initial search of Pauli's account conducted by a Dropbox employee. Because the subsequent review by the Center did not exceed the search performed by Dropbox, the State argued there was no Fourth Amendment violation.

After reviewing the briefs and evidence submitted by the parties on the suppression motion, the district court was "unable at this time to determine the lynchpin issue." The district court found that "a large factual divide" existed as to what procedures were used by Dropbox and the Center. Due to the lack of clarity, the district court found that "it would be inappropriate . . . to decide the factual issues." The district court denied Pauli's motion to suppress the evidence based on a "lack of necessary information," but allowed Pauli to renew the motion upon the development of new information.

Pauli filed a motion to reconsider. The parties agreed to reopen the record, which the district court approved. The State submitted a letter from Dropbox that broadly described the procedures used by the private company when responding to reports of potential child sexual abuse content. The letter stated that "all apparent child pornography is manually reviewed by a member of the content safety team before it is reported to [the

Center]."[3] The State also submitted a summary of multiple conversations between the prosecutor in this case and legal counsel for Dropbox.

On February 8, 2019, legal counsel for Dropbox objected to a subpoena duces tecum sent by Pauli on procedural grounds, but stated that "[i]f you were to comply with these procedures, Dropbox would not have responsive records in any event . . . Dropbox does not have records of who may have reviewed any content associated with the account in question or who submitted the report in question to [the Center]."

On April 17, 2019, the district court issued an order denying Pauli's motion to reconsider its ruling on his suppression motion. The district court found that although Pauli likely had a subjective expectation of privacy in his Dropbox account, based on Dropbox's terms of service, his expectation was not reasonable. But even if Pauli had a reasonable expectation of privacy in his Dropbox account, the district court found that the private search doctrine applied because the government's subsequent searches did not expand the initial private search of files by the Dropbox employee.

Pauli waived his right to a jury trial and agreed to a stipulated facts trial under Minn. R. Crim. P. 26.01, subd. 4, recognizing that the ruling on the motion to suppress was dispositive of the case. The district court found Pauli guilty of all four counts of possession of pornography involving minors.

---

[3] The letter also stated that when a file is "publicly available," Dropbox is referring to the fact that a user created a shared link for a file. Each of the 63 image files of suspected child pornography found in Pauli's Dropbox account were marked as reviewed by the company and publicly available.

Pauli appealed his convictions, arguing that the search of his online cloud storage account violated the U.S. and Minnesota constitutions. In an unpublished decision, the court of appeals affirmed, finding that Pauli did not have an objectively reasonable expectation of privacy in his Dropbox account. *State v. Pauli*, No. A19-1886, 2020 WL 7019328, at *3 (Minn. App. Nov. 30, 2020). The court of appeals observed that "[i]n this case, the undisputed evidence reflects that Pauli voluntarily stored his child-pornography content with Dropbox despite clear and unambiguous warnings that such content violated Dropbox's policies; that Dropbox could review Pauli's conduct and content for compliance; and that Dropbox could report his content to law enforcement." *Id.* The court of appeals noted that "[i]n the context of electronic service providers like Dropbox, courts are split with regard to whether terms of service eliminate or diminish a user's objectively reasonable expectation of privacy." *Id.* The court of appeals reasoned, however, that here "[t]he terms are clear and unambiguous that although users retain ownership of the files stored in their Dropbox accounts, Dropbox's terms of service prohibit publishing or sharing illegal content of any kind, specifically including unlawful pornographic content . . . ." *Id.* Ultimately, the court of appeals concluded that when "Pauli agreed to Dropbox's terms of service before he established his Dropbox account," it undermined any objectively reasonable expectation of privacy. *Id.* at 3–4. The court of appeals did not address the applicability of the private search doctrine. *Id.* at *4.

This court granted Pauli's request for further review.

ANALYSIS

The United States and Minnesota Constitutions prohibit unreasonable searches and seizures. *See* U.S. Const. amend. IV; Minn. Const. art. I, § 10. An unreasonable search occurs when law enforcement intrudes upon an individual's subjective expectation of privacy that society is prepared to recognize as reasonable. *United States v. Katz*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see Smith v. Maryland*, 442 U.S. 735, 740 (1979) (explicitly adopting Justice Harlan's formulation for unreasonable searches as articulated in *Katz*); *State v. Leonard*, 943 N.W.2d 149, 156 (Minn. 2020).

"Warrantless searches and seizures are generally unreasonable." *State v. Taylor*, 965 N.W.2d 747, 752 (Minn. 2021). But such protections are intended as a restraint on the activities of the government, not the actions of private parties. *See State v. Buswell*, 460 N.W.2d 614, 617 (Minn. 1990); *see also State v. Hodges*, 287 N.W.2d 413, 415–16 (Minn. 1979). This legal principle serves as the foundation for the private search doctrine, which recognizes that government agents may duplicate searches performed previously by private parties without running afoul of the Fourth Amendment. *See United States v. Jacobsen*, 466 U.S. 109, 117 (1984).

The parties dispute whether Pauli had a reasonable expectation of privacy in his online cloud storage account. But even if he did, the State asserts that the search of Pauli's account was permissible under the private search doctrine. As a preliminary matter, the parties dispute two aspects of the legal analysis for the proper application of the private search doctrine. First, the parties dispute who bears the burden of proving that the private search doctrine applies to the search. Second, the parties question whether the district court

improperly considered inadmissible evidence to decide the issue below. We address these two issues first, and then apply the private search doctrine to the facts of this case.

I.

The private search doctrine's applicability depends on (1) whether a private party conducted the search; and (2) whether a subsequent search by law enforcement or other government actors exceeded the scope of the initial private search. *Jacobsen*, 466 U.S. at 113–17. The rationale behind the private search doctrine is that once an individual's reasonable expectation of privacy is frustrated by a private party, the government can perform the same search without a further violation of the person's privacy. *See id.* at 117. This rationale necessarily contemplates that an individual has a reasonable expectation of privacy in the area initially searched,[4] and a subsequent search by a government actor exceeding the scope of the initial search would therefore presumptively violate the Fourth Amendment. *Id.* at 117–18. It follows that, for the private search doctrine to apply, the State bears the burden to prove that a private actor conducted the initial search, and that the scope of the initial search and the scope of the subsequent search were the same. *See*

[4] We recognize that the court of appeals affirmed the district court's denial of Pauli's suppression motion by holding that Pauli lacked a reasonable expectation of privacy in his online cloud storage account. As the Supreme Court suggested in *City of Ontario v. Quon*, in cases involving reasonable expectation of privacy determinations for rapidly changing technologies, it may be preferable to dispose of the case on narrow grounds and avoid "implications for future cases that cannot be predicted." 560 U.S. 746, 759–60 (2010). Cloud storage is a rapidly changing technology with rapidly changing social norms, and as the resolution of whether users have a reasonable expectation of privacy in their account is immaterial to the outcome of this case, we choose to assume without deciding that users have an objective expectation of privacy in their accounts.

State v. Edstrom, 916 N.W.2d 512, 517 (Minn. 2018) (holding that once a defendant demonstrates a reasonable expectation of privacy in the area searched, the State generally bears the burden of establishing whether the challenged evidence was obtained in accordance with the constitution); *see also United States v. Wilson,* 13 F.4th 961, 971 (9th Cir. 2021) ("[t]he government bears the burden to prove [a] warrantless search was justified by the private search exception . . . .").[5]

But after the State satisfies its burden, a defendant may still be entitled to suppression of the evidence if the evidence shows that the private party who conducted the warrantless search was acting as an agent of the government. *State v. Dexter*, 941 N.W.2d 388, 394 (Minn. 2020). Other jurisdictions have placed the burden on the party seeking suppression to prove that the private party was acting on behalf of the government. *See United States v. Cleaveland*, 38 F.3d 1092, 1093 (9th Cir. 1994) ("The defendant has the burden of establishing government involvement in a private search."); *see also United States v. Feffer*, 831 F.2d 734, 739 (7th Cir. 1987) ("[I]t is the movant's burden to establish by a preponderance of the evidence that the private party acted as a government instrument or agent.").

We indirectly adopted the prevailing view from other jurisdictions in *State v. Dexter*, 941 N.W.2d. at 394–95. In *Dexter*, the defendant requested evidence held by the

---

[5] Based on this understanding of the private search doctrine as to the State's initial burden, the district court likely erred in denying Pauli's first suppression motion. At that point, the State had not proven the scope of the search, and the court should have therefore granted Pauli's motion to suppress. But Pauli did not challenge the district court's decision to keep the record open on appeal, and the argument is therefore forfeited. *See State v. Myhre*, 875 N.W.2d 799, 806 (Minn. 2016).

State to determine whether a confidential informant was acting as a government agent for the purposes of the private search doctrine. *Id*. We held that the defendant was entitled to receive the information to support his claim that a private actor conducted the search on behalf of the government. *Id.* Notably, we did not suggest that the burden was on the State to affirmatively prove that the confidential informant was not acting on behalf of the government. Instead, the logical presumption is that a private actor is conducting the search for its own interests.

Accordingly, we now clarify and explicitly hold that the burden to prove that a private party was acting on behalf of the government when conducting a Fourth Amendment search falls on the party seeking suppression of the evidence.

II.

The parties also disagree over what evidence can be considered by a district court at a suppression hearing. Pauli argues that the evidence submitted by the State in this case—communications from legal counsel for Dropbox—was inadmissible as both hearsay and lacking personal knowledge. In ruling on Pauli's motion to reconsider the suppression issue, the district court considered a letter from legal counsel for Dropbox setting forth general company practices and policies when reviewing potentially illegal material in accounts, as well as summaries of several conversations between the prosecutor and legal counsel for Dropbox. Pauli contends that this evidence was improperly considered by the district court, as statements by attorneys who lack personal knowledge of a case are inadmissible. *See* Minn. R. Evid. 602. Pauli also contends that this evidence falls within

the definition for hearsay under Minnesota Rules of Evidence 801 and does not meet any of the exceptions set forth in Minnesota Rules of Evidence 803.

The State argues that district courts are not bound by the Rules of Evidence at suppression hearings, and therefore the district court properly considered the letter from legal counsel for Dropbox as well as the conversation summaries. The State also argues that our precedent only establishes that comments of counsel made during trial are not evidence and points out that Pauli does not explain why this rule should be extended to suppression hearings.

When interpreting the Minnesota Rules of Evidence, we start by looking at the plain language of the rules themselves. *State v. Willis*, 898 N.W.2d 642, 645 (Minn. 2017). In *Willis*, the district court admitted hearsay evidence offered by the State during a restitution hearing over defendant's objections. *Id.* at 644. On appeal, the court of appeals affirmed the district court's findings that the Rules of Evidence do not apply to restitution hearings. *Id.* at 645. We reversed, holding that Rule 1101, which governs the rules' applicability to certain types of proceedings, does not exclude the application of evidentiary rules to restitution hearings. *Id.* at 645–66. Our view in *Willis* was that because, at the time, restitution hearings were not included in the specific exceptions listed in Rule 1101(b)(3), and because "[w]e have interpreted similar silence to mean that the Rules of Evidence

apply to any unlisted proceedings," the Rules of Evidence apply to restitution hearings.[6] *Id.* at 645–48.

Certain pretrial hearings, however, are specifically exempted from the Rules of Evidence. For example, Minnesota Rule of Evidence 1101(b)(1) and Rule 104(a) exempt the "determination of questions of fact preliminary to admissibility of evidence. . . ." Minn. R. Evid. 1101(b)(1) (stating that the Rules of Evidence do not apply to such proceedings "to be determined by the court under Rule 104(a)"); *see also* Minn. R. Evid. 104(a) ("Preliminary questions concerning . . . the admissibility of evidence shall be determined by the court . . . . In making its determination it is not bound by the rules of evidence except those with respect to privileges."). In a pretrial suppression hearing, courts are tasked with determining whether evidence was obtained unconstitutionally. *See State ex rel. Rasmussen v. Tahash*, 141 N.W.2d 3, 13 (Minn. 1965). Generally, unconstitutionally obtained evidence is inadmissible. *See State. v. Jackson*, 742 N.W.2d 163, 175 (Minn. 2007). During a suppression hearing, judges conduct fact-finding to help them reach determinations of admissibility. *See Rasmussen*, 141 N.W.2d at 13 ("[i]f the defendant . . . contest[s] the admissibility of the evidence upon Federal constitutional grounds, a *pretrial fact hearing on the admissibility of the evidence* will be held . . .") (emphasis added); *Waller v. Georgia*, 467 U.S. 39, 47 (1984) (stating that the resolution of suppression hearings frequently turn on "factual matters"); *State v. Jackson*, 964 N.W.2d

---

[6] Rule 1101(c) was amended in 2019, following *Willis*, "to clarify the applicability of the Rules of Evidence to criminal restitution and expungement hearings." Minn. R. Evid. 1101 cmt.—2019.

659, 666 (Minn. App. 2021) (noting that pre-trial suppression hearings are "fact-finding proceedings").[7] Based on the plain text of the rule, suppression hearings are precisely the type of proceedings Rule 104(a) is intended to cover.

Relevant precedent further supports our conclusion. Rule 104 of the Federal Rules of Evidence, which is virtually identical to Rule 104 of the Minnesota Rules of Evidence, has been consistently interpreted to exempt suppression hearings.[8] *United States v. Matlock*, 415 U.S. 164, 172–73 (1974) ("[T]he rules of evidence normally applicable in criminal trials do not operate with full force at hearings before the judge to determine the admissibility of evidence."); *United States v. Raddatz*, 447 U.S. 667, 679 (1980) ("At a suppression hearing, the court may rely on hearsay and other evidence, even though that evidence would not be admissible at trial."). Other states have also found that their Federal Rule 104 analogues exempt suppression hearings from the strict confines of their state's rules of evidence. *See*, *e.g.*, *State v. Piper,* 855 N.W.2d 1, 9–10 (Neb. 2014) (holding the Rules of Evidence do not apply to address preliminary questions of admissibility, which includes suppression hearings); *State v. Boczar,* 863 N.E.2d 155, 159 (Ohio 2007) ("[T]he

---

[7] Pauli asserts that *Rasmussen* requires "competent" evidence, but that phrase is noticeably absent from the *Rasmussen* opinion. *See generally Rasmussen*, 141 N.W.2d. 3. Instead, *Rasmussen* only requires a "showing that the circumstances under which [evidence] was obtained were consistent with constitutional requirements." *Id* at 14.

[8] *Compare* Minn. R. Evid. 104(a) ("[p]reliminary questions concerning . . . the admissibility of evidence shall be determined by the court . . . In making its determination it is not bound by the rules of evidence except those with respect to privileges."), *with* Fed. R. Evid. 104(a) ("[t]he court must decide any preliminary question about whether . . . evidence is admissible. In so deciding, the court is not bound by evidence rules, except those on privilege.").

Rules of Evidence do not apply to suppression hearings."); *State v. Wright,* 843 P.2d 436, 439 (Or. 1992) (concluding that suppression hearings involve preliminary questions of fact governed by Oregon Evidence Code 104(1), and so the Rules of Evidence relating to the admissibility of hearsay do not apply); *see generally* 4 Wayne R. LaFave et. al., *Criminal Procedure* § 14.4(b) at 382–392 (4th ed. 2015). Our own court of appeals has reached the same conclusion, holding that "the technical rules of evidence do not apply to suppression hearings." *State v. Schuft*, No. C4-00-1320, 2001 WL 378955, at *3 (Minn. App. Apr. 17, 2001).

Finally, judicial economy weighs in favor of not requiring application of the Rules of Evidence during a suppression hearing. *See United States v. De La Fuente*, 548 F.2d 528, 532–533 (5th Cir.1977). Rule 104 is designed to excuse "time-consuming compliance with a superfluous formality." *See id.* at 533. If the Rules of Evidence were strictly applied to suppression hearings, more witnesses would have to testify, which would take more of the district court's time and more of the State's resources.

We recognize that in many instances, the admissibility of certain evidence is dispositive of a case. One could argue that suppression hearings have taken on such importance that application of the Rules of Evidence is necessary to protect the interests of litigants. *Cf. Waller*, 467 U.S. at 46 ("[S]uppression hearings often are as important as the trial itself."). But a district court's ability to reject unreliable evidence is not eliminated by allowing the court to consider evidence beyond what is admissible under the rules. In *Matlock*, the Supreme Court suggested that the judge "should receive the evidence and give it such weight as his judgment and experience counsel." 415 U.S. at 175. This approach

is consistent with Rule 104(a); though not bound to follow the Rules of Evidence, district court judges can and should still exclude evidence they deem unreliable. *See* 4 Wayne R. LaFave et. al., *Criminal Procedure* § 14.4(b) at 383 (4th ed. 2015) (stating that the inapplicability of the Rules of Evidence at a preliminary hearing "[does] not restrict the magistrate's authority to insist upon adherence to the rules of evidence where the magistrate believes that the offered incompetent evidence is not sufficiently reliable."); *see also Schuft*, 2001 WL 378955, at *3 ("The court is at liberty to exercise its discretion judiciously so as to conduct an efficient hearing that is fair in both perception and actuality."). District court judges still serve a vital gatekeeping function that Rule 104(a) does not eliminate.[9] But Rule 104(a) by its plain text—and supported by principles of judicial economy and rulings from other jurisdictions—does not require rigid adherence to the Rules of Evidence at suppression hearings.

Accordingly, we hold that the district court did not abuse its discretion in considering evidence from Dropbox's legal counsel when ruling on the suppression motion.

---

[9] We also recognize that procedural safeguards are in place to protect a defendant's constitutional rights during suppression hearings. *See Rasmussen*, 141 N.W.2d at 13 (discussing the procedure for suppression hearings, including holding the hearing in open court and requiring representation or advice by counsel). The Supreme Court has articulated that "the process due at a suppression hearing may be less demanding and elaborate than the protections accorded the defendant at the trial itself." *Raddatz*, 447 U.S. at 679. But the fact that the process due may be less does not mean safeguards are absent. Furthermore, some courts concerned about the fairness of the proceedings have distinguished between substantive rules within the rules of evidence, like hearsay, and procedural rules, like the sequestration of witnesses, finding that while courts are not bound by the former rules, they are still bound by the latter. *See United States v. Brewer*, 947 F.2d 404, 410 (9th Cir. 1991).

III.

Having established the legal principles above, we now consider the application of the private search doctrine in this case.

The determination of whether the private search doctrine applies is a question of fact. *Buswell*, 460 N.W.2d at 618. We will not reverse the district court's factual findings unless they are "clearly erroneous or contrary to law." *State v. Licari*, 659 N.W.2d 243, 250 (Minn. 2003) (citation omitted) (internal quotation marks omitted). A factual finding is clearly erroneous only when, after reviewing all the evidence, "we are left with the definite and firm conviction that a mistake occurred." *State v. Andersen*, 784 N.W.2d 320, 334 (Minn. 2010).

Here, the district court found the State met its burden to prove that the private search doctrine applies. The district court found that the initial search was conducted by a private party, Dropbox. Based on the letter from Dropbox and communications from Dropbox's counsel, the district court found that the initial search involved a manual review of Pauli's files. Because the searches conducted by the Center and the BCA involved manual searches of the same files, the subsequent searches were no more intrusive than the initial search performed by Dropbox.[10] While the factual findings supporting this conclusion may

[10] Jurisdictions disagree on whether the Center is a government actor under the private search doctrine. *Compare United States v. Ackerman*, 831 F.3d 1292, 1301 (10th Cir. 2016) (holding that the Center was a government actor under the private search doctrine), *with People v. Pierre*, 29 N.Y.S.3d 110, 120 (N.Y. Sup. Ct. 2016) (holding the Center was not a government actor under the private search doctrine). Other jurisdictions have declined to decide either way when the Center's status would not change the case's outcome. *See United States v. Bebris*, 4 F.4th 551, 558 (7th Cir. 2021). Because the

be minimal, they do not appear to be "clearly erroneous." *See Buswell*, 460 N.W.2d at 618. Accordingly, the State proved the applicability of the private search doctrine. Because the State satisfied its burden to prove that the private search doctrine applies, the burden shifted to Pauli to prove that Dropbox was acting on behalf of the government when the Dropbox employee searched his account. If Pauli could prove that Dropbox was acting as a government instrument or agent in searching his files, the private search doctrine would not permit subsequent search of those files by the government.

In Minnesota, the question of whether a private actor is acting as a government instrument or agent when conducting a search focuses on two considerations: (a) whether the State knew of and acquiesced in the search; and (b) whether the search was conducted to assist law enforcement's interests or the interests of the private party. *State v. Jorgensen*, 660 N.W.2d 127, 131 (Minn. 2003). "If the government does not know of and acquiesce in the search, the search cannot be attributed to the government and the inquiry ends." *Id.* We will not overturn a district court's determination of whether a private party acted as a government instrument or agent in their search unless the determination is clearly erroneous. *Id.*

Pauli suggests that law enforcement could have initiated the search of his account because, according to the correspondence from legal counsel for Dropbox, sometimes internal searches of accounts are initiated based on tips from law enforcement. Pauli also

---

Center's status as a governmental or non-governmental actor is immaterial to the outcome of this case, we decline to decide whether the Center is a government agent for the purposes of the private search doctrine.

claims that 18 U.S.C. § 2258A (2018), which requires companies to report child pornography found on their servers to the Center via the CyberTipline, effectively turns Dropbox into a government agent. But even if Pauli's arguments about either hypothetical law enforcement involvement or the role of 18 U.S.C. § 2258A had merit, his challenge to the district court's application of the private search doctrine would still fail. To defeat the application of the private search doctrine, a defendant must meet two separate and necessary requirements: not only must the defendant show the government knew of and acquiesced in the search, but he must also show that the search was conducted to assist law enforcement's interests, not the interests of the private party. *See Jorgensen*, 660 N.W.2d at 131. Dropbox has explicitly expressed its desire to keep child pornography off its servers. Regardless of where the tip came from, there is no evidence that Dropbox searched Pauli's account for any reason other than its own business interest in keeping child pornography off its servers. Pauli therefore failed to meet his burden to demonstrate Dropbox was acting as a government agent in searching his files.[11]

We agree with the district court that the State met its burden to prove the applicability of the private search doctrine. We also agree that Pauli failed to meet his

[11] Pauli also argues that the contents of his Dropbox account were his digital "papers" and "effects" and the government's search was therefore an unconstitutional trespass under *United States v. Jones*, 565 U.S. 400, 404 (2012). Under *Jones*, an unconstitutional trespass occurs where the government "obtains information by physically intruding on a constitutionally protected area . . . ." *Id.* at 406–07 n.3. The Tenth Circuit has found *Jones* applicable in cases involving government agents opening electronic files. *Ackerman*, 831 F.3d at 1307–1308. But in this case, the government did not directly access Pauli's online cloud storage account before obtaining a search warrant. Instead, the Center and the BCA viewed copies of his files provided by Dropbox. Therefore, even if *Jones* applies to trespasses on electronic files, it would not apply in this case.

burden to prove that Dropbox conducted the search on behalf of the government. Accordingly, the initial warrantless search of Pauli's online cloud storage account did not violate the Fourth Amendment.

CONCLUSION

For the foregoing reasons, we affirm the decision of the court of appeals, but we do so on different grounds.

Affirmed.