STATE OF WISCONSIN

C O U R T O F A P P E A L S

DISTRICT II

Case No. 2023AP2319 - CR

STATE OF WISCONSIN,

Plaintiff-Appellant,

v.

MICHAEL JOSEPH GASPER,

Defendant-Respondent.

APPEAL FROM AN ORDER GRANTING DEFENDANT'S MOTION TO SUPPRESS EVIDENCE, ENTERED IN WAUKESHA COUNTY CIRCUIT COURT, THE HONORABLE SHELLEY J. GAYLORD, PRESIDING.

BRIEF AND APPENDIX OF PLAINTIFF-APPELLANT

JOSHUA L. KAUL
Attorney General of Wisconsin

MICHAEL J. CONWAY
Assistant Attorney General
State Bar #1134356

Attorneys for Plaintiff-Appellant

Wisconsin Department of Justice
Post Office Box 7857
Madison, Wisconsin 53707-7857
(608) 267-8910
(608) 294-2907 (Fax)
conwaymj@doj.state.wi.us

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutions

Statutes

Other Authorities

INTRODUCTION

The State appeals the order granting Michael Joseph Gasper's motion to suppress a child pornography video found in his Snapchat account and other child pornography found on his phone following a search of his home pursuant to a warrant.

Snapchat detected the video in Gasper's account using software designed to detect copies of known child pornography files based on their "hash values." Snapchat reported the video to the National Center for Missing and Exploited Children (NCMEC) without opening it. NCMEC sent the video to the Wisconsin authorities without opening it. A detective opened the video and confirmed that it contained child pornography before preparing and executing the search warrant. This is "a fact pattern common in internet child pornography cases." *State v. Silverstein*, 2017 WI App 64, ¶ 5, 378 Wis. 2d 42, 902 N.W.2d 550.

Where this case departs from the prototypical case is the circuit court's suppression order. The circuit court suppressed the video because the detective opened it without a warrant or an exception, and it suppressed the additional child pornography recovered from the later-obtained search warrant as fruit of the poisonous tree.

The circuit court's conclusion that the detective could not open a video referred to him as child pornography by a private party runs counter to the holdings of two federal courts of appeals and four state appellate courts and has the support of only one federal court of appeals. Most critically, the circuit court's reasoning is legally flawed. The order should be reversed for three reasons.

First, Gasper failed to prove his reasonable expectation of privacy in the video. Snapchat's policies unambiguously prohibit child pornography and inform users that it scans for and reports such content to law enforcement. The circuit court

reasoned that because Gasper had a reasonable expectation of privacy in his cell phone and because he used his cell phone to access Snapchat, he had a reasonable expectation of privacy in the child pornography on his Snapchat account. The circuit court erred because the relevant area to analyze was Gasper's Snapchat account—the actual area searched—not the device he used to access it.

Second, the detective lawfully opened the video under the private-search doctrine. Because Snapchat frustrated Gasper's expectation of privacy by flagging and forwarding the video to law enforcement and because the detective had a virtual certainty that it contained nothing but child pornography based purely on the information Snapchat provided, the detective did not expand Snapchat's private search.

Finally, even if a Fourth Amendment violation occurred, the circuit court should have applied the good faith exception to the exclusionary rule. This case presents issues of first impression in Wisconsin. Neither the detective nor the issuing judge could have known that the search warrant was defective for relying on the opened video from Snapchat.

STATEMENT OF THE ISSUES

1. Does Gasper have a reasonable expectation of privacy in child pornography saved to his Snapchat account?

The circuit court answered: Yes.

This Court should answer: No.

2. Did the private-search doctrine apply when the detective opened a video that Snapchat identified as child pornography and reported to the authorities?

The circuit court answered: No.

This Court should answer: Yes.

3. Did the good faith exception to the exclusionary rule apply when the detective prepared a search warrant of Gasper's home based on viewing the video when the lawfulness of opening the video is unsettled in Wisconsin?

The circuit court did not answer this question.

This Court should answer: Yes.

STATEMENT ON ORAL ARGUMENT AND PUBLICATION

The State requests oral argument and publication. This case raises issues of first impression in Wisconsin law. The issues are also likely to recur as they arise from a common fact pattern in child pornography cases. The decision will therefore "[e]nunciate a new rule of law" and dispose of a "case of substantial and continuing public interest." Wis. Stat. § (Rule) 809.23(1)(a)1., 5. Given the novelty and importance of the issues, oral argument is also appropriate.

STATEMENT OF THE CASE

Snapchat,[1] an electronic service provider (ESP), detected a child pornography video that had been "saved, shared, or uploaded" to Gasper's Snapchat account. (R. 38:3; 60:86.) The video was not made publicly available, and no other user saw it. (R. 38:3–4.) Snapchat detected the video using Microsoft's PhotoDNA, a program that scans files to determine if they are copies of known and reported child pornography files. (R. 38:4; 60:24–25.) PhotoDNA operates through the use of "hash values." (R. 60:21–22.)

[1] Snapchat is a social media platform where users can "share text, photographs, and video recordings, collectively known as 'snaps.'" *Commonwealth v. Carrasquillo*, 179 N.E.3d 1104, 1109 (Mass. 2022).

A hash value is "an algorithmic calculation that yields an alphanumeric value for a file." *United States v. Stevenson*, 727 F.3d 826, 828 (8th Cir. 2013). This Court has described hash values as a "digital signature." *State v. Baric*, 2018 WI App 63, ¶ 5, 384 Wis. 2d 359, 919 N.W.2d 221. The algorithm derives the hash value by analyzing all the "bits" of data in a particular file. (R. 60:13–14.) A file's hash value remains constant regardless of the file's name. (R. 60:20.) If one bit is altered, however, then the entire hash value will change. (R. 60:13–16, 18.)

Because of the uniqueness of a file's hash value, many ESP's use hash value scanning software to detect child pornography. (R. 60:10–11.) The program can scan a file, derive its hash value, and compare that hash value to a database of hash values of known child pornography files. (R. 60:11); *see Baric*, 384 Wis. 2d 359, ¶ 6 (describing such a program). If the hash value of the scanned file matches a hash value in the database, then the ESP knows it has found a copy of that known child pornography file. (R. 60:11, 15.)

PhotoDNA represents an advancement in hash value scanning technology. Because a hash value changes so substantially if the file is only slightly altered, users can evade hash matching technologies by editing a single pixel. (R. 60:22.) PhotoDNA can detect these slightly edited files. It divides each image, or a still image from a video, into individual pieces and generates a hash value for each piece. (R. 60:22, 24, 88–89.) Rather than compare the hash values of *files*, PhotoDNA compares the hash values of *pieces* within files. (R. 60:24, 29.) If the hash values for the majority of pieces matches the hash values for the majority of pieces in a known child pornography file, PhotoDNA flags the scanned file as child pornography. (R. 60:24.) "A PhotoDNA hash is not reversible, and therefore cannot be used to recreate an image." (R. 37:2.)

In the present case, Snapchat forwarded the video flagged by PhotoDNA and Gasper's account information to NCMEC as required by federal law.[2] (R. 38:3; 60:37–38.) No Snapchat employee viewed the video before sending it. (R. 38:4.) That same day, Snapchat locked Gasper's account. (R. 60:52.)

NCMEC prepared a "CyberTip." (R. 60:37–38.) The CyberTip listed Gasper's username, email address, and date of birth. (R. 38:3.) NCMEC attached the reported video to the CyberTip and identified it as "Apparent Child Pornography." (R. 38:1.) No NCMEC representative opened the video. (R. 38:1.) The CyberTip stated that the categorization of "Apparent Child Pornography" was "based on NCMEC's review of uploaded files in this report **OR** a 'Hash Match' of one or more uploaded files to visually similar files that were previously viewed and categorized by NCMEC." (R. 38:5.) Since NCMEC did not review the video, the file was necessarily a "Hash Match." (R. 38:1, 5; 60:86–87.) The CyberTip did not include any other content from Gasper's account. (R. 60:54.)

NCMEC traced the IP address tied to Gasper's account to Wisconsin. (R. 60:37–38.) Accordingly, it sent the CyberTip to the Wisconsin Department of Justice (DOJ). (R. 60:38.) Upon receiving the tip, a DOJ policy analyst prepared and submitted an administrative subpoena that returned the subscriber information for the IP address. (R. 60:38–39.) The response listed Gasper as one of the subscribers and provided his address. (R. 40:3; 60:40–41.)

Detective David Schroeder received the CyberTip and the results of the administrative subpoena. He opened the video and confirmed that it depicted child pornography.

---

[2] "NCMEC is directed by federal law to serve as a clearinghouse for such tips and as a liaison to law enforcement." *Silverstein*, 378 Wis. 2d 42, ¶ 5.

(R. 60:88.) He then confirmed that Gasper occupied the residence connected to the IP address and that the available Wi-Fi networks outside Gasper's home were password-protected and not publicly accessible. (R. 6:22.) He subsequently prepared and executed a search warrant at Gasper's home. (R. 60:70–71.)

Police seized electronic devices from Gasper's home and took him into custody. (R. 46; 60:71–72.) After waiving his *Miranda*[3] rights (R. 60:72), Gasper disclosed to Detective Schroeder additional child pornography files that he accessed via the Kik messenger application on his phone. (R. 60:80–84.)

After being charged with 10 counts of possessing child pornography and 9 counts of sexual exploitation of a child (R. 20), Gasper filed a motion to suppress, raising several issues, (R. 23). This appeal concerns only Gasper's claim that all child pornography evidence should be suppressed. He claimed that the Snapchat video should be suppressed because Detective Schroeder opened it without a warrant or an exception. (R. 23:3.) He argued that all evidence recovered from the search warrant should be suppressed as fruit of the poisonous tree. (R. 23:3–4.) The parties briefed this issue prior to a suppression hearing. (R. 30; 33.)

Detective Schroeder was the lone witness to testify at the hearing. He explained hash values, described how PhotoDNA operates, and recounted how he responded to the CyberTip consistent with the foregoing facts.

The State submitted into evidence Snapchat policies that Gasper accepted when he made his account. (R. 41; 42; 44; 60:45–53, 56–57.) These policies banned child pornography and informed users that Snapchat was actively scanning for child pornography. (R. 41:4; 42:2; 44:3.) Detective

[3] *Miranda v. Arizona*, 384 U.S. 436 (1966).

Schroeder demonstrated how he was required to acknowledge the Terms of Service in order to create a Snapchat account. (R. 60:55–56.)

Detective Schroeder relayed his experience with the reliability of CyberTips and PhotoDNA. Every file from a CyberTip that he ever reviewed in an estimated 100 child pornography investigations had been child pornography, including those triggered by PhotoDNA. (R. 60:66, 68–69.) When he opens a file from a CyberTip, he knows that it is "likely going to be child sexual abuse material." (R. 60:66.)

On cross-examination, Gasper asked Detective Schroeder about the risk of hash value "collision." (R. 60:135.) Detective Schroeder defined "collision" as the theoretical risk that two distinct files have the same hash value. (R. 60:135–36.) He observed no evidence of collision in the present case and explained that collision had only ever been observed in laboratory settings with extremely small-sized files. (R. 60:148–50.) He was unsure if collision was a risk with PhotoDNA. (R. 60:139.) He clarified that Snapchat detected the video with PhotoDNA, not a one-to-one hash value match. (R. 60:26–27, 150.)

The State urged the circuit court to deny Gasper's motion to suppress for two primary reasons. First, Gasper had failed to prove that he had a reasonable expectation of privacy in a child pornography video saved to his account when Snapchat specifically prohibited and scanned for such content. (R. 60:162–64.) The State asserted that Gasper's theory depended entirely on conflating his expectation of privacy in his cell phone that he used to access Snapchat with an expectation of privacy in his Snapchat account. (R. 60:163.) Second, Detective Schroeder lawfully opened the video from the CyberTip pursuant to the private-search doctrine because Snapchat had already frustrated Gasper's expectation of privacy by scanning the video, identifying it as child pornography, and forwarding it to law enforcement.

(R. 60:164–69.) The State added that, even if Detective Schroeder violated the Fourth Amendment, he acted in good faith because the motion implicated a novel issue in Wisconsin. (R. 60:170.)

Gasper maintained that he had a reasonable expectation of privacy in his Snapchat account because it was an extension of his cell phone. (R. 60:205.) He argued that the private-search doctrine could not apply because no Snapchat employee opened the video and because the State had failed to establish the reliability of PhotoDNA. (R. 60:195–96.)

The circuit court[4] granted Gasper's motion to suppress in a written ruling following the hearing. It did not address Gasper's reasonable expectation of privacy other than to state "[t]here is a legitimate privacy interest in cell phones." (R. 56:3.) It concluded that the private-search doctrine could not apply for two reasons. First, Detective Schroeder exceeded the scope of Snapchat's private search when he opened the video because no Snapchat employee "eyeballed" the video first. (R. 56:3–5.) Second, it found that the MD-5 hash algorithm, which is not the algorithm that was used in this case (R. 60:26–27), is categorically unreliable because of the risk of collision and because it is "broken cryptographically" (R. 56:5–6). The circuit court did not address the reliability of PhotoDNA. It derived its "broken cryptographically" finding from visiting a website that the State provided in a footnote in its pre-hearing brief opposing suppression, rather than from any evidence offered at the suppression hearing. (R. 30:5 n.4; 56:6.) The order did not address any of Gasper's other suppression claims.

The State now appeals the order granting suppression.

---

[4] The Honorable Shelley J. Gaylord, retired Dane County circuit judge sitting as a Reserve Judge in Waukesha County.

ARGUMENT

I. Gasper lacked a reasonable expectation of privacy in a child pornography video that he uploaded to Snapchat in violation of Snapchat's terms of service.

The Fourth Amendment to the U.S. Constitution and Article I, § 11 of the Wisconsin Constitution protect against "unreasonable searches and seizures." *State v. Post*, 2007 WI 60, ¶ 10, 301 Wis. 2d 1, 733 N.W.2d 634. To challenge a search, "a defendant must have 'a legitimate expectation of privacy' in the area or items subjected to a search." *State v. Tentoni*, 2015 WI App 77, ¶ 7, 365 Wis. 2d 211, 871 N.W.2d 285 (citation omitted). This Court reviews the ultimate legal determination on this issue *de novo* and any underlying factual findings for clear error. *Id.* ¶ 6.

A defendant bears the burden of establishing a reasonable expectation of privacy. *State v. Bruski*, 2007 WI 25, ¶ 22, 299 Wis. 2d 177, 727 N.W.2d 503. The defendant must establish two elements by a preponderance of the evidence: (1) that he or she has an actual or subjective expectation "in the area searched and the item seized"; and (2) that society is willing to recognize that expectation of privacy as reasonable. *Id.* ¶ 23. Failure on either element dooms the defendant's motion to suppress. *See Baric*, 384 Wis. 2d 359, ¶ 18 n.5. "[T]he reasonableness of an expectation of privacy in digital files shared on electronic platforms is determined by considering the same factors as in any other Fourth Amendment context." *Id.* ¶ 19.

The circuit court did not address either the subjective or the objective inquiry. (R. 56:3–6.) Instead, it accepted without explanation Gasper's assertion that he had a reasonable expectation of privacy because he used a cell phone to access Snapchat, citing *Riley v. California*, 573 U.S. 373 (2014) and *Carpenter v. United States*, 138 S. Ct. 2206

(2018). (R. 56:3 & n.8; 60:205.) The circuit court erred because it analyzed the wrong "area" to be searched. The video was acquired from Gasper's Snapchat account, not his phone. That made Gasper's Snapchat account the relevant "area" that was searched.

This Court recently concluded that a person has a reasonable expectation of privacy in a cloud-storage account with an ESP in *State v. Bowers*, 2023 WI App 4, ¶¶ 26, 45, 405 Wis. 2d 716, 985 N.W.2d 123. In *Bowers*, it was undisputed that the relevant "area" was the account, not the device used by the defendant to access it. *See id.* ¶¶ 17, 20, 40. The account was a digital version of a physical storage container. *Id.* ¶ 26.

While *Bowers* held that an individual has a reasonable expectation of privacy in a password-protected cloud storage account, that expectation of privacy is not unlimited. Although not yet addressed by Wisconsin courts, then-Judge Gorsuch observed that an ESP's terms of service can circumscribe or dissolve a user's expectation of privacy in *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016).

In *Ackerman*, the defendant moved to suppress child pornography images that AOL had detected on the defendant's email and forwarded to NCMEC. *Id.* at 1294–95. While the district court assumed that the defendant had a reasonable expectation of privacy in the message and its attachments, Judge Gorsuch invited a second look. *Id.* at 1305. Judge Gorsuch directed the district court to consider "Mr. Ackerman's subjective expectations of privacy or the objective reasonableness of those expectations *in light of the parties' dealings* (e.g. the extent to which AOL regularly accessed emails and the extent to which users were aware of or acquiesced in such access)." *Id.* (emphasis added).

On remand, the district court concluded that AOL's terms of service precluded the defendant from establishing an objectively reasonable expectation of privacy in child pornography attached to an email. *United States v. Ackerman*, 296 F. Supp. 3d 1267, 1272–73 (D. Kan. 2017). The terms of service compelled this result because they barred the defendant from using AOL for illegal activity or posting explicit sexual acts. *Id.* at 1272. They also advised him that AOL could take technical, legal, or other actions to enforce the terms. *Id.* at 1272.[5]

Federal circuit courts have acknowledged *Ackerman* in analogous factual circumstances but have so far not addressed the reasonable expectation of privacy issue. *See United States v. Reddick*, 900 F.3d 636, 638 n.1 (5th Cir. 2018); *United States v. Miller*, 982 F.3d 412, 426–27 (6th Cir. 2020); *United States v. Bebris*, 4 F.4th 551, 562 (7th Cir. 2021); *United States v. Wilson*, 13 F.4th 961, 967 (9th Cir. 2021).

In noting this issue, however, nearly all of these courts have accepted *Ackerman*'s assertion that the answer turns on the "dealings" between the individual and the ESP, which will most often be memorialized in the ESP's terms of service. *See Reddick*, 900 F.3d at 638 n.1 (declining to decide reasonable expectation of privacy because "'the most useful evidence on which to make the determination' of whether Reddick's expectation of privacy was reasonable—'the end user agreement governing Reddick's use of Microsoft Skydrive'—is not in the record."); *Miller*, 982 F.3d at 427 (noting that "Google's terms of service" may limit the defendant's expectation of privacy); *Bebris*, 4 F.4th at 557 (stating that the

[5] The Tenth Circuit affirmed this decision in an unpublished decision on the basis of the good faith exception to the exclusionary rule. *See United States v. Ackerman*, 804 F. App'x 900, 905 (10th Cir. 2020).

district court determined that the defendant lacked a reasonable expectation of privacy based on Facebook's Community Standards and terms of service).

The "dealings" between Gasper and Snapchat as captured in Snapchat's written policies reveal that Gasper had neither a subjective nor an objectively reasonable expectation of privacy in child pornography files that he saved or uploaded to his account. Three documents in the record lead to this conclusion: (1) the "Snap Inc. Terms of Service" (the "TOS") (R. 41)[6]; (2) the "Community Guidelines" (R. 42); and (3) the "Sexual Content Community Guidelines Explainer Series" (the "Sexual Content Explainer") (R. 44).

The TOS forbids using Snapchat "in any way not expressly permitted by these Terms or [the] Community Guidelines." (R. 41:6.) By making an account, users allow Snapchat to "access, review, screen, and delete [their] content at any time and for any reason." (R. 41:4.) The section entitled "Safety" states that Snapchat "reserve[s] the right to remove any offending content, terminate or limit the visibility of your account, and notify third parties—including law enforcement—and provide those third parties with information relating to your account." (R. 41:7.) The TOS includes a hyperlink to the Community Guidelines. (R. 41:7; 60:56.)

The Community Guidelines absolutely prohibits "any activity that involves sexual exploitation or abuse of a minor." (R. 42:2.) Further, the Community Guidelines orders users to "[n]ever post, save, send, forward, distribute, or ask for nude or sexually explicit content involving anyone under the age of 18." (R. 42:2.) Snapchat vows to "report all instances of child

[6] Record Item 41 consists of two consecutive copies of the TOS.

sexual exploitation to authorities, including attempts to engage in such conduct." (R. 42:2.)

The Community Guidelines refers users and includes a hyperlink to the Sexual Content Explainer "[f]or more information about sexual conduct and content that violates [the] Community Guidelines." (R. 42:2.) The Sexual Content Explainer restates Snapchat's absolute prohibition on any content or activity related to the sexual exploitation of a child. (R. 44:1.) It also has a paragraph describing how it scans user accounts and reports child pornography to NCMEC, just as it did in the present case:

> Preventing, detecting, and eradicating Child Sexual Abuse Material (CSAM) on our platform is a top priority for us, and we continuously evolve our capabilities to address CSAM and other types of child sexually exploitative content. We report violations of these policies to [NCMEC], as required by law. NCMEC then, in turn, coordinates with domestic or international law enforcement, as required.

(R. 44:3.)

In light of these documents, Gasper cannot satisfy his burden to prove either his subjective or his objective expectation of privacy.

Gasper cannot prove his subjective expectation of privacy because he consented to these policies by making a Snapchat account. (R. 60:55–56.) He violated those terms by saving, sharing, or uploading a child pornography video to his account. (R. 41:6; 42:2; 44:3.) Snapchat informed him that it would be scanning and accessing his account for content that violated the TOS like child pornography and would report violations to law enforcement. (R. 41:4, 7; 42:2; 44:3.) Accordingly, Snapchat vitiated any subjective expectation of privacy Gasper might have had in child pornography saved to his account.

Gasper offered no evidence to support his subjective expectation of privacy other than the use of his phone. (R. 60:96.) Gasper did not testify or provide any affirmative evidence that he believed his account to be completely private notwithstanding those policies.[7] That argument would have been meritless anyway. He assented to Snapchat's policies when he made his account, the documents conveyed the prohibition on child pornography simply and succinctly, and Detective Schroeder demonstrated that a user had to affirmatively acknowledge the TOS to create an account. (R. 60:55–56.) Gasper therefore cannot carry his burden to prove his subjective expectation of privacy.

Snapchat's policies also prevent Gasper from proving an objectively reasonable expectation of privacy. This inquiry turns on the totality of the circumstances, including the following non-exclusive factors:

> (1) whether the accused had a property interest in the premises; (2) whether the accused is legitimately (lawfully) on the premises; (3) whether the accused had complete dominion and control and the right to exclude others; (4) whether the accused took precautions customarily taken by those seeking privacy; (5) whether the property was put to some private use; [and] (6) whether the claim of privacy is consistent with historical notions of privacy.

Bruski, 299 Wis. 2d 177, ¶ 24 (citation omitted).

This Court concluded in *Bowers* that these factors weighed in favor of the defendant's objectively reasonable expectation of privacy in his cloud storage account. *Bowers*, 405 Wis. 2d 716, ¶¶ 20–25. However, that reasoning does not fit the present case.

---

[7] Gasper attempted to submit this evidence through an affidavit without testifying, but the circuit court sustained the State's objection to it. (R. 60:140–46.)

For one, in *Bowers*, the State conceded that the first two factors favored the defendant: the defendant had a property interest in his account, and he maintained his account lawfully. *Id.* ¶ 20. Neither concession is warranted here. Snapchat limited Gasper's property interest in his account by the terms of the TOS, the Community Guidelines, and the Sexual Content Explainer, which clearly barred him from saving, sharing, or uploading child pornography to his account. That conduct was obviously unlawful. Accordingly, these factors weigh against Gasper.

The third factor, Gasper's level of dominion and control over his account, also weighs against a reasonable expectation of privacy. Even assuming that Gasper exercised exclusive control over his Snapchat account like the defendant in *Bowers*, 405 Wis. 2d 716, ¶¶ 21–22, the policies limited that control when it came to child pornography. Snapchat monitored accounts for content violations, reserved the right to access offending accounts, actively scanned for child pornography, and reported child pornography to the authorities. (R. 41:4, 7; 42:2 44:3.) Gasper, thus, could not exclude Snapchat from his account when it came to child pornography.

Assuming Gasper took precautions to secure his account for private use like using a password, *see Bowers*, 405 Wis. 2d 716, ¶¶ 23–24, the fourth and fifth factors still cut against him. Gasper, unlike Bowers, used his account to access content that violated both Snapchat's policies and the law. Snapchat expressly denied him permission, control, or privacy with respect to child pornography, no matter what precautions he took. These two factors favor the State as well.

Finally, there is no historical notion of privacy for items that have no lawful purpose like child pornography. *See United States v. Jacobsen*, 466 U.S. 109, 122 (1984) ("[A]n interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the

mere expectation, however well justified, that certain facts will not come to the attention of the authorities."); *Illinois v. Caballes*, 543 U.S. 405, 408–09 (2005) (reiterating *Jacobsen*).

Thus, all six factors weigh against an objectively reasonable expectation of privacy in child pornography saved or uploaded to Gasper's Snapchat account. The circuit court did not even consider these factors. It therefore erred and should be reversed.

The circuit court concluded that Gasper had a reasonable expectation of privacy because "[t]here is a legitimate privacy interest in cell phones." (R. 56:3.) As explained, this analysis does not comport with *Bowers*. It also dramatically expands *Riley* or *Carpenter* in a manner that invites absurd results.

In *Riley*, the U.S. Supreme Court observed that "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse." *Riley*, 573 U.S. at 393. These privacy concerns stem from the sensitive information kept on cell phones, their large storage size, and their even greater storage potential when combined with cloud storage. *Id.* at 393–98.

Snapchat's search did not implicate these broad privacy concerns. It merely used PhotoDNA to scan content within Gasper's Snapchat account without accessing or searching any of his devices or data stored outside Snapchat. Detective Schroeder viewed only the single video that Snapchat forwarded to NCMEC. (R. 60:54.)

Carpenter has virtually no bearing on this appeal. *Carpenter* narrowly held that a person has a reasonable expectation of privacy in cell-site location information (CSLI) and that the third-party doctrine's exception to the warrant requirement does not apply to CSLI. *Carpenter*, 138 S. Ct. at 2217, 2220. Because Gasper's CSLI is not at issue in the

present case, *Carpenter* is inapplicable. *See Miller*, 982 F.3d at 431.

If the circuit court were correct, it would cast doubt on prevailing Wisconsin law. For example, a person loses a reasonable expectation of privacy in text messages sent from his phone to another person's phone. *State v. Tentoni*, 2015 WI App 77, ¶¶ 11–12, 365 Wis. 2d 211, 871 N.W.2d 285. Yet under the circuit court's reasoning, the sender of the text message would have a claim to an expectation of privacy in text messages on a recipient's phone simply because he sent them with his own cell phone. Similarly, this reasoning would threaten the holding that there is no reasonable expectation of privacy in files made publicly available on a peer-to-peer network. *See Baric*, 384 Wis. 2d 359, ¶ 26. A defendant would be able to circumvent *Baric* simply by using a smart phone to access the peer-to-peer network.

* * * * *

The circuit court's principal error was hastiness. It assumed that the motion to suppress concerned a cell phone, cited *Riley*, and then jumped to the next issue. As the foregoing reveals, the circuit court's perfunctory analysis began and ended with a fatally erroneous premise. The relevant "area" that was searched was Gasper's Snapchat account, not his cell phone. Had the circuit court proceeded more methodically and carefully, it might have recognized how Snapchat's written policies precluded Gasper from establishing either his subjective or objective expectation of privacy. In addition, the circuit court may have appreciated the absurd results that would follow from its overly broad reading of *Riley*. Because the correctly applied analysis reveals that Gasper failed to establish a reasonable expectation of privacy in child pornography on his Snapchat account, this Court should reverse the order granting suppression.

II. The detective could lawfully open the video flagged and forwarded by Snapchat pursuant to the private-search doctrine.

Even if Gasper established a reasonable expectation of privacy, the circuit court still erred in granting his motion to suppress. Detective Schroeder did not violate the Fourth Amendment by opening the flagged video because the private-search doctrine applied.

"Private searches are not subject to the Fourth Amendment's protections because the Fourth Amendment applies only to government action." *State v. Payano-Roman*, 2006 WI 47, ¶ 17, 290 Wis. 2d 380, 714 N.W.2d 548. Whether a search is a private search or a government search presents a mixed question of law and fact. The circuit court's factual findings are reviewed for clear error, but the legal conclusion is reviewed *de novo*. *Id.* ¶ 16.

Payano-Roman identifies three criteria to gauge whether a private party conducts a private or government search. *Id.* ¶ 18. However, it is undisputed in this case that Snapchat did not act as a government agent. (R. 33:6; 60:195.) It is also immaterial to the present case whether NCMEC is a government agent because it did nothing more than Snapchat did.[8] *See Bebris*, 4 F.4th at 558 (noting that whether NCMEC was a government agent was immaterial since NCMEC merely forwarded the images flagged by the ESP to law enforcement).

The application of the private-search doctrine in the present case turns on whether Detective Schroeder expanded Snapchat's private search by opening the video. The relevant inquiry is: "Did the police search exceed the scope of the

[8] Federal circuit courts have divided on this issue. *Compare Ackerman*, 831 F.3d at 1295–1300 (categorizing NCMEC as a government entity) *with United States v. Meals*, 21 F.4th 903, 908–09 (5th Cir. 2021) (deeming NCMEC a non-government entity).

private search so as to further frustrate the defendant's expectation of privacy?" *State v. Cameron*, 2012 WI App 93, ¶ 25, 344 Wis. 2d 101, 820 N.W.2d 433.

Whether an investigator expands an ESP's private search by opening a file that the ESP flagged as child pornography based on the file's hash value and forwarded to law enforcement without reviewing it presents an issue of first impression in Wisconsin. Three federal courts have addressed this particular issue.[9] They are divided in their answers.[10] The Fifth Circuit in *Reddick* and the Sixth Circuit in *Miller* held that the investigator did not expand the search by opening the flagged file. The Ninth Circuit in *Wilson* concluded otherwise.

Other state courts have followed the reasoning in *Reddick* and *Miller* in the same circumstances. *See Walker v. State*, 669 S.W.3d 243, 252–55 & n.8 (Ark. Ct. App. 2023); *People v. Wilson*, 270 Cal. Rptr. 3d 200, 220–25 (Cal. Ct. App. 2020), *cert. denied* 142 S. Ct. 751 (2022); *Morales v. State*, 274 So.3d 1213, 1217–18 (Fla. Dist. Ct. App. 2019); *cf. State v. Harrier*, 475 P.3d 212, 215 (Wash. Ct. App. 2020) (holding that defendant lacked a reasonable expectation of privacy in

---

[9] *Ackerman* is factually distinguishable from the present case. In *Ackerman*, the ESP forwarded an image that it flagged as child pornography, as well as three images that had not been flagged and the email to which the images were attached. 831 F.3d at 1306–07. The investigator viewed all the images and the email. *Id.* at 1294. The Tenth Circuit concluded that the investigator expanded the private search doctrine because he viewed media that had not even been identified as child pornography by the ESP. *Id.* at 1306. It left for another day whether the result would have changed if the investigator had opened only the flagged image. *Id.*

[10] When an employee of the ESP *does* review the flagged file, federal courts agree that an investigator's review of the same file does not expand the private search. *See Bebris*, 4 F.4th at 562; *United States v. Ringland*, 966 F.3d 731, 737 (8th Cir. 2020); *United States v. Powell*, 925 F.3d 1, 6 (1st Cir. 2018).

contraband found by a private party). No state court has yet followed *Wilson*. This Court should join the states that have adopted the persuasive reasoning of *Reddick* and *Miller*.

A. The private-search doctrine applies when a private actor presents a container for inspection and provides the government agent a virtual certainty about its contents.

Two decisions from the U.S. Supreme Court continue to guide the analysis for when a government agent expands the scope of a private party's search.

In *Walter v. United States*, the Court suppressed the content of pornographic filmstrips that had been misdelivered to a company. 447 U.S. 649, 651–52 (1980) (lead opinion of Stevens, J.). Company employees had opened the packages and observed "suggestive drawings" and "explicit descriptions" on the boxes of filmstrips, but they never watched the films. *Id.* at 652. Instead, they gave the boxes to the FBI. *Id.* Agents then viewed the films over the next two months without first obtaining a warrant. *Id.* The Court ruled that "[t]he projection of the films" by the FBI agents "was a significant expansion of the search that had been conducted previously by a private party." *Id.* at 657. "Prior to the Government screening one could only draw inferences about what was on the films." *Id.*

In *Jacobsen*, on the other hand, the government agent did not exceed the private search when he reopened a package that Federal Express had damaged with a forklift. *Jacobsen*, 466 U.S. at 111, 118. Pursuant to company policy, employees opened the damaged package to examine the contents before preparing an insurance claim. *Id.* at 111. The package contained a tube concealed within newspaper. *Id.* The tube contained several plastic baggies of white powder. *Id.* Federal Express called the police, and agents from the Drug Enforcement Administration (DEA) responded. *Id.* Before the

DEA agents arrived, the Federal Express employees repackaged the box. *Id.* Upon arrival, a DEA agent reopened the package, reopened the tube, and tested the white powder in the baggies, which tested positive for cocaine. *Id.* at 111–12.

Jacobsen held that the DEA agent did not expand the private search because the defendants could not have retained a privacy interest in the package after the Federal Express employees had opened it, examined its contents, and invited the authorities to look at it. *Jacobsen*, 466 U.S. at 119. It did not matter whether the Federal Express employees "were accidental or deliberate" or "reasonable or unreasonable" in infringing the defendants' privacy. *Id.* at 115. "The agent's viewing of what a private party had freely made available . . . did not violate the Fourth Amendment." *Id.* at 119. The drug test was also lawful, even though it exceeded the scope of the private search, because the defendants had no legitimate privacy interest in whether or not the powder was cocaine. *Id.* at 123.

The holding in *Jacobsen* rested on "the virtual certainty that nothing else of significance was in the package." *Id.* at 119. The agent's reopening of the package "merely avoid[ed] the risk of a flaw in the employees' recollection, rather than in further infringing respondents' privacy." *Id.* This "virtual certainty" distinguished the package from the filmstrips in *Walter*, which supported only inferences about the contents of the films. *Compare Walter*, 447 U.S. at 657, *with Jacobsen*, 466 U.S. at 119. Consistent with that reasoning, federal courts have since recognized that a government agent does not exceed a private search of a container if the agent has a "virtual" or "substantial" certainty that the search will not reveal anything more than the private party has represented. *See United States v. Runyan*, 275 F.3d 449, 463 (5th Cir. 2001); *Rann v. Atchison*, 689 F.3d 832, 836–37 (7th Cir. 2012);

United States v. Lichtenberger, 786 F.3d 478, 488 (6th Cir. 2015).

Jacobsen declined to predicate the lawfulness of the DEA agent's actions on the plain-view doctrine. Justice White concurred in the judgment because he believed that the facts showed that the DEA agent found the tube holding the baggies of white powder in plain view. *Jacobsen*, 466 U.S. at 126–27 (White, J., concurring); *see also Walter*, 447 U.S. at 661–62 (White, J., concurring) (advancing the same position). The Court rejected Justice White's approach because it "would have this case turn on the fortuity of whether the Federal Express agents placed the tube back into the box." *Jacobsen*, 466 U.S. at 120 n.17 (majority opinion). The Court explained that "the precise character of the white powder's visibility to the naked eye is far less significant than the facts that the container could no longer support any expectation of privacy, and that it was virtually certain that it contained nothing but contraband." *Id.*

Cameron is the Wisconsin application of *Jacobsen* most analogous to the present case. In *Cameron*, the defendant's ex-girlfriend discovered physical copies of child pornography in a closet in the defendant's home. *Cameron*, 344 Wis. 2d 101, ¶ 3. She put the child pornography into a duffel bag and put the bag in her car. *Id.* She notified the police that she found what "she believed to be child pornography." *Id.* ¶ 4. The officer arrived, removed the bag from the car, opened it, and confirmed that it contained child pornography. *Id.* ¶ 5. This Court found "very little, if anything, to distinguish *Jacobsen* from this case." *Id.* ¶ 28. The ex-girlfriend "destroyed" the defendant's expectation of privacy by going through his belongings, putting the child pornography into a duffel bag, and presenting the bag to the police. *Id.* The officer's "viewing of what a private party had freely made available did not violate the Fourth Amendment." *Id.* ¶ 27 (emphasis omitted) (quoting *Jacobsen*, 466 U.S. at 119).

B. *Reddick* and *Miller* correctly concluded that an investigator may open a file that an ESP flagged as child pornography based on its hash value.

The Fifth Circuit in *Reddick* and the Sixth Circuit in *Miller* applied *Jacobsen*'s "virtual certainty" standard to conclude that the private-search doctrine applied in the same circumstances as the present case.

In *Reddick*, the Fifth Circuit concluded that the investigator did not expand Microsoft's private search by opening files flagged with PhotoDNA because "whatever expectation of privacy Reddick might have had in the hash values of his files was frustrated by Microsoft's private search." *Reddick*, 900 F.3d at 639. The court observed that "hash value comparison 'allows law enforcement to identify child pornography with almost *absolute certainty*' since hash values are 'specific to the makeup of a particular image's data.'" *Id.* (emphasis added) (citation omitted). The court equated opening the files to the drug test in *Jacobsen*, reasoning that "opening the file merely confirmed that the flagged file was indeed child pornography, as suspected." *Id.*

The Sixth Circuit in *Miller* reached the same conclusion but through slightly different reasoning. The Sixth Circuit deemed the search of the package to be the apt comparison from *Jacobsen*, not the drug test. *Miller*, 982 F.3d at 429. Like the Federal Express employees' prior search of the box, the hash value match from the ESP (Google) created a "virtual certainty" that the investigator would view child pornography upon opening the files. *Id.* at 428–30. "Google's technology 'opened' and 'inspected' the files, revealing that they had the same content as files that Google had already found to be child pornography." *Id.* at 431. The defendant never challenged the reliability of Google's hash matching technology. *Id.* at 430. Accordingly, "[t]his (unchallenged) information satisfies

Jacobsen's virtual-certainty test and triggers its private-search doctrine." *Id.*

Although *Reddick* and *Miller* differ in the analogue to be drawn from *Jacobsen*, both cases base their holding on the virtual certainty that the files opened by the investigators would contain nothing but child pornography. *See Reddick*, 900 F.3d at 639; *Miller*, 982 F.3d at 430. The investigators merely confirmed what the private party had already reported, just like the DEA agent in *Jacobsen*. *See Reddick*, 900 F.3d at 639–40; *Miller*, 982 F.3d at 429–31.

Miller made two additional observations germane to the present case. First, *Miller* explained that it would be absurd to treat hash value scanning technologies differently than human observations. A private individual can trigger the private-search doctrine simply with a "quick view" of a picture of child pornography before handing it to the police, "despite the 'risk of a flaw in the [person's] recollection.'" *Miller*, 982 F.3d at 430–31 (alteration in original) (quoting *Jacobsen*, 466 U.S. at 119). Based on that "quick view," an investigator would be able to examine the picture "more thoroughly." *Id.* at 431 (quoting *Runyan*, 275 F.3d at 464); *accord United States v. Simpson*, 904 F.2d 607, 610 (11th Cir. 1990); *United States v. Tosti*, 733 F.3d 816, 822 (9th Cir. 2013). "Common hash algorithms, by contrast, catalogue every pixel." *Miller*, 982 F.3d at 430. "What sense would it make to treat a more accurate search of a file differently?" *Id.* at 431.

Second, *Miller* rejected the argument that the doctrine could not apply because of the risk of the hash value matching technology misidentifying child pornography. *Id.* "Just because a private party turns out to be wrong about the legality of an item that the party discloses to police does not mean that the police violate the Fourth Amendment when they reexamine the item." *Id.*

C. The circuit court erred by failing to apply the private-search doctrine.

Four key principles about the private-search doctrine emerge from the foregoing caselaw. First, the doctrine applies when a private party "destroy[s]" the defendant's expectation of privacy and "freely ma[kes] available" for inspection the fruits of the private search. *Cameron*, 344 Wis. 2d 101, ¶¶ 27–28 (quoting *Jacobsen*, 466 U.S. at 119). Second, a government agent can open a container that a private party has freely made available for inspection if the officer has a "virtual certainty that nothing else of significance" will be found in it. *Jacobsen*, 466 U.S. at 119. Third, law enforcement may conduct a more thorough examination of the privately disclosed items than the private party. *See, e.g.*, *Miller*, 982 F.3d at 430–31. Fourth, it is immaterial whether the "private party turns out to be wrong about the legality of an item that the party discloses to police," *id.* at 431, or whether the private party's intrusion was "accidental or deliberate," or "reasonable or unreasonable," *Jacobsen*, 466 U.S. at 115.

Applying these four principles in the present case reveals that the circuit erred in granting Gasper's motion to suppress.

1. Snapchat destroyed Gasper's expectation of privacy by scanning his account with PhotoDNA.

Snapchat destroyed Gasper's expectation of privacy in the child pornography video by scanning it with PhotoDNA, labeling it as "Apparent Child Pornography" (R. 38:1, 4; 60:24–25), and forwarding it to NCMEC. (R. 60:37–38.) The PhotoDNA scan was equivalent to opening and inspecting Gasper's files. *See Miller*, 982 F.3d at 431. Snapchat "freely made [the video] available" for inspection by sending it to NCMEC, which then sent it to Wisconsin law enforcement. *Cameron*, 344 Wis. 2d 101, ¶ 27 (quoting *Jacobsen*, 466 U.S.

at 119). Snapchat effectively did digitally what the ex-girlfriend in *Cameron* did physically: it searched a space held by Gasper on its own volition, found what it "believed to be child pornography," and invited law enforcement to examine what had been found. *Id.* ¶¶ 3–4, 28. Whatever expectation of privacy Gasper had in the video "was frustrated by [Snapchat's] private search." *Reddick*, 900 F.3d at 639.

Thus, Snapchat triggered the private-search doctrine by scanning Gasper's child pornography video with PhotoDNA and making it available for inspection by law enforcement.

2. Detective Schroeder could open the flagged video without a warrant because he had a virtual certainty that it contained nothing but the reported child pornography.

Detective Schroeder did not need a warrant to open the flagged video because he had a virtual certainty that the file contained nothing but child pornography.

The CyberTip helped establish a virtual certainty by virtue of its inherent reliability. Snapchat was required by federal law to report the video to NCMEC. *See Silverstein*, 378 Wis. 2d 42, ¶ 5 & n.3. As this Court noted approvingly in *Silverstein*, courts in other jurisdictions "have held that this obligation itself heightens the reliability of the tip." *Id.* ¶ 19. Moreover, in *Silverstein*, the CyberTip was reliable enough to help establish probable cause in a warrant. *Id.* ¶¶ 22–26 & n.12.

The CyberTip in the present case provided Detective Schroeder a virtual certainty of what he would see in the video. Snapchat had identified a single video as "apparent child pornography" with PhotoDNA. (R. 38:1; 60:24–25.) Detective Schroeder knew that PhotoDNA could detect slightly altered copies of known child pornography files.

(R. 60:22.) The CyberTip informed him that, since neither Snapchat nor NCMEC opened the video, the flagged video was a "'Hash Match' of one or more uploaded files to visually similar files that were previously viewed and categorized by NCMEC." (R. 38:5; 60:86–87.) He knew that Snapchat locked Gasper's account shortly after reporting the video. (R. 60:52.) Given this information, Detective Schroeder had a virtual certainty that the video contained nothing but child pornography.

Detective Schroeder also had personal experience with the reliability of CyberTips. He had never received a false positive in a CyberTip in about 100 child pornography investigations. (R. 60:66.) Accordingly, he expected "to open child sexual abuse material when [he] click[ed] on that video." (R. 60:67.) He also knew that he received *nothing else* from Snapchat that could be something other than child pornography. (R. 60:54.)

By opening the video, Detective Schroeder merely guarded against the risk of an erroneous report and engaged in a more thorough examination of the video than Snapchat—both of which are permissible under the private-search doctrine. *See Jacobsen*, 466 U.S. at 119; *Reddick*, 900 F.3d at 639–40; *Miller*, 982 F.3d at 430–31. Stated another way, he did not exceed Snapchat's private search when he opened a video that Snapchat claimed was child pornography and had made available for his inspection. Thus, the record "satisfies *Jacobsen*'s virtual-certainty test and triggers its private-search doctrine." *Miller*, 982 F.3d at 430.

The circuit court erroneously read *Jacobsen* to require a human to "eyeball" the contraband in order to trigger the private-search doctrine. (R. 56:2–5.) In effect, the circuit court adopted Justice White's plain-view approach that *Jacobsen* rejected. The circuit court would have the result "turn on the fortuity of whether" an ESP employee viewed the flagged image before reporting it. *Jacobsen*, 466 U.S. at 120 n.17.

Jacobsen, however, disclaimed the importance of "the white powder's visibility to the naked eye" compared to the significance of "the facts that the container could no longer support any expectation of privacy, and that it was virtually certain that it contained nothing but contraband." *Id.* Both of those significant facts were present here.

It would be irrational for the circuit court's "eyeball" requirement to be the law. As *Miller* observed, a person's "quick view" of a picture of child pornography is sufficient to trigger the private-search doctrine. *Miller*, 982 F.3d at 431. It makes little sense to treat the more thorough pixel-by-pixel analysis offered by hash value technology differently than an individual person's cursory glance. *See id.*

It is immaterial that Snapchat reported the video as "Apparent Child Pornography." (R. 38:1.) Both *Jacobsen* and *Cameron* applied the private-search doctrine notwithstanding the risk of private party error. In *Jacobsen*, "the risk of a flaw in the employees' recollection" actually supported applying the private-search doctrine. *Jacobsen*, 466 U.S. at 119. In *Cameron*, the defendant's ex-girlfriend's report that she found what "she *believed* to be child pornography" was sufficient to trigger the doctrine. *Cameron*, 344 Wis. 2d 101, ¶ 4 (emphasis added).

Accordingly, Detective Schroeder could open the video without a warrant because he had a virtual certainty that it contained nothing but child pornography.

3. The reliability of PhotoDNA is immaterial to the private-search doctrine, but the record established its reliability anyway.

The circuit court also granted the motion to suppress because it concluded that the MD-5 hash algorithm—which Snapchat did not use to identify the video in Gasper's account—is unreliable. It found that the risk of "collision"—

two different files having the same hash value—precluded the private-search doctrine from applying. (R. 56:5–6.) It erred in so reasoning both because the reliability of hash values is immaterial to the private-search doctrine and because its finding of unreliability is clearly erroneous for at least two reasons.

Despite *Miller*'s reliance on the unchallenged reliability of the hash value matching technology, *Miller*, 982 F.3d at 430, no court had previously made the private party's reliability a prerequisite to the private-search doctrine. To the contrary, in *Jacobsen*, "the risk of a flaw in the employees' recollection" justified the DEA agent's reopening of the package. *Jacobsen*, 466 U.S. at 119. Similarly in *Cameron*, this Court did not suggest that the investigator's authority to open the duffel bag was limited by the ex-girlfriend's mere "belie[f]," rather than certitude, that she had discovered child pornography. *Cameron*, 344 Wis. 2d 101, ¶ 4.

Even *Miller* rejected the circuit court's particular reliability argument. The circuit court's concern with collision was "that the suspected image may contain innocuous material." (R. 56:5.) *Miller* squarely rejected this argument: "Just because a private party turns out to be wrong about the legality of an item that the party discloses to police does not mean that the police violate the Fourth Amendment when they reexamine the item." *Miller*, 982 F.3d at 431. This statement aligns with *Jacobsen*'s pronouncement that it does not matter whether the private party's intrusion is "accidental or deliberate," or "reasonable or unreasonable." *Jacobsen*, 466 U.S. at 115. What matters is that the private party "destroyed" the defendant's expectation of privacy. *Cameron*, 344 Wis. 2d 101, ¶ 28; *see Jacobsen*, 466 U.S. at 115. Accordingly, it was legal error for the circuit court to base suppression on the alleged unreliability of hash values.

Moreover, the finding of unreliability is clearly erroneous for two reasons. First, MD-5 is not relevant. Snapchat detected the video in Gasper's account using PhotoDNA, not MD-5. (R. 60:24–26.) Even if MD-5 is categorically unreliable, that finding is therefore insufficient to reject the hash match obtained by PhotoDNA in the present case.

Second, even if the reliability of MD-5 or PhotoDNA mattered, and even if MD-5 had been used in this case, the circuit court clearly erred by finding MD-5 technology unreliable due to the risk of collision. The record does not support that finding. The only evidence regarding hash value collision came from Detective Schroeder. He acknowledged the theoretical risk but explained that collisions had only ever been observed in laboratory settings with extremely small-sized files. (R. 60:148–49.)[11] He observed no evidence of hash value collision in this case and was not familiar with collisions afflicting PhotoDNA. (R. 60:139, 150.) The record is otherwise silent on the topic of collisions for the MD-5 algorithm. Gasper did not even call an expert to advance this theory as at least one federal defendant did in a failed attempt to assail hash value matching. *See United States v. Cartier*, 543 F.3d 442, 446 (8th Cir. 2008).

In contrast with this paucity of evidence regarding collision, Detective Schroeder provided a sound basis for PhotoDNA's reliability. He explained how PhotoDNA addresses a limitation of hash values. It can detect very slightly altered copies of existing child pornography files

---

[11] Detective Schroeder testified consistent with the evidence in *Miller* in which one source calculated the risk of hash value collision as "1 in 9.2 *quintillion*." *Miller*, 982 F.3d at 430; *see also* Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38, 40 n.8 (2005) ("It is extremely unlikely that collisions would happen in the wild, much less in the context of digital media imaging and forensics.").

because it divides the image into pieces and generates a hash value for each piece. (R. 60:22, 24, 29.) It uses all of the pieces as a means of comparison rather than just the file's MD-5 hash value. (R. 60:24, 29.) In his experience, every PhotoDNA tip that he has reviewed has been accurate. (R. 60:66–69.)

The circuit court offered a second reason to find MD-5 unreliable that was completely divorced from the record—the fact that it is "broken cryptographically." (R. 56:6.) It plucked that expression from a website cited in the State's pre-hearing brief to provide background information on the MD-5 hashing algorithm. (R. 30:5 n.4.) The issue was not addressed at the suppression hearing. The circuit court appeared to believe that the susceptibility of MD-5 to hacking creates the risk of collision. However, it offered no explanation for how hacking might create a collision that has so far only ever been observed in laboratory environments with artificially small files. (R. 60:148–49.) The record provides no further clues.

Thus, the reliability of MD-5 or PhotoDNA does not matter to the application of the private-search doctrine. Even if it does, the evidence in the record establishes PhotoDNA's reliability, and the circuit court clearly erred by finding to the contrary.

* * * * *

In sum, Snapchat destroyed Gasper's expectation of privacy in the child pornography video in his account and made it available for inspection by law enforcement. Detective Schroeder had a virtual certainty that the forwarded video contained nothing but child pornography as Snapchat reported. The reliability of PhotoDNA was both immaterial and established by the record. The circuit court therefore should have denied Gasper's motion to suppress based on the private-search doctrine.

D. The Ninth Circuit's decision in *Wilson* is unpersuasive.

The Ninth Circuit's decision in *Wilson* concluded that the investigator did expand the ESP's private search by opening files that the ESP had flagged but not reviewed. *Wilson*, 13 F.4th at 979–80.[12] The Ninth Circuit reasoned that the investigator obtained additional information by opening the images—namely the ability to describe the child pornography in the files. *Id.* at 972–74. It held further that even if the government could prove that the defendant possessed duplicates of files previously viewed and categorized as child pornography, the defendant still had an expectation of privacy in *his* personal copies of those files. *Id.* at 974–76. This Court should deem *Wilson* unpersuasive and decline to follow it.

First, *Wilson* misread *Jacobsen* in the same manner as the circuit court. It applied Justice White's plain-view approach that *Jacobsen* rejected, having the private-search doctrine "turn on the fortuity of whether" an employee of the ESP viewed the flagged image before forwarding it to NCMEC. *Jacobsen*, 466 U.S. at 120 n.17; *see Wilson*, 13 F.4th at 972–73. As discussed previously, *Jacobsen* imposed a "virtual certainty" standard, not an "eyeball" requirement.

Second, *Wilson* misread *Walter* by citing it for the proposition that an investigator expands a private search any time he gains "additional information" not obtained from the private search. *See Wilson*, 13 F.4th at 973–74. In *Walter*, the Supreme Court concluded that the FBI agents exceeded the private search not because they gained "additional information" by viewing the films, but because they had only an inference—not a virtual certainty—about what the

[12] On the same facts and with the same defendant, the California Court of Appeals reached a contrary conclusion. *See Wilson*, 270 Cal. Rptr. 3d at 220–25.

filmstrips depicted before viewing them. *See Walter*, 447 U.S. at 657. *Wilson*'s reading runs directly counter to the numerous courts—including *Tosti* in the Ninth Circuit itself—that have recognized that a government officer may examine the fruits of a private search more thoroughly than the private party. *See Miller*, 982 F.3d at 431; *Runyan*, 275 F.3d at 464; *Simpson*, 904 F.2d at 610; *Tosti*, 733 F.3d at 822. The dispositive issue is whether there is a "virtual certainty that nothing else of significance" was in the flagged files, not whether law enforcement learned additional information. *Jacobsen*, 466 U.S. at 119.

Finally, in emphasizing the "personal" nature of Fourth Amendment rights, the Ninth Circuit erected a strawman. *Wilson* rejected the private-search doctrine because, in its view, the defendant "ha[d] an expectation of privacy in *his* files, even if others had identical files." *Wilson*, 13 F.4th at 975. The circuit court adopted this reasoning. (R. 56:5.) This characterization, however, misstated the basis for the private-search doctrine. Detective Schroeder did not infer that Gasper had broken the law based on some other person's possession of child pornography. Rather, he had a "virtual certainty" that the video flagged by Snapchat in *Gasper's personal account* contained nothing but child pornography. Because Snapchat had already invaded Gasper's privacy and because of that virtual certainty, the Fourth Amendment—and whatever personal rights came with it—did not apply.

For these reasons, *Wilson* is unpersuasive.

* * * * *

The circuit court cloaks its order in the appearance of judicial humility, purporting not to apply the private-search doctrine because the U.S. Supreme Court has not yet dictated that result in these circumstances. (R. 56:1, 5–6.) This Court should not be so fooled.

Unlike every other state court to have considered this issue in these particular circumstances, the circuit court followed *Wilson* instead of *Reddick* and *Miller*—even though only *Reddick* and *Miller* correctly applied *Jacobsen*. Unlike every court to consider the role of hash values—including *Wilson* and this Court in *Baric*—the circuit court categorically rejected the entire technology. In forging ahead alone, the circuit court makes it harder for law enforcement to open a single digital file flagged by software specifically designed to identify child pornography than a duffel bag that one person reports as containing child pornography.

The circuit court's unprecedented order has dramatic consequences. In 2022, Wisconsin DOJ investigated 7,039 CyberTips, which amounted to a 740 percent increase in CyberTips since 2013.[13] According to the circuit court, law enforcement will need to obtain thousands of warrants just to *open* the files received through CyberTips each year. (R. 56:5.) This avalanche of warrant applications will grind both law enforcement agencies and the courts charged with reviewing warrant applications to a halt.

The Supreme Court's silence does not compel the circuit court's order. The private-search doctrine applies to this case based on a faithful application of *Jacobsen*. The circuit court erred in concluding otherwise. This Court should reverse.

---

[13] Wisconsin DOJ, *AG Kaul, Wisconsin ICAC Task Force Highlight Safer Internet Day* (Feb. 7, 2023) https://www.doj.state.wi.us/news-releases/ag-kaul-wisconsin-icac-task-force-highlight-safer-internet-day (last accessed Feb. 8, 2024).

III. Even if a Fourth Amendment violation occurred, the good faith exception to the exclusionary rule applies.

Even if the private-search doctrine does not apply, the circuit court's suppression order should still be reversed as to the evidence obtained via the search warrant pursuant to the good faith exception to the exclusionary rule. In its order, the circuit court erroneously asserted that the State did not raise this issue. (R. 56:4.) The State raised this issue at the suppression hearing. (R. 60:170.)

The application of the good faith exception raises an issue of law reviewed *de novo*. *State v. Scull*, 2015 WI 22, ¶ 17, 361 Wis. 2d 288, 862 N.W.2d 562. The State bears the burden of establishing "good faith" reliance on a search warrant. *United States v. Leon*, 468 U.S. 897, 924 (1984).

The exclusionary rule "operates as 'a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than [as] a personal constitutional right of the party aggrieved.'" *Leon*, 468 U.S. at 906 (citation omitted). "[S]uppression of evidence obtained pursuant to a warrant should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion will further the purposes of the exclusionary rule." *Id.* at 918.

The "good faith" exception to the exclusionary rule provides that evidence obtained by a police officer through a search warrant is admissible in evidence—despite inadequate probable cause or technical insufficiency—so long as the officer acted in "objectively reasonable" reliance upon the warrant. *Leon*, 468 U.S. at 919; *State v. Eason*, 2001 WI 98, ¶ 74, 245 Wis. 2d 206, 629 N.W.2d 625.

To assist courts in applying the "good faith" exception, the Supreme Court in *Leon* identified the following four situations in which "good faith" *should not* be recognized: (1)

if the magistrate was intentionally misled by false information in an affidavit; (2) if the magistrate acted as a "rubber stamp" for the State; (3) if the affidavit was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; and (4) if the warrant so "fail[ed] to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid." *Leon*, 468 U.S. at 923.

The Wisconsin Supreme Court added two additional requirements: whether "the process used in obtaining the search warrant included [1] a significant investigation and [2] a review by either a police officer trained and knowledgeable in the requirements of probable cause and reasonable suspicion, or a knowledgeable government attorney." *Eason*, 245 Wis. 2d 206, ¶ 74.

None of the circumstances identified in *Leon* counsel against applying the exception. After opening the video, Detective Schroeder prepared a detailed, 11-page affidavit in support of his warrant application that led to the issuance of a facially valid search warrant. (R. 6:9–22.) The issuing authority was neutral and detached. All of the information was accurate. The warrant and warrant application specified Gasper's home as the subject of the search and individually listed the electronic devices to be seized. (R. 6:4–5, 9–11.)

The only potential flaw in the otherwise thoroughly supported warrant was Detective Schroeder's reliance on viewing the video from the CyberTip. (R. 6:21.) However, neither Detective Schroeder nor the issuing authority could have known with certainty that it was unlawful for Detective Schroeder to open the video. The issue is unsettled in Wisconsin. *Reddick*, *Miller*, and several state courts have held that it was lawful to open the video. Only *Wilson* ruled otherwise. Detective Schroeder had, in fact, been trained on this area of law and been informed that he did not have to follow *Wilson*. (R. 60:154–55.) Given the silence of Wisconsin

law and the clear weight of authority from other jurisdictions, it was reasonable for Detective Schroeder to apply for a search warrant based on viewing the video and for the issuing authority to grant it. *See Scull*, 361 Wis. 2d 288, ¶ 30 ("Given the precedent, the commissioner's decision to grant the warrant appears to be a reasonable application of the unsettled law at the time the warrant issued.").

The Wisconsin-specific requirements for the exception are also met. The affidavit in support of the search warrant reveals that Detective Schroeder undertook a "significant investigation." He obtained Gasper's name and home address from the administrative subpoena. (R. 6:20–21.) He confirmed that Gasper still occupied the home by consulting four other sources. (R. 6:22.) He parked outside Gasper's home to verify that the available Wi-Fi signals were locked and not accessible by people outside the home. (R. 6:22.) The second Wisconsin-specific requirement is satisfied because Waukesha County Assistant District Attorney Kristina Gordon reviewed and approved the warrant application for legal sufficiency. (R. 6:23.)[14]

Accordingly, the good faith exception to the exclusionary rule should apply. The child pornography evidence should not be suppressed.

[14] Although the signature does not make the name clear, the state bar identification number is legible and belongs to ADA Gordon.

CONCLUSION

This Court should reverse the order granting Gasper's motion to suppress and remand for further proceedings.

Dated: March 18, 2024

Respectfully submitted,

JOSHUA L. KAUL
Attorney General of Wisconsin

Electronically signed by:

Michael J. Conway
MICHAEL J. CONWAY
Assistant Attorney General
State Bar #1134356

Attorneys for Plaintiff-Appellant

Wisconsin Department of Justice
Post Office Box 7857
Madison, Wisconsin 53707-7857
(608) 267-8910
(608) 294-2907 (Fax)
conwaymj@doj.state.wi.us

FORM AND LENGTH CERTIFICATION

I hereby certify that this brief conforms to the rules contained in Wis. Stat. § (Rule) 809.19(8)(b), (bm) and (c) for a brief produced with a proportional serif font. The length of this brief is 10,621 words.

Dated: March 18, 2024.

Electronically signed by:

Michael J. Conway
MICHAEL J. CONWAY
Assistant Attorney General

CERTIFICATE OF EFILE/SERVICE

I certify that in compliance with Wis. Stat. § 801.18(6), I electronically filed this document with the clerk of court using the Wisconsin Appellate Court Electronic Filing System, which will accomplish electronic notice and service for all participants who are registered users.

Dated: March 18, 2024.

Electronically signed by:

Michael J. Conway
MICHAEL J. CONWAY
Assistant Attorney General