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

REPLY BRIEF 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

Other Authority

INTRODUCTION

Defendant-Respondent Michael Joseph Gasper's response brief illustrates the legal adage as expressed by poet Carl Sandburg: "'If the law is against you, talk about the evidence,' said a battered barrister. 'If the evidence is against you, talk about the law, and, since you ask me, if the law and the evidence are both against you, then pound on the table and yell like hell.'"[1]

Without the facts or law on his side, Gasper pounds and yells, offering a series of arguments that are too clever by half and that fail to withstand cursory scrutiny. This Court should reverse the lower court's order granting his motion to suppress.

ARGUMENT

I. Gasper has failed to establish a reasonable expectation of privacy in the child pornography video in his Snapchat account.

A. The State had no burden to prove a warrant exception.

While acknowledging his burden to prove that he had a subjective and objectively reasonable expectation of privacy in the child pornography video in his Snapchat account, Gasper maintains that the State nevertheless had to prove an exception to the warrantless search. (Gasper's Br. 21, 24–25.) Gasper puts the cart before the horse.

If an inspection "does not intrude upon a legitimate expectation of privacy, there is no 'search' subject to the Warrant Clause." *Illinois v. Andreas*, 463 U.S. 765, 771 (1983); *accord Minnesota v. Dickerson*, 508 U.S. 366, 375

[1] Carl Sandburg, *The People, Yes* 181 (Harcourt, Brace & Co. 1936).

(1993). If Gasper cannot prove a reasonable expectation of privacy, the Fourth Amendment does not apply, obviating the State's duty to prove a warrant exception. *See Andreas*, 463 U.S. at 773. Gasper cannot avoid his burden to prove a reasonable expectation of privacy by prematurely discussing warrant exceptions.

B. Gasper has not identified any evidence with which to prove his subjective expectation of privacy.

Gasper claims that he established his subjective expectation of privacy through Detective David Schroeder's affidavit in support of the search warrant and through an affidavit that he personally completed. (Gasper's Br. 21–22.) Neither is sufficient.

Gasper cites the search warrant's affidavit because it established that his home's Wi-Fi connection was password protected. (Gasper's Br. 21 (citing R. 45:18).) While this fact may establish Gasper's subjective expectation of privacy in his home internet connection, it has no bearing on his Snapchat account.

Gasper's personal affidavit is insufficient because the lower court ruled it inadmissible. (R. 60:144, 146). The ruling was not ambiguous: "[Y]ou can either rest with argument that [the State] ha[sn't] provided any proof that it was in a public forum or you can call [Gasper] as a witness. But I think the affidavit is entirely self-serving and therefore not reliable, so you make a choice." (R. 60:144.) Gasper accepted the ruling but read the affidavit into the record as an offer of proof. (R. 60:144–46.) Gasper now improperly uses this offer of proof as substantive proof of his subjective expectation of privacy. (Gasper's Br. 21–22.) He obviously cannot rely on inadmissible evidence.

C. *Riley* does not apply because Snapchat did not search Gasper's cell phone.

Gasper stakes his entire theory of an objectively reasonable expectation of privacy on the privacy interest in cell phones recognized by *Riley v. California*, 573 U.S. 373 (2014). (Gasper's Br. 19–25, 38–41.) Although he acknowledges that Snapchat scanned his Snapchat account, he argues that Snapchat conducted a *de facto* search of his phone because he always used his phone to access Snapchat. For factual support, he relies entirely on the fact that all of his charges arose from his cell phone. (Gasper's Br. 21 (citing R. 60:96.) Try as he might, Gasper cannot bring his case within *Riley*'s ambit.

The location of the media files is irrelevant to Gasper's theory of suppression. It is true that all 10 media files for which the State charged Gasper were extracted from Gasper's cell phone pursuant to a search warrant—including the video flagged in the CyberTip. (R. 2:11.) However, the lawfulness of that extraction or the search warrant had nothing to do with the lower court's suppression order. The lower court ordered suppression because it agreed with Gasper that a Fourth Amendment violation occurred *before* Detective Schroeder even applied for the search warrant. It ruled that Detective Schroeder needed a warrant to open the video in the CyberTip, and it suppressed the nine other media files as fruit of the poisonous tree. (R. 56:1, 5.) Thus, the theory of suppression advanced by Gasper and accepted by the lower court had nothing to do with a search of Gasper's phone. (R. 23:2–3; 56:1.)

In addition, Gasper's reasoning, like the lower court's, is flawed. Snapchat's scan of his account was not tantamount to a cell phone search. *Riley* premised its holding on the fact that modern cell phones hold a virtually limitless amount of information, much of it sensitive in one hand-held device. *Riley*, 573 U.S. at 393–98. *Riley*'s logic does not apply in

reverse to any data accessed by a cell phone. The privacy concerns implicated by a search of a modern cell phone do not arise from searching a defined set of data held outside a phone. *See United States v. Bah*, 794 F.3d 617, 632 (6th Cir. 2015). *Riley*'s holding centered entirely on the technological features of a cell phone, not the data that users accessed with it.

This Court understood this distinction in *State v. Bowers*, 2023 WI App 4, 405 Wis. 2d 716, 985 N.W.2d 123. *Bowers* concluded that the defendant had a reasonable expectation of privacy in his Dropbox account, "a cloud-based storage center, [that] can be accessed from one device or a thousand devices." *Id.* ¶ 27 (alteration in original) (citation omitted). That conclusion turned on the features of the Dropbox account, not the device that Bowers used to access it. *See id.* ¶¶ 19–27, 40–42. Indeed, this Court rejected the State's argument that Bowers had a reduced expectation of privacy in the account because he used his county government email to register for it. *Id.* ¶¶ 22, 42. This Court explained that the county "did not search its own devices to access the information in Bowers' Account; it used the internet as a tool to access the outside server on which the Account was located." *Id.* ¶ 42. Here, Snapchat scanned the data held on its own servers and identified the child pornography video in Gasper's account without accessing any of his devices.

D. Gasper mischaracterizes the State's argument regarding Snapchat's policies.

Gasper believes that the State argues that no search warrant was required because the content at issue was child pornography, and that Gasper waived his Fourth Amendment rights by accepting Snapchat's Terms of Service. (Gasper's Br. 24–26.) Gasper misunderstands the State's argument.

The Fourth Amendment never applied in the first place because Gasper never had a reasonable expectation of privacy in the child pornography video. Snapchat's policies informing Gasper that it banned such videos, actively scanned for them, and reported them to law enforcement as a matter of policy precluded Gasper from establishing a subjective or objectively reasonable expectation of privacy in the video. As explained in Section I.A, *supra*, that means the Fourth Amendment never applied to the video. *See State v. Bruski*, 2007 WI 25, ¶ 46, 299 Wis. 2d 177, 727 N.W.2d 503. This argument does not turn solely on the unlawfulness of the child pornography—although that is one of several factors making Gasper's alleged subjective expectation of privacy objectively unreasonable. *See id.* ¶ 24.

The State hesitates to dignify Gasper's related argument that the Ninth Circuit's decision in *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021) is *binding* on Wisconsin courts by virtue of Snapchat's choice-of-law provision in its Terms of Service. (Gasper's Br. 26–28.) The argument is obviously frivolous. Wisconsin courts are not bound by any federal court other than the U.S. Supreme Court's interpretations of federal law. *See Alberte v. Anew Health Care. Svcs.*, 232 Wis. 2d 587, 591, 605 N.W.2d 515 (2000). The Terms of Service govern only the contractual relationship between Gasper and Snapchat in any potential civil action between them. (R. 41:1.) No such action is at issue here, and this private contract does not and cannot displace Wisconsin law in a criminal action brought by the State.

Moreover, even if Gasper were correct, he would *lose*. If California law applied, he would be bound by the decisions from California state court, not the Ninth Circuit. The California Court of Appeals already addressed these issues in an appeal stemming from a parallel state prosecution of the *Wilson* defendant. *People v. Wilson*, 270 Cal. Rptr. 3d 200 (Cal. Ct. App. 2020). The California Court of Appeals held

that the private-search doctrine applied and rejected Wilson's contrary argument based on *Riley*. *See Wilson*, 270 Cal. Rptr. at 218–25. Gasper cannot even prevail on this entirely fantastical argument.

II. Gasper fails to rebut the State's private-search doctrine argument.

A. The lower court did not err in finding that it was undisputed that Snapchat used PhotoDNA.

Gasper insists that the record does not establish that Snapchat identified the video in his account using PhotoDNA. (Gasper's Br. 13–16.) This argument is mystifying because the lower court deemed this fact undisputed. (R. 56:1–2.) That places Gasper in the unusual position of a Respondent arguing that the lower court clearly erred in reaching a factual finding. *See Bruski*, 299 Wis. 2d 177, ¶ 19. He falls well short of meeting that substantial burden.

Detective Schroeder clearly testified that Snapchat used PhotoDNA to detect the video in Gasper's account. (R. 60:24–25.) He drew this fact from the "Additional Information" section on page 4 of the CyberTip. (R. 60:26 (citing R. 38:4).) The relevant passage reads: "fileViewedByESP = false indicates that the reported media was detected by PDNA hash matching technology and was reported without review by a Snap team member." (R. 38:4.) "[F]alse," Detective Schroeder explained, refers to the fact that no Snapchat employee—the reporting ESP—reviewed the child pornography video. (R. 60:26.) He noted that the previous page also conveyed that fact in more conventional English: "Did Reporting ESP view entire contents of uploaded file? No." (R. 38:3; 60:26.) Since no human reviewed the file, "the reported media was detected by PDNA hash matching technology." (R. 38:4.) Detective Schroeder explained that "PDNA" is an abbreviation for PhotoDNA. (R. 60:26.)

For some reason, Gasper believes that "false" refers to "the use of PhotoDNA." (Gasper's Br. 16.) That interpretation runs directly contrary to Detective Schroeder's testimony and to a reasonable understanding of the CyberTip.

Gasper maintains that, actually, Snapchat used MD5 hash matching because the CyberTip provided an MD5 hash value for the reported video. (Gasper's Br. 13–15 (citing R. 38:7).) Again, Gasper completely misreads the record. Detective Schroeder explained that the CyberTip provided the MD5 hash value for the flagged video, but that PhotoDNA had identified it in a manner distinct from a one-to-one MD5 hash value match. (R. 60:26–27.)

For the sake of clarity, the lower court asked Detective Schroeder to confirm that PhotoDNA, not MD5, had detected the video. Detective Schroeder obliged.

> THE COURT: Well, I just want to be clear. There was an MD5 and PhotoDNA both for this?
>
> THE WITNESS: In their report, they report the MD5 hash value of the actual reported image.
>
> THE COURT: Did they report PhotoDNA or not?
>
> THE WITNESS: They're saying it was used to detect this image, yes.
>
> THE COURT: That's the sole thing that was used was PhotoDNA?
>
> THE WITNESS: To my understanding, yes.

(R. 60:30–31.)

Shortly thereafter, the lower court obtained a second confirmation from Detective Schroeder that PhotoDNA had been used:

> THE COURT: . . . My question is, what was used to detect this? PhotoDNA that was converted to hash values or hash values and PhotoDNA?
>
> THE WITNESS: PhotoDNA.
>
> THE COURT: Thank you.

(R. 60:31.)

Taking all of this evidence together, Gasper has failed to show that the lower court clearly erred by finding that Snapchat used PhotoDNA—particularly when Gasper did not dispute that fact below.

Even more baffling, Gasper repeatedly states that artificial intelligence detected the video. The record and the lower court's findings do not even mention artificial intelligence. It is unclear why Gasper believes otherwise. Regardless, he is incorrect.

B. Although Analyst Lochowitz viewed the video first, that fact is immaterial to the application of the private-search doctrine.

Gasper is correct that the State erroneously stated that Detective Schroeder was the first agent of the State to open the video. (Gasper's Br. 17, 24, 36–37.) In fact, Analyst Matthew Lochowitz opened it first. (R. 60:38–40.) The State regrets the oversight.

However, that fact is immaterial to the private-search doctrine issue. The dispositive legal question remains whether the State expanded Snapchat's private search by having an agent open a video that no Snapchat employee had previously viewed. The lower court clearly recognized this fundamental issue because it, too, neglected to mention Analyst Lochowitz's involvement. (R. 56:1–2.)

Regardless of which State agent opened the video first, the CyberTip established a virtual certainty that it contained child pornography. As this Court observed previously, an ESP's mandate under federal law to report instances of child pornography heightens the reliability of a CyberTip, and a CyberTip can be sufficient to establish probable cause in a warrant. *State v. Silverstein*, 2017 WI App 64, ¶¶ 19, 22–26 & n.12, 378 Wis. 2d 42, 902 N.W.2d 550. The CyberTip in the

present case stated that Snapchat had identified a child pornography video with PhotoDNA and reported it pursuant to its statutory obligation. (R. 38:4.)

Gasper attempts to undermine the reliability of a CyberTip by noting that any individual can file a report with NCMEC. (Gasper's Br. 36–37.) This argument is a red herring. Like in *Silverstein*, this case concerns a report generated by an ESP with a legal obligation to report child pornography. In these circumstances, the CyberTip is inherently reliable. *See Silverstein*, 378 Wis. 2d 42, ¶ 19. The State does not argue anything more than that.

C. Gasper has failed to show that the State lacked a virtual certainty that the flagged video depicted child pornography.

Gasper offers several arguments that are best construed as challenging the State's argument that the State had a virtual certainty that the flagged video in the CyberTip depicted child pornography. (Gasper's Br. 14–15, 28–40.) These arguments are meritless.

First, Gasper contends that the State presented no evidence of PhotoDNA's reliability. (Gasper's Br. 14–15.) The State maintains, as it argued in its opening brief, that the reliability of the hash value matching technology is not relevant to the application of the private-search doctrine. (State's Br. 35.)

However, even if PhotoDNA's reliability does matter, Gasper's argument falls short. Gasper assails PhotoDNA's reliability without addressing the evidence cited by the State in support of its reliability. (State's Br. 33, 36–37.) Specifically, Detective Schroeder testified that every CyberTip that he has ever reviewed in approximately 100 investigations, including those triggered by PhotoDNA, had accurately flagged child pornography. (R. 60:66, 68–69.) The CyberTip included nothing else from Gasper's account that

could have been something other than child pornography. (R. 60:54.) Gasper also fixates on the fact that the lower court sustained his objection to Detective Schroeder's testimony that PhotoDNA advertises itself as having only a 1 in 10 billion risk of a false positive. (Gasper's Br. 14–15 (citing R. 60:67).) Because of that objection, however, the State has not relied on that statistic.[2]

Second, Gasper argues, pursuant to the Ninth Circuit's reasoning in *Wilson*, that the private-search doctrine cannot apply because Detective Schroeder learned more about the video by watching it than by reading the CyberTip. (Gasper's Br. 28–29.) In so arguing, Gasper repeats *Wilson*'s error of replacing the objective "virtual certainty" standard from *United States v. Jacobsen*, 466 U.S. 109, 119 (1984), with a squishy "information learned" standard. An "information learned" standard runs directly counter to the numerous appellate courts—including the Ninth Circuit—that recognize that a government officer may examine the fruits of a private search more thoroughly than the private party, enabling the officer to learn more information than the private party. *See United States v. Miller*, 982 F.3d 412, 431 (6th Cir. 2020); *United States v. Tosti*, 733 F.3d 816, 822 (9th Cir. 2013); *United States v. Runyan*, 275 F.3d 449, 463–64 (5th Cir. 2001); *United States v. Simpson*, 904 F.2d 607, 610 (11th Cir. 1990).

The "information learned" standard is also irreconcilable with this Court's application of *Jacobsen* in *State v. Cameron*, 2012 WI App 93, 344 Wis. 2d 101, 820 N.W.2d 433. There, a woman handed a police officer a duffel bag of what she "believed to be" child pornography found in her ex-boyfriend's closet. *Id.* ¶ 4. The officer examined the

[2] Gasper has not defended the lower court's finding that hash value matching technology is unreliable due to the theoretical risk of hash value "collisions." (*See* R. 56:5–6.)

documents in the duffel bag and confirmed that they were child pornography. *Id.* ¶¶ 5–6. This Court found "very little, if anything, to distinguish *Jacobsen* from this case." *Id.* ¶ 28. Yet under *Wilson*'s reasoning, the private-search doctrine could not apply if the officer learned more from his review of the documents than what the ex-girlfriend informed him, which was only that she "believed" that she found child pornography. *Id.* ¶ 4. That is untenable. It would make the private-search doctrine intensely fact-specific and lead to different outcomes in otherwise similar cases. In this respect, *Wilson*'s "information learned" standard runs counter to established Wisconsin law.

Third, Gasper relies on *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016). (Gasper's Br. 30.) *Ackerman* is inapt. In *Ackerman*, law enforcement opened one file flagged as child pornography and three unflagged files. *Ackerman*, 831 F.3d at 1294, 1306–07. *Ackerman* held that law enforcement expanded the private search by opening the three unflagged files. *Id.* at 1306. It expressly declined to address the circumstances in the present case—whether the result would have changed had law enforcement opened only the flagged image. *Id.*

Fourth, Gasper claims that no virtual certainty existed because the search warrant affidavit that Detective Schroeder prepared *after* opening the video did not establish the reliability of PhotoDNA. (Gasper's Br. 31–33.) This argument misses the point. By then, Detective Schroeder had no need to establish the reliability of PhotoDNA. He could simply describe the child pornography video that he had just watched to establish probable cause. (R. 6:21.) Allegations regarding the reliability of PhotoDNA would have been extraneous and less probative. Their omission reflects sensible affidavit drafting, not a lack of reliability. The lower court even rejected this very argument when Gasper made it at the suppression hearing. (R. 60:112–16.)

Fifth, Gasper attempts to distinguish *United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018), and *Miller*. Gasper claims that *Reddick* was effectively superseded by the U.S. Supreme Court's decision in *Carpenter v. United States*, 585 U.S. 296 (2018). (Gasper's Br. 35.) That is plainly incorrect. *Carpenter* expressly limited its holding to cell-site location data. *Id.* at 316–17. *Reddick* had nothing to do with cell-site location data. *See Reddick*, 900 F.3d at 637–38. Therefore, *Carpenter* does not disturb *Reddick*.

Gasper argues that *Miller* is inapt because the defendant there—unlike him—did not challenge the reliability of the hash value matching technology. (Gasper's Br. 35–36.) The State explained in its opening brief that *Jacobsen* does not require proof of reliability as *Miller* suggests. (State's Br. 35.) In addition, *Miller* expressly rejected the argument advanced by Gasper and the lower court that the theoretical risk of PhotoDNA accidentally identifying non-contraband media precluded applying the private-search doctrine. (Gasper's Br. 35–37.) (*See also* R. 56:5.) "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 violated the Fourth Amendment when they reexamine the item." *Miller*, 982 F.3d at 431. Gasper cannot distinguish *Miller* with an argument that *Miller* rejected.

Sixth, Gasper relies generally on *Riley* and *Carpenter*. (Gasper's Br. 33–40.) As explained in Section I.C, *supra*, *Riley* does not apply because no cell phone search is relevant to the lower court's suppression order. *Carpenter* does not apply because Gasper's cell-site location data is not at issue.

Finally, Gasper states in passing that the evidence failed to establish the reliability of the database used as a source of comparison for the flagged video file. (Gasper's Br. 14, 35–36, 37–38.) Assuming, *arguendo*, that the database's

reliability matters, the record establishes both the database used and its reliability.

The CyberTip states, "Automated file categorization is 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.) NCMEC did not open this video. (R. 38:1.) Therefore, the latter situation in which the "uploaded fil[e]" was "visually similar" to files that NCMEC had "previously viewed and categorized" applied. (R. 38:5; *see also* R. 60:87.) Detective Schroeder explained how NCMEC compiles this database based on his personal experience. Following a completed case, he submits child pornography files to NCMEC. (R. 60:59–60.) Law enforcement officers around the world follow the same practice. (R. 60:64.) NCMEC stores both the media file itself and the hash value associated with the file. (R. 60:60.) NCMEC can then coordinate interjurisdictional law enforcement cooperation when other investigations encounter the same media files. (R. 60:60–61, 64.) Taken together, this evidence established the reliability of NCMEC's database.

III. The good faith exception to the exclusionary rule should apply.

Gasper's arguments regarding the good faith exception to the exclusionary rule are unavailing.

Gasper initially contends that the State forfeited this issue. (Gasper's Br. 13.) His argument depends on a deceptively truncated quotation from the suppression hearing. The State's full argument is below:

> This is an issue of first impression in Wisconsin. I don't think that it's unreasonable for the officers to have acted in the way that they did, given the status of the case law here in Wisconsin. None of the federal circuits that the defense cites to as I guess telling the court that you should rule in their favor

> are necessarily binding on how this officer acted in good faith of what his understanding of the law was.

(R. 60:170.) The lower court understood this argument because, at the end of the hearing, it commented that the State had "covered good faith." (R. 60:191.) The State therefore did not forfeit a good faith argument.

On the merits, Gasper argues that the good faith exception should not apply because he claims that Wisconsin law enforcement has adopted a policy in direct defiance of *Riley* and *Carpenter*. (Gasper's Br. 40–43.) However, as previously explained, neither *Riley* nor *Carpenter* applies in this case.

Rather, this case raises two novel issues of Wisconsin law. Detective Schroeder knew from training that *Wilson* is not binding in Wisconsin. (R. 60:154–55.) In fact, *Wilson* is an outlier. *Reddick* and *Miller* reached different conclusions. All state courts to have considered these issues in these specific circumstances opted to follow *Reddick* and *Miller* rather than *Wilson*. *See Walker v. State*, 669 S.W.3d 243, 252–55 & n.8 (Ark. Ct. App. 2023); *Wilson*, 270 Cal. Rtpr. 3d at 220–25; *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). In these circumstances, application of the good faith exception to the exclusionary rule is appropriate.

CONCLUSION

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

Dated: May 7, 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 3984 words.

Dated: May 7, 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: May 7, 2024.

Electronically signed by:

Michael J. Conway
MICHAEL J. CONWAY
Assistant Attorney General