STATE OF WISCONSIN

IN SUPREME COURT

Case No. 2023AP2319-CR

STATE OF WISCONSIN,

Plaintiff-Appellant,

v.

MICHAEL JOSEPH GASPER,

Defendant-Respondent-Petitioner.

ON REVIEW FROM A DECISION OF THE WISCONSIN COURT OF APPEALS REVERSING AN ORDER GRANTING SUPPRESSION ENTERED IN WAUKESHA COUNTY CIRCUIT COURT, THE HONORABLE SHELLEY J. GAYLORD, PRESIDING

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)
michael.conway@wisdoj.gov

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Statutes

Other Authorities

INTRODUCTION

Snapchat detected a video of child sexual abuse material (CSAM) in Michael Joseph Gasper's Snapchat account and reported it. The video and report ultimately came to a Wisconsin detective, who viewed the video and confirmed that it depicted CSAM. He then obtained a search warrant for Gasper's home and electronic devices. The search warrant led to the discovery of CSAM on Gasper's cell phone. That CSAM led the State to charge Gasper with several child pornography offenses.

The circuit court determined that the detective violated the Fourth Amendment by viewing the reported CSAM video without a warrant and, therefore, granted Gasper's motion to suppress all CSAM discovered after that point. Importantly, the circuit court did not address the lawfulness of the search warrant or the search of Gasper's cell phone.

The State appealed, and the court of appeals reversed. It determined that Gasper lacked an objectively reasonable expectation of privacy in the reported CSAM video based on Snapchat's Terms of Service. The court of appeals did not address the State's alternative arguments that the private-search doctrine applied to the detective's viewing of the video or that the exclusionary rule should not apply.

All three of those issues are now before this Court. Gasper either distorts or misrepresents them all. Most prominently, Gasper erroneously believes that this is a cell phone case. However, the alleged Fourth Amendment violation is the detective's viewing of the reported video, not the search of the cell phone pursuant to a warrant. This case presents two novel issues of law. By stubbornly insisting that this is a cell phone case, Gasper fails to meet the moment. While Gasper at least makes a reasonable-expectation-of-privacy argument, he fails to meaningfully address the private-search doctrine. Instead, he inexplicably picks nits in

the affidavit in support of the search warrant. Again, though, the search warrant is not at issue because the circuit court ruled that the Fourth Amendment violation occurred before the warrant was issued—when the detective viewed the reported video. Finally, Gasper contends that the exclusionary rule should not apply because he again erroneously asserts that this is a cell phone case.

The State's arguments are not just more persuasive. They are the only arguments on point. This Court should affirm the court of appeals' order reversing suppression.

ISSUES PRESENTED

1. Did Gasper prove that he had a reasonable expectation of privacy in a CSAM video viewed by a detective after Snapchat detected it in Gasper's Snapchat account and reported it to law enforcement pursuant to its Terms of Service?

The circuit court answered: Yes.

The court of appeals answered: No.

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.

The court of appeals did not address this issue.

This Court should answer: Yes.

3. If a Fourth Amendment violation occurred, should the exclusionary rule apply when the violation arose in the context of a novel issue of Wisconsin law and did not involve police misconduct?

The circuit court did not address this issue.

The court of appeals did not address this issue.

This Court should not reach this issue. If it does, this Court should answer: No.

STATEMENT ON ORAL ARGUMENT AND PUBLICATION

This Court typically publishes its opinions and holds oral argument. Both are appropriate.

STATEMENT OF THE CASE

Snap, Inc., an electronic service provider (ESP), detected a video depicting CSAM that had been "saved, shared, or uploaded" to Gasper's account on Snap's social media platform, Snapchat. (R. 38:3; 60:86.) Snapchat users can "share text, photographs, and video recordings, collectively known as 'snaps.'" *Commonwealth v. Carrasquillo*, 179 N.E.3d 1104, 1109 (Mass. 2022). The video was not made publicly available, and no other user saw it. (R. 38:3–4.) Snapchat detected the video using PhotoDNA, a program that scans files to determine if they are copies of known CSAM files. (R. 38:4; 60:24–25.) PhotoDNA uses "hash value[s]." (R. 60:21–22.)

A hash value "is a string of characters obtained by processing the contents of a given computer file and assigning a sequence of numbers and letters that correspond to the file's contents." *United States v. Reddick*, 900 F.3d 636, 637 (5th Cir. 2018). A hash value can be derived for any digital image. (R. 60:13.) The hash value is derived by an algorithm that analyzes 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, making it like a "serial number" for the file. (R. 60:13, 20.) If one bit is altered, then the entire hash value changes. (R. 60:13–16, 18.)

Because of the uniqueness of a file's hash value, many ESPs use hash value scanning software to detect CSAM. (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 CSAM files. (R. 60:11). If the hash value of the scanned file matches a hash value in the database, then the scanned file is a copy of that known CSAM 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 a sufficient number of pieces have matching hash values, PhotoDNA flags the scanned file as CSAM. (R. 60:24.)

Snapchat reported the flagged video and Gasper's username, date of birth, and IP address, to the National Center for Missing and Exploited Children (NCMEC). (R. 38:3; 60:37–38, 54.) No Snapchat employee viewed the video before sending it. (R. 38:4.) NCMEC prepared a CyberTipline Report ("CyberTip") and attached the video as "Apparent Child Pornography." (R. 38:1, 3; 60:37–38.) No NCMEC representative viewed 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.)

Because the IP address came from Wisconsin, NCMEC electronically sent the CyberTip to the Wisconsin Department

of Justice (DOJ) via an electronic portal. (R. 60:37–38, 90, 100.) A DOJ policy analyst viewed the video and then issued an administrative subpoena to obtain the subscriber information for the IP address. (R. 60:38–40.)[1] It returned Gasper as a subscriber and his home address. (R. 40:3; 60:40–41.)

Detective David Schroeder reviewed the CyberTip, viewed the video, and confirmed that it depicted CSAM. (R. 60:88, 100–01.) He subsequently prepared and executed a search warrant for Gasper's home and personal electronic devices. (R. 45:1–3; 60:70–71.) Detective Schroeder found 10 CSAM files on Gasper's cell phone. (R. 2:11; 60:81–82, 96.) The State subsequently charged Gasper with ten counts of possessing child pornography and nine counts of sexual exploitation of a child. (R. 2:1–9.)

Gasper filed a motion to suppress, raising several issues. (R. 23.) This appeal concerns only Gasper's claim that all CSAM recovered by police should be suppressed because Detective Schroeder unlawfully viewed the Snapchat video attached to the CyberTip without a warrant or warrant exception. (R. 23:3–4; 33:5–6.)

Detective Schroeder was the lone witness to testify at a suppression 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's Terms of Service that Gasper accepted when he made his account. (R. 41; 42; 44; 60:45–53, 56–57.) These policies banned CSAM, disclosed that Snapchat actively scanned for CSAM, and

---

[1] Gasper repeatedly notes that the DOJ analyst who issued the administrative subpoena viewed the CSAM video before Detective Schroeder. (Gasper's Br. 19, 26, 32.) However, Gasper never explains the significance of this undisputed fact and never incorporates it into any of his arguments.

warned that Snapchat would report CSAM to NCMEC or law enforcement. (R. 41:4; 42:2; 44:3.) Detective Schroeder demonstrated how Snapchat required him to accept the Terms of Service to create an account. (R. 60:55–56.)

Gasper cross-examined 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.)

Gasper attempted to submit an affidavit in which he asserted that he had a subjective expectation of privacy. (R. 60:140–46.) The State objected, and the circuit court sustained it, ruling the affidavit inadmissible. (R. 60:144, 146.) The circuit court permitted Gasper to submit the affidavit as an offer of proof to preserve the admissibility challenge for appeal. (R. 60:144–46.)

The State urged the circuit court to deny Gasper's motion to suppress. Gasper had failed to prove that he had a reasonable expectation of privacy in the CSAM video viewed by Detective Schroeder because Snapchat's Terms had specifically warned him that it banned, scanned for, and reported CSAM. (R. 60:162–64.) Even if Gasper had a reasonable expectation of privacy, Detective Schroeder lawfully opened the video from the CyberTip pursuant to the private-search doctrine. (R. 60:164–69.) Even if Detective Schroeder violated the Fourth Amendment, the exclusionary rule should not apply. (R. 60:170.)

Gasper opposed the State's arguments. He maintained that he had a reasonable expectation of privacy in the CSAM

file because it came from his Snapchat account, which was an extension of his cell phone. (R. 60:205.)

The circuit court granted Gasper's motion to suppress all CSAM recovered after Detective Schroeder viewed the video attached to the CyberTip. (R. 56:1.) 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 is categorically unreliable. (R. 56:5–6). The circuit court did not address the reliability of PhotoDNA, despite finding that Snapchat used it to detect the video. (R. 56:1–2, 5–6.)

The State appealed, and the court of appeals reversed in a published decision: *State v. Gasper*, 2024 WI App 72, 414 Wis. 2d 532, 16 N.W.3d 279. The court of appeals determined that Gasper failed to prove either a subjective or objectively reasonable expectation of privacy in the CSAM video viewed by Detective Schroeder. *Id.* ¶¶ 20, 28. It did not address the private-search doctrine or the applicability of the exclusionary rule. *Id.* ¶ 29 n.8. Gasper abandoned a challenge to the admissibility of his personal affidavit. *Id.* ¶ 20 n.7.

Gasper petitioned this Court for review. While his petition was pending, a different panel of the court of appeals certified a different CSAM case because the panel disagreed with *Gasper*'s reasoning—although not its result. *State v. Rauch Sharak*, No. 2024AP469-CR, 2025 WL 213713, at *1 (Wis. Ct. App. Jan. 16, 2025). (R-App. 3–17.) This Court granted review.

SUMMARY OF ARGUMENT

This Court should affirm the court of appeals' decision reversing the circuit court's suppression order for two independently sufficient reasons.

First, Gasper failed to prove either an objectively reasonable or subjective expectation of privacy in the reported CSAM viewed by Detective Schroeder. He lacked an objectively reasonable expectation of privacy because he agreed to Snapchat's Terms of Service, and those Terms deprived him of the right to exclude and other rights intrinsic to an expectation of privacy with respect to CSAM. This result accurately reflects Gasper's relationship with Snapchat. Gasper created a bailment with Snapchat by uploading the video to his account, and Snapchat refused to be a bailee of CSAM. Gasper failed to present any admissible evidence to support a subjective expectation of privacy. Instead, Gasper tries to turn this case into a cell phone case. However, the alleged Fourth Amendment violation is Detective Schroeder's viewing of the CSAM video attached to the CyberTip, not a search of Gasper's phone.

Second, even if Gasper had a reasonable expectation of privacy in the reported CSAM video, Detective Schroeder still lawfully viewed the video pursuant to the private-search doctrine. The private-search doctrine applies when a private party invites a government agent to recreate the private party's search and provides a virtual certainty about the result of the search. Here, Snapchat invited Detective Schroeder to view a video that it had already scanned and identified as CSAM. The CyberTip provided a virtual certainty about the file's contents because it stated that Snapchat detected the CSAM with PhotoDNA. The counterargument advanced by other courts is flawed because it erroneously grafts the plain-view doctrine to the private-search doctrine.

This Court can affirm the court of appeals for either of these two reasons. Either no Fourth Amendment event occurred because Gasper failed to prove a reasonable expectation of privacy, or Detective Schroeder's viewing of the reported video fell within the warrant exception provided by the private-search doctrine. Nevertheless, both issues merit this Court's attention because both issues recur and have statewide importance.

Finally, even if Gasper suffered a Fourth Amendment violation, the exclusionary rule should not apply.

STANDARD OF REVIEW

When reviewing a suppression order, this Court accepts the circuit court's factual findings unless they are clearly erroneous and "independently appl[ies] constitutional principles to those facts." *State v. Tullberg*, 2014 WI 134, ¶ 27, 359 Wis. 2d 421, 857 N.W.2d 120 (citation omitted).

ARGUMENT

I. Gasper lacked a reasonable expectation of privacy in the reported CSAM video viewed by the detective.

The Fourth Amendment to the U.S. Constitution protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." *State v. Bruski*, 2007 WI 25, ¶ 20, 299 Wis. 2d 177, 727 N.W.2d 503 (alteration in original). To challenge a search, a defendant must establish both a subjective and objectively reasonable expectation of privacy in the area searched. *Id.* ¶¶ 22–23. The court of appeals correctly concluded that Gasper failed to satisfy either burden for the CSAM video viewed by Detective Schroeder. *Gasper*, 414 Wis. 2d 532, ¶ 29.

A. The court of appeals correctly concluded that Snapchat's policies deprived Gasper of an objectively reasonable expectation of privacy in the CSAM video viewed by the detective.

This Court has identified the following, non-exclusive factors as relevant to determining the reasonableness of an expectation of privacy:

> (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).

These factors invoke property law concepts. The first two factors expressly refer to an individual's property interests. The third factor invokes fundamental concepts of property law. The "right to exclude" others is "universally held to be a fundamental element of the property right." *Cedar Point Nursery v. Hassid*, 594 U.S. 139, 150 (2021) (citation omitted). "[D]ominion and control" are synonymous with the right to exclude as their "very essence . . . includes the right to exclude others." *State v. Wisumierski*, 106 Wis. 2d 722, 737, 317 N.W.2d 484 (1982). The fourth and fifth factors ask whether the individual took actions consistent with exercising the right to exclude.

Thus, "property rights alone, although not controlling, are relevant" to determining an individual's expectation of privacy. *State v. Rewolinski*, 159 Wis. 2d 1, 18, 464 N.W.2d 401 (1990) (citing *Rakas v. Illinois*, 439 U.S. 128, 143 (1978)). The U.S. Supreme Court has more recently reiterated that "[l]egitimation of expectations of privacy by law must have a

source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." *Byrd v. United States*, 584 U.S. 395, 405 (2018) (alteration in original) (quoting *Rakas*, 439 U.S. at 144 n.12.) *Byrd* identified the right to exclude as one of these important sources of privacy: "'One of the main rights attaching to property is the right to exclude others,' and, in the main, 'one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of the right to exclude.'" *Id.* (quoting *Rakas*, 439 U.S. at 144 n.12.)

Generally, a user has a reasonable expectation of privacy in an ESP account because it is tantamount to a "container used to store personal documents and effects." *State v. Bowers*, 2023 WI App 4, ¶ 26, 405 Wis. 2d 716, 985 N.W.2d 123. In the present case, the court of appeals correctly recognized that this expectation of privacy did not extend to the CSAM video that Detective Schroeder viewed outside of Gasper's account after Snapchat reported it pursuant to three of its policies. *Gasper*, 414 Wis. 2d 532, ¶¶ 16, 22, 28. First, Snapchat's Terms of Service informed users that they could not use their accounts for unlawful purposes, and that Snapchat "reserve[s] the right" to remove and report content to law enforcement that violates Snapchat's content policies or the law. *Id.* ¶ 17 (alteration in original); (R. 41:4, 6–7). Second, the Snapchat Community Guidelines expressly prohibited all content involving sexually explicit content with a minor. *Gasper*, 414 Wis. 2d 532, ¶ 18; (R. 42:2). The Community Guidelines also informed users that Snapchat reports any instance of the sexual exploitation of a minor to law enforcement. *Gasper*, 414 Wis. 2d 532, ¶ 18; (R. 42:2). Third, the Sexual Content Explainer reiterated Snapchat's prohibition on CSAM and stated that Snapchat reports all CSAM to NCMEC. *Gasper*, 414 Wis. 2d 532, ¶ 19; (R. 44:1, 3).

Given these policies, any subjective expectation of privacy would have been "objectively unreasonable." *Gasper*, 414 Wis. 2d 532, ¶ 22.

The court of appeals correctly applied Snapchat's Terms of Service to the *Bruski* factors. Snapchat's Terms "limited Gasper's property interest in his account, which prohibited him from saving, sharing, or uploading child pornography to his account." *Gasper*, 414 Wis. 2d 532, ¶ 22. By agreeing to allow Snapchat to monitor and access his account for CSAM, Gasper surrendered his dominion and control. *Id.* Snapchat's Terms specifically provided that Gasper could not take precautions to secure the privacy of CSAM in his account. *Id.* ¶ 24. Rather, Snapchat retained the right to circumvent or override those precautions to remove and report CSAM. *See id.* At bottom, "Gasper could not exclude Snapchat from his account when it came to child pornography." *Id.* ¶ 23.

Although the factual basis for *Gasper*'s holding arises from Snapchat's Terms of Service, the legal conclusion rests on how the Terms restricted Gasper's right to exclude. A property-law analogue for the relationship between Gasper and Snapchat confirms the soundness of *Gasper*'s holding. *See Byrd*, 584 U.S. at 404 (stating that "[r]eference to property concepts . . . aids the Court" in deciding the reasonable expectation of privacy question). The relevant relationship is the bailment. Snapchat reasonably restricted Gasper's right to exclude with respect to CSAM within the context of a bailment.

"A bailment is created by delivery of personal property from one person to another to be held temporarily for the benefit of the bailor (the person who delivers personal property . . .), the bailee (the person who receives possession or custody of property . . .), or both, under an express or implied contract." *Toyota Motor Credit Corp. v. N. Shore Collision, LLC*, 2011 WI App 38, ¶ 11, 332 Wis. 2d 201, 796 N.W.2d 832. Stated more simply, "[e]ntrusting your stuff to

others is a bailment." *Carpenter v. United States*, 585 U.S. 296, 399 (2018) (Gorsuch, J., dissenting) (emphasis omitted). "[B]ailment law touches our lives on an almost daily basis." Michael J. O'Connor, *Digital Bailments*, 22 U. Pa. J. Const. L. 1271, 1307 (2020). "When I lend my drill to a neighbor, park my car in a commercial garage, or check my bag on an airline, bailment law governs the relationship." *Id.*

One professor has explained that a bailment is created when a user stores files in a cloud storage account run by an ESP, just like it would in the context of physical storage:

> The owners of the file, like the less[ees] of a storage unit or safe deposit box, retain the right to access their property and may have some control over how secure the property is, but they do not control the infrastructure that makes the storage possible. Decisions about the infrastructure lie with the cloud storage company or the owner of the self-storage site.

Danielle D'Onfro, *The New Bailments*, 97 Wash. L. Rev. 97, 128 (2022); *see also Carpenter*, 585 U.S. at 400 (Gorsuch, J., dissenting) (theorizing that delivering data to a third party creates a bailment). Moreover, "if the cloud storage provider is scanning the files for contraband and touting its security, the best analogy might be to the attended parking lot—which usually does create a bailment relationship." D'Onfro, *supra*, at 128; *see O'Brien v. Isaacs*, 17 Wis. 2d 261, 264, 116 N.W.2d 246 (1962) (stating that patron's use of an attended parking lot created a bailment).

A bailment is governed by "an express or implied contract." *Toyota Motor*, 332 Wis. 2d 201, ¶ 11. "An express agreement will prevail against general principles of law that would apply in the absence of such an agreement." 8 C.J.S. Bailments § 36 & n.7 (2024) (collecting cases). "Absent any law of bailment that contemplates cloud storage, the law of contract will be its alpha and omega." D'Onfro, *supra*, at 147.

This Court considered bailments in *Wisumierski* to conclude that the defendant lacked a reasonable expectation of privacy in a van. The defendant had been a passenger in the van when a police officer stopped it. *Wisumierski*, 106 Wis. 2d at 726–27. The defendant planned to drive the van away after the officer arrested the driver, who owned the van. *Id.* at 726. Before the defendant entered the driver's seat, however, the officer found a gun in the van and arrested the defendant on that basis. *Id.* The defendant argued that he had a reasonable expectation of privacy in the van by virtue of his "dominion and control" of the van. *Id.* at 733. This Court disagreed based on bailment law. While the driver, as bailor, had intended to convey the van to the defendant, as bailee, the defendant never took possession of the van. *Id.* at 736. As a result, the bailment did not arise. *Id.* at 736–37. Without the bailment, the defendant lacked "the requisite dominion and control over the van" to establish a reasonable expectation of privacy. *Id.* at 737; *see also State v. Dixon*, 177 Wis. 2d 461, 470, 501 N.W.2d 442 (1993) (holding that non-owner driver had a reasonable expectation of privacy in a car because he was a bailee).

By saving, sharing, or uploading files to his Snapchat account, Gasper created a bailment with Snapchat. *See Gasper*, 414 Wis. 2d 532, ¶ 2. He controlled the files in his account, and Snapchat provided the infrastructure of his account. *See* D'Onfro, *supra*, at 128. Moreover, Gasper allowed Snapchat to scan his account for CSAM, making the relationship akin to the bailment that arises in an attended parking lot. *See id.*; *O'Brien*, 17 Wis. 2d at 264.

Because Gasper's use of a Snapchat account constituted a bailment, the court of appeals appropriately looked to the contract between the parties—as set forth in Snapchat's Terms of Service—to determine the scope of Gasper's right to exclude within the bailment and, thus, his reasonable expectation of privacy. The Terms required Gasper to

relinquish his right to exclude Snapchat from CSAM and consent to Snapchat's monitoring and reporting policies. Stated another way, Snapchat refused to facilitate the storage or transmission of CSAM in its role as bailee. The court of appeals appropriately gave effect to the bailment as defined by the Terms of Service in evaluating the reasonableness of Gasper's claimed expectation of privacy. *See Toyota Motor*, 332 Wis. 2d 201, ¶ 11.

Gasper cannot demonstrate that he had an objectively reasonable expectation of privacy under *Bruski* in the reported CSAM video viewed by Detective Schroeder. Under the Terms of Service, Gasper lacked a property interest in CSAM, could not exclude Snapchat from CSAM in his account, and could not exercise dominion and control over CSAM. *See Bruski*, 299 Wis. 2d 177, ¶ 24 (factors one and three). He accepted that he could not take precautions to exclude Snapchat from his CSAM or to put the CSAM to some private use. *See id.* (factors four and five). He could not otherwise legitimately possess CSAM under contemporary or historical notions of privacy. *See id.* (factors two and six); *see also Illinois v. Caballes*, 543 U.S. 405, 408–09 (2005) ("[A]ny interest in possessing contraband cannot be deemed 'legitimate.'" (citation omitted)).

Gasper mistakenly believes that the court of appeals held that he lacked a reasonable expectation of privacy in his Snapchat account. (Gasper's Br. 26.) The court of appeals concluded only that "Gasper has not met his burden in demonstrating that any expectation of privacy *in the video* was either subjectively or objectively reasonable." *Gasper*, 414 Wis. 2d 532, ¶ 28 (emphasis added). That ruling reflected Gasper's Fourth Amendment claim that the circuit court accepted in granting suppression. (R. 23:3–4; 33:5–6; 56:1.)

Gasper argues that Snapchat's Terms should not have been admitted into evidence for lack of foundation. (Gasper's Br. 31.) However, Gasper made and then withdrew this

objection at the suppression hearing. (R. 43:5; 60:50–52.) He abandoned this admissibility challenge in the court of appeals.

Gasper also appears to argue that Snapchat's Terms were not specific enough to deprive him of a right to exclude with respect to CSAM. (Gasper's Br. 29–31.) This argument lacks merit. Snapchat promised to "report all instances of child sexual exploitation to authorities," (R. 42:2), and to "report violations of these policies to [NCMEC]," which then "coordinates with domestic or international law enforcement," (R. 44:3). These statements are unambiguous.

Thus, Gasper lacked an objectively reasonable expectation of privacy in the reported CSAM video viewed by Detective Schroeder. In so holding, this Court should issue the following rule: When an ESP's terms require a user to relinquish the right to exclude the ESP with respect to CSAM and notify the user that the ESP will take actions on CSAM that includes reporting to the authorities, the user lacks an objectively reasonable expectation of privacy in CSAM that the ESP removes from the user's account and reports to law enforcement.

B. The court of appeals properly considered Snapchat's Terms of Service.

Gasper appears to argue that the court of appeals erred by considering Snapchat's Terms of Service at all, citing *Byrd*. (Gasper's Br. 28–29.) He is incorrect.

Byrd plainly requires that an objectively reasonable expectation of privacy be rooted in "a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." *Byrd*, 584 U.S. at 405 (citation omitted) One of these "concepts" is the "right to exclude." *Id.* (citation omitted). The court of appeals squarely applied *Byrd* by considering how Snapchat's Terms of Service

impacted Gasper's property rights in CSAM, particularly his right to exclude.

For that reason, Gasper's reliance on *United States v. Thomas*, 65 F.4th 922 (7th Cir. 2023) is misplaced. *Thomas* followed *Byrd*. (Gasper's Br. 28.) There, the defendant leased a condo in Georgia under a false identity while a fugitive. *Thomas*, 65 F.4th at 923. While "using an alias to sign a lease . . . does not by itself deprive a tenant of a legitimate expectation of privacy," the landlord "retained an ownership interest in the property and was entitled to protect her interest from a fugitive." *Id.* at 923–24. The question was "*how* she was entitled to protect this interest," which "b[ore] on the reasonableness of Thomas's expectation of privacy." *Id.* Georgia eviction law provided that "how." *Id.* Because Thomas's landlord had not completed the eviction process under Georgia law, "Thomas was entitled to all the rights of any other leaseholder, including *the right to exclude* strangers such as police officers." *Id.* (emphasis added).

Conversely, had the landlord completed Georgia's legal process for eviction, Thomas would have lost the right to exclude and, consequently, his expectation of privacy. *See State v. Whitrock*, 161 Wis. 2d 960, 981, 468 N.W.2d 696 (1991) (holding that defendant lacked a reasonable expectation of privacy in an apartment as a guest because his alleged host "was not a party to a rental agreement, did not pay rent, and had been served with an eviction notice"); *United States v. Cunag*, 386 F.3d 888, 895 (9th Cir. 2004) (concluding that hotel employee's "private acts of dominion" to evict defendant deprived defendant of a reasonable expectation of privacy in a hotel room (citation omitted)). *Gasper* ruled consistently with *Thomas* by considering how Snapchat's Terms of Service "b[ore] on the reasonableness of [Gasper's] expectation of privacy." *Thomas*, 65 F.4th at 924.

C. Gasper also failed to prove a subjective expectation of privacy.

The court of appeals also correctly concluded that Gasper failed to prove a subjective expectation of privacy. *Gasper*, 414 Wis. 2d 532, ¶ 20. Snapchat's Terms of Service clearly informed Gasper that it prohibited CSAM, scanned for CSAM, and reported CSAM. (R. 41:4, 6–7; 42:2; 44:3.) Gasper agreed to these policies to create his account. (R. 60:55–56.) "Gasper did not testify, nor did he submit any admissible evidence to meet his burden to show that he believed the video downloaded on Snapchat was private." *Gasper*, 414 Wis. 2d 532, ¶ 20. That omission is dispositive. As the Seventh Circuit recently observed, "it is almost impossible to find a privacy interest without an affidavit or testimony from the defendant." *United States v. Dixon*, 137 F.4th 592, 602 (7th Cir. 2025). Gasper does not explain why his case presents the exception to that rule.

Instead, Gasper relies on the affidavit that the circuit court ruled inadmissible. (Gasper's Br. 24.)[2] The circuit court clearly limited Gasper to reading the affidavit into the record as an offer of proof. (R. 60:143–45.) Contrary to Gasper's apparent understanding (Gasper's Br. 23–24), an offer of proof is not evidence. An offer of proof is "[a] presentation of evidence . . . so that the evidence can be preserved on the record for an appeal of the judge's ruling." *Offer of Proof*, Black's Law Dictionary (12th ed. 2024); *see* Wis. Stat. § 901.03(1)(b) (requiring an offer of proof to preserve a challenge to a ruling excluding evidence). Gasper abandoned the admissibility challenge in the court of appeals. *Gasper*,

[2] Gasper also claims that the fact that he had a password-protected home WiFi network supports his subjective expectation of privacy. (Gasper's Br. 23–24.) This bare fact is too attenuated from either the Snapchat account or the CSAM video to satisfy Gasper's burden.

414 Wis. 2d 532, ¶ 20 n.7. Therefore, the circuit court's ruling excluding the affidavit stands.

D. Gasper's cell phone and third-party doctrine arguments are irrelevant.

Gasper's two primary arguments miss the mark entirely.

First, Gasper argues that he has a categorical expectation of privacy in the reported CSAM video under *Riley v. California*, 573 U.S. 373 (2014), because he accessed Snapchat exclusively through his cell phone. (Gasper's Br. 21–25.) *Riley* held that warrantless searches of cell phones are presumptively unreasonable. *Riley*, 573 U.S. at 401.

Riley is irrelevant because the alleged Fourth Amendment violation is when Detective Schroeder viewed the CSAM video attached to the CyberTip. (R. 23:3; 28:5–6; 56:1, 5.) Detective Schroeder did not access Gasper's phone or Snapchat account when reviewing the CyberTip. *Gasper*, 414 Wis. 2d 532, ¶¶ 3–4. No law enforcement officer accessed Gasper's phone until the execution of the search warrant. (R. 46; 60:70–71, 80–82.) Therefore, *Riley* is inapt.

Gasper argues otherwise only by misapprehending *Riley*. *Riley* observed that cell phones "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 and their large storage size, particularly when combined with cloud storage. *Id.* at 393–98. Gasper reverses that reasoning, affording privacy protection to any data that a cell phone could plausibly access through cloud computing. (Gasper's Br. 23.) Unlike a cell phone, however, the single CSAM video attached to the CyberTip did not provide Detective Schroeder a toehold in a digital environment in which to examine other data—let alone all the data accessible by a cell phone. (R. 60:54.)

Were Gasper correct, absurd results would follow. Currently, a person lacks a reasonable expectation of privacy in text messages sent from that person's phone but viewed by law enforcement on the recipient's phone. *State v. Tentoni*, 2015 WI App 77, ¶¶ 11–12, 365 Wis. 2d 211, 871 N.W.2d 285. According to Gasper, the police would need a warrant to view the text messages on the recipient's phone because the sender retained an expectation of privacy in the messages as data accessible by his cell phone. That result would be unreasonable.

Gasper makes this *Riley* argument alone. Even those who support Gasper's conclusion do not support his reasoning. *See United States v. Maher*, 120 F.4th 297, 307–09 (2d Cir. 2024); *Rauch Sharak*, 2025 WL 213713, at *4, 6. Defendant Rauch Sharak distanced himself from Gasper's argument in the court of appeals, calling it "confusing" and "missing the point." (R-App. 19.) The State agrees.

Second, Gasper argues that the court of appeals erroneously applied the third-party doctrine. (Gasper's Br. 27–29.) Neither the State nor the court of appeals has relied on the third-party doctrine. The third-party doctrine would arguably deprive Gasper of a reasonable expectation of privacy in *all* data in his Snapchat account merely because Snapchat, a third party, was the custodian of that data. *See United States v. Miller*, 425 U.S. 435, 442 (1976) (concluding that defendant lacked reasonable expectation of privacy in checks and deposit slips submitted to and held by bank). The court of appeals issued a far narrower decision, holding only that Gasper lacked a reasonable expectation of privacy in a single CSAM video reported by Snapchat pursuant to its Terms of Service.

II. The detective lawfully opened the reported CSAM video under the private-search doctrine.

Even if Gasper established a reasonable expectation of privacy, the circuit court still erred in granting his motion to suppress. It should have applied the private-search doctrine.

"The touchstone of the Fourth Amendment is reasonableness. The Fourth Amendment does not proscribe all state-initiated searches and seizures; it merely proscribes those which are unreasonable." *Tullberg*, 359 Wis. 2d 421, ¶ 29 (citations omitted). While a warrantless search is presumptively unreasonable, a court will uphold a search if it falls within an exception to the warrant requirement. *Id.* ¶ 30.

The private-search doctrine is a warrant exception. The Fourth Amendment applies "only [to] governmental action; it is wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual.'" *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (citation omitted). Once a private party has searched an item, the owner's "expectation of privacy" in that item "has . . . been frustrated" such that the owner no longer has a "legitimate expectation of privacy." *Id.* at 117, 119–20. A government agent may therefore "view[ ] what a private party ha[s] freely made available for his inspection" without offending the Fourth Amendment. *Id.* at 119.[3]

Four federal appellate circuits have divided in applying the private-search doctrine to Gasper's circumstances when an ESP reports CSAM without first having an employee manually view the CSAM.[4] The Fifth Circuit in *Reddick*, and

---

[3] It is undisputed that Snapchat acted as a private party. (R. 33:6; 60:195.)

[4] When an ESP employee views the flagged file before reporting it, federal courts agree that the private-search doctrine

the Sixth Circuit in *United States v. Miller*, 982 F.3d 412 (6th Cir. 2020), held that the private-search doctrine applied. The Ninth Circuit in *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021), and the Second Circuit in *Maher* concluded otherwise. This is an issue of first impression in Wisconsin.

Other state courts have followed *Reddick* and *Miller*. *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); *Morales v. State*, 274 So.3d 1213, 1217–18 (Fla. Ct. App. 2019). No state court has yet followed *Wilson* and *Maher*.

This Court should join *Reddick*, *Miller*, and the states that have followed them in holding that the private-search doctrine applied to Detective Schroeder's viewing of the CSAM video.[5]

A. The private-search doctrine applies when a private actor invites a government agent to recreate the private actor's search and provides a virtual certainty about the search's result.

The U.S. Supreme Court suppressed the content of pornographic filmstrips that had been misdelivered to a company in *Walter v. United States*, 447 U.S. 649, 651–52

---

applies to an investigator's viewing of the same file. *See United States v. Bebris*, 4 F.4th 551, 562 (7th Cir. 2021); *United States v. Ringland*, 966 F.3d 731, 737 (8th Cir. 2020); *United States v. Powell*, 925 F.3d 1, 6 (1st Cir. 2018); *see also United States v. Meals*, 21 F.4th 903, 908 (5th Cir. 2021) (reaching this conclusion with respect to NCMEC while assuming NCMEC to be a government actor).

[5] Gasper does not suggest that the answer to this question changes because the DOJ analyst viewed the CSAM video before Detective Schroeder, nor could he. Whether a government agent expanded Snapchat's private search by viewing the video does not turn on which government agent viewed the video first.

(1980) (lead opinion of Stevens, J.). Company employees opened the packages, observed "suggestive drawings" and "explicit descriptions" on the boxes, and then gave the boxes to the FBI. *Id.* at 652. Agents viewed the films over the next two months without a warrant. *Id.* The lead opinion ruled that "[t]he projection of the films" by the FBI agents "was a significant expansion" of the employees' private search. *Id.* at 657. "Prior to the Government screening one could only draw inferences about what was on the films." *Id.*

Walter, however, provides little guidance. Justice Stevens's lead opinion was joined only by Justice Stewart. *See id.* at 649. Justice White, joined by Justice Brennan, rejected the premise of the lead opinion that "private searches insulate from Fourth Amendment scrutiny subsequent governmental searches of the same or lesser scope." *Id.* at 650 (White, J., concurring). Justice Marshall concurred in the judgment without writing or joining an opinion. *See id.* Justice Blackmun, joined by the three remaining justices, dissented. *See id.* at 662–66 (Blackmun, J., dissenting). "All in all, *Walter* is surely among the least edifying additions to Fourth Amendment case law in recent memory." Anne Tommey McKenna & Clifford S. Fishman, *Wiretapping and Eavesdropping* § 6:39, Westlaw (database updated Dec. 2024).

Jacobsen produced a true majority and explained the private-search doctrine that applies today. Federal Express employees accidentally damaged a package with a forklift and then opened it to prepare an insurance claim. *Jacobsen*, 466 U.S. at 111. The package contained a tube concealed within newspaper, and 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, which tested positive for cocaine. *Id.* at 111–12.

"The agent's viewing of what a private party had freely made available for his inspection did not violate the Fourth Amendment." *Id.* at 119. *Jacobsen*'s holding rested on "the virtual certainty that nothing else of significance was in the package." *Id.* 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.*

Jacobsen determined that the drug test exceeded the scope of the private search but still did not violate the Fourth Amendment. *Id.* at 123. The Court "assess[ed] the reasonableness of this conduct" by comparing the individual's Fourth Amendment interests to "the importance of the governmental interests alleged to justify the intrusion." *Id.* at 125 (citation omitted). The impact of the drug test "on any protected property interest" was "*de minimis*" because it merely destroyed an indeterminately small amount of a substance that was already lawfully detained. *Id.* The government's interest, on the other hand, was "substantial," particularly since it was "virtually certain that the substance tested was in fact contraband." *Id.* Therefore, the drug test "was reasonable" and did not run afoul of the Fourth Amendment. *Id.*

Justice White concurred in the judgment because he determined that the tube holding the baggies of white powder was in plain view. *Jacobsen*, 466 U.S. at 126–27 (White, J., concurring). He maintained that a private person's search did not relieve the government of its Fourth Amendment obligations. *Id.* at 131. The Court rejected Justice White's approach because it refused to "have this case turn on the fortuity of whether the Federal Express agents placed the tube back into the box." *Id.* 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.* (emphasis added).

Subsequently, federal appellate courts have applied the private-search doctrine when there is a "virtual" or "substantial" certainty that the government agent's search will not reveal anything more than the private party represented. *See United States v. Phillips*, 32 F.4th 865, 870 (9th Cir. 2022); *United States v. Rivera-Morales*, 961 F.3d 1, 11, 15 (1st Cir. 2020); *United States v. Lichtenberger*, 786 F.3d 478, 488 (6th Cir. 2015); *Rann v. Atchison*, 689 F.3d 832, 836–37 (7th Cir. 2012); *United States v. Runyan*, 275 F.3d 449, 463 (5th Cir. 2001).

Although the Supreme Court has never defined "virtual certainty," the term "implies something less than absolute confidence." *Rivera-Morales*, 961 F.3d at 11. "[T]he 'virtual certainty' inquiry requires a common-sense determination into whether there is anything more than a remote or highly unlikely possibility that the officer's actions will uncover something of significance apart from what the private searcher has found and reported." *Id.* This standard is objective. *Id.* at 10; *Phillips*, 32 F.4th at 870.

B. *Reddick* and *Miller* correctly concluded that an investigator may open a file that an ESP flags and reports as CSAM.

The Fifth Circuit in *Reddick* and the Sixth Circuit in *Miller* persuasively applied *Jacobsen* to Gasper's circumstances.

Reddick concluded that the investigator's viewing of the flagged files was equivalent to the drug test in *Jacobsen*. *Reddick*, 900 F.3d at 639. *Reddick* 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). Like the *de minimis* additional intrusion of the drug test in *Jacobsen*, "opening the file merely confirmed that the flagged file was indeed child pornography, as suspected." *Id.*

Miller reached the same conclusion but deemed the search of the package to be the apt comparison from *Jacobsen*. *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 CSAM 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.*

Miller made two additional observations germane to the present case. First, *Miller* explained that it would be absurd to treat hash value scanning software differently than human observation. A private individual can trigger the private-search doctrine with a "quick view" of a picture, "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. Tosti*, 733 F.3d 816, 822 (9th Cir. 2013); *United States v. Simpson*, 904 F.2d 607, 610 (11th Cir. 1990). "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 that the hash value software misidentified CSAM. *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 private-search doctrine applied to the detective's viewing of the CSAM video.

The circuit court erred by concluding that the private-search doctrine did not apply for two reasons. First, viewing the reported video did not expand Snapchat's private search because the CyberTip provided a virtual certainty that the video depicted nothing but CSAM. Second, even if viewing the video expanded Snapchat's search, the additional intrusion was *de minimis* and, thus, reasonable under the Fourth Amendment. Either conclusion leads to holding that Detective Schroeder lawfully viewed the video without a warrant.

1. The private-search doctrine applied because the CyberTip established a virtual certainty that the flagged file contained nothing but CSAM.

The private-search doctrine applied to the viewing of the CSAM video because the CyberTip provided a virtual certainty that the video contained nothing but a slightly altered copy of a known CSAM file.

The CyberTip reported the attached video as "Apparent Child Pornography." (R. 38:5.) It explained that this classification arose from either "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.) The CyberTip also stated that no NCMEC representative viewed the video. (R. 38:1.) Accordingly, the CyberTip disclosed that the reported video

was a hash match to a "visually similar fil[e]" that NCMEC had "previously viewed and categorized." (R. 38:5.)

The CyberTip stated that PhotoDNA identified the reported file as known CSAM. (R. 38:4; 60:26.) A file's hash value is a powerful identifier because it remains constant and remains unique for that file, operating like a "serial number" for the file. (R. 60:13–14.) That "serial number," however, is subject to manipulation. The alteration of a single pixel in the file will drastically change the file's hash value, so individuals can evade one-to-one hash value matches by slightly altering the file. (R. 60:13–14, 22.) PhotoDNA rectifies this weakness by dividing the scanned file and the known CSAM files into pieces, deriving the hash value for each piece, and then comparing the pieces. (R. 60:24, 29.) Thus, the use of PhotoDNA provided a virtual certainty that the flagged video depicted nothing but a slightly altered copy of a previously reported CSAM file. In fact, *Reddick* concluded that PhotoDNA created an "almost absolute certainty" that the files contained CSAM. *Reddick*, 900 F.3d at 639 (citation omitted). That certainty exceeded *Jacobsen*'s virtual certainty standard, which "implies something less than absolute confidence." *Rivera-Morales*, 961 F.3d at 11.

In addition, CyberTips generated by ESPs are inherently reliable. Once Snapchat became aware of the video, it was required by federal law to report it to NCMEC. 18 U.S.C. § 2258A(a)(1), (b)(1). "[C]ourts in other jurisdictions have held that this obligation itself heightens the reliability of the tip." *State v. Silverstein*, 2017 WI App 64, ¶ 19, 378 Wis. 2d 42, 902 N.W.2d 550 (collecting cases). *Silverstein* determined that the CyberTip constituted a tip from an identified citizen informant. *Id.* Because of this reliability, a hash value match reported by an ESP can establish probable cause for a search warrant, even when the investigator does not view the reported files. *See United States v. Cartier*, 543 F.3d 442, 446 (8th Cir. 2008); *Maher*, 120 F.4th at 319

(opining that a hash value match would "demonstrate probable cause to support warrants" for "searches of Maher's Google accounts and residence").

In sum, the private-search doctrine applied to the viewing of the video because the CyberTip established that the video was a slightly altered copy of known CSAM. By viewing the video, Detective Schroeder guarded against the risk of an erroneous report and engaged in a more thorough examination of the video—both of which were permissible under the private-search doctrine. *See Jacobsen*, 466 U.S. at 119; *Phillips*, 32 F.4th at 870; *Miller*, 982 F.3d at 430–31.

2. If opening the video was an additional intrusion, it was *de minimis* and reasonable under the Fourth Amendment.

Even if Detective Schroeder's viewing of the video expanded Snapchat's private search, that expansion was *de minimis* and did not violate the Fourth Amendment.

Like the drug test in *Jacobsen*, the government had a substantial interest in having an agent view the reported video to safeguard children from the physical and mental harm caused by CSAM. *See United States v. Mecham*, 950 F.3d 257, 262 (5th Cir. 2020). In addition, the CyberTip made it "virtually certain" that the video's contents were "in fact contraband." *Jacobsen*, 466 U.S. at 125. Gasper, on the other hand, had only the "mere expectation . . . that certain facts will not come to the attention of the authorities." *Id.* at 122. Even if the CyberTip erroneously reported the video, Detective Schroeder could not access any other content from Gasper's Snapchat account. (R. 60:54.) "Under these circumstances, the safeguards of a warrant would only minimally advance Fourth Amendment interests," making Detective Schroeder's viewing of the video "reasonable." *Jacobsen*, 466 U.S. at 125.

Indeed, allowing Detective Schroeder to view the video furthers Fourth Amendment interests. In the extremely unlikely event of an erroneous report, Detective Schroeder would have noticed the error and closed the investigation. If he needed a warrant to view the video, then he may have prepared and executed a search warrant on Gasper's home and electronic devices without viewing the video. The CyberTip's report combined with Detective Schroeder's training and experience would establish probable cause. *See Cartier*, 543 F.3d at 446. Even the Second Circuit in *Maher*, while refusing to apply the private-search doctrine, agreed that the hash value match reported by the CyberTip would have "demonstrated probable cause to support warrants for [the government's] own searches of Maher's *Google accounts and residence*." *Maher*, 120 F.4th at 319 (emphasis added). This result, however, would be puzzling. It is more *reasonable* to enable officers to view the flagged video before obtaining a search warrant for the individual's home to spare innocent individuals from the significant invasion occasioned by a search of the home. *Tullberg*, 359 Wis. 2d 421, ¶ 29.

D. The circuit court erred.

The circuit court erred both as a matter of law and fact in rejecting the private-search doctrine.

Legally, the circuit court erroneously read *Jacobsen* to require a human to "eyeball" the CSAM for the private-search doctrine to apply. (R. 56:2–5.) The circuit court effectively adopted Justice White's plain-view approach. *Jacobsen* explicitly rejected that approach because it refused to have the result "turn on the fortuity of whether the Federal Express" employees repackaged the box. *Jacobsen*, 466 U.S. at 120 n.17. By predicating the private-party doctrine on the "fortuity" of an ESP's employee's eyeballs, the circuit court ruled contrary to *Jacobsen*. The "eyeball" requirement is also irrational. As *Miller* observed, a person's "quick view" can

trigger the private-search doctrine. *Miller*, 982 F.3d at 431. It makes little sense to treat the pixel-by-pixel analysis offered by PhotoDNA differently than an individual person's cursory glance. *See id.*

The circuit court also erred as a matter of law by refusing to apply the private-search doctrine because of the undefined risk that the CyberTip lodged an erroneous report. (R. 56:5–6.) "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. The "virtual certainty" standard allows for the "remote or highly unlikely possibility" that the government agent finds something in addition to what the private party reported. *Rivera-Morales*, 961 F.3d at 11.

Even if the reliability of hash values mattered, the circuit court clearly erred as a matter of fact in finding them unreliable and rejecting the CyberTip. Most critically, the circuit court considered the wrong hash value program. The circuit court rejected the CyberTip because it found the MD-5 hash algorithm unreliable. (R. 56:5–6.) However, it also found that Snapchat "closed Gasper's account after Microsoft's PhotoDNA algorithm matched one set of identifying data of a video to a database of the identifying data of [CSAM]." (R. 56:1–2.) It therefore should have recognized that the reliability of MD-5 was irrelevant. It appears to have been confused by the fact that the CyberTip reported an MD-5 hash value for the flagged video. (R. 38:7; 56:5.) Gasper shares that confusion. (Gasper's Br. 7, 16–18.) However, an MD-5 hash value can be generated for any file. (R. 60:13.) The CyberTip simply ran that process for the flagged video. (R. 60:27, 150.) The CyberTip still stated that PhotoDNA detected the video.

(R. 38:4; 60:26–27.) The circuit court erroneously conflated those two separate facts.[6]

The circuit court also clearly erred in finding that the risk of "collision"—two different files having the same hash value—rendered hash values unreliable. (R. 56:5–6.) 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.)[7] He observed no evidence of hash value collision in this case and was not familiar with collisions afflicting PhotoDNA. (R. 60:139, 150.) Gasper did not even call an expert to substantiate his claimed risk of collision as one federal defendant did in a failed attempt to assail hash value matching. *See Cartier*, 543 F.3d at 446.

E. *Wilson* and *Maher* are unpersuasive.

The circuit court drew persuasive support from the Ninth Circuit's decision in *Wilson*. (R. 56:4–5.) The Second Circuit in *Maher* agreed with *Wilson*. Both *Wilson* and *Maher* misapply *Jacobsen*.

---

[6] Gasper asserts that Snapchat used MD-5 in his Statement of the Case, (Gasper's Br. 7, 16–18), but that alleged fact never features in any of his arguments. In any event, he does not even attempt to show that the circuit court clearly erred in finding that Snapchat used PhotoDNA. (R. 56:1–2.) The circuit court considered the underlying facts undisputed. (R. 56:1.)

[7] In *Miller*, one source calculated the risk of hash value collision as "1 in 9.2 *quintillion*." *United States v. Miller*, 982 F.3d 412, 430 (6th Cir. 2020); *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.").

Wilson cited *Jacobsen* for the following rule: "When the government views anything other than the specific materials that a private party saw during the course of a private search, the government search exceeds the scope of the private search." *Wilson*, 13 F.4th at 974. *Wilson* measured whether the government "saw" more than the private party by evaluating whether the investigator "learned" more information by viewing the files than provided by the private party. *Id.* at 972–74. With that understanding, *Wilson* held that the private-search doctrine did not apply because the CyberTip did not describe the specific ways in which the child victims had been sexually abused in the flagged CSAM files, but the investigator learned that information by viewing the files. *Id.* at 972–74. *Maher* adopted *Wilson*'s understanding and application of *Jacobsen*. *See Maher*, 120 F.4th at 314–15.

Wilson and *Maher* erroneously applied *Jacobsen* in two respects. First, they effectively adopted the circuit court's "eyeball" requirement, which is indistinguishable from the plain-view standard that *Jacobsen* rejected.

Second, *Wilson* and *Maher* erroneously made the investigating officer's subjective knowledge dispositive. It is true that *Jacobsen* applied the private-search doctrine because there was a "virtual certainty" that "nothing else of significance was in the package and that a manual inspection . . . would not tell [the DEA agent] anything more than he had already been told." *Jacobsen*, 466 U.S. at 119. However, *Wilson* and *Maher* turned *Jacobsen* on its head by turning the final clause about what the private party "told" the agent into the operative test. What the private party "told" the agent described *how* the agent acquired a "virtual certainty." *Id.* But it was that "virtual certainty" that compelled *Jacobsen*'s result, not how the agent acquired the virtual certainty.

Following *Wilson*, the Ninth Circuit implicitly rejected *Wilson*'s conception of *Jacobsen*. In *Phillips*, the Ninth Circuit explained that *Jacobsen*'s holding arose from that the fact

"that the DEA agent's search 'enabled [him] to learn nothing that had not previously been learned during the private search,' not that he ha[d] subjective knowledge of what was learned during the private search." *Phillips*, 32 F.4th at 870 (quoting *Jacobsen*, 566 U.S. at 120 (first alteration in original)). "The description of the DEA agent's knowledge simply made clear that he was not exceeding the private search." *Id.* "'As in other Fourth Amendment contexts,' then, the inquiry remains an 'objective one.'" *Id.* (citation omitted); *see Torres v. Madrid*, 592 U.S. 306, 317 (2021) ("[W]e rarely probe the subjective motivations of police officers in the Fourth Amendment context.").

Wilson and *Maher* also ignored the other courts 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 more thorough search may enable the trained officer to subjectively "learn" more than the lay private citizen. But that additional knowledge reflects specialized expertise, not an expanded search.

Wilson and *Maher* did not even correctly apply their own rule. Both decisions failed to grasp the significance of the fact that the ESPs had detected copies of *known* CSAM files that had previously been reviewed and memorialized in a database by their hash values. *Wilson*, 13 F.4th at 972; *Maher*, 120 F.4th at 314. The report of a known CSAM file is, thus, akin to a report of a known film. A CyberTip reporting a copy of the *The Godfather* would inform the reader that the flagged file contained known and previously-viewed content—even if the CyberTip did not provide the script to *The Godfather*. *See United States v. Holmes*, 121 F.4th 727, 745 (9th Cir. 2024) (Collins, J., dissenting) (equating a CyberTip's report of a known CSAM file to "enclosing a book in a sealed envelope . . . with a statement that the enclosed book

corresponds to a specific Library of Congress classification number").

Finally, *Wilson* and *Maher* both refused to address whether opening the CSAM was equivalent to the *de minimis* intrusion of the drug test in *Jacobsen*. *See Wilson*, 13 F.4th at 970–71, 978; *Maher*, 120 F.4th at 315–16. However, the drug test establishes that not all government intrusions that exceed the private party's search offend the Fourth Amendment. *Wilson* and *Maher* erred by ignoring this important point.

F. Gasper's arguments miss the point.

Gasper largely fails to address the private-search doctrine or Detective Schroeder's viewing of the CSAM video. Instead, he assails the affidavit in support of the search warrant. (Gasper's Br. 32–37.) The validity of the search warrant is not presently at issue.

Construing Gasper's argument charitably, he adopts *Wilson* and *Maher*. He argues that because Detective Schroeder learned more about the CSAM in the video by viewing it than by reading the CyberTip—as illustrated by his affidavit supporting the search warrant—Detective Schroeder expanded Snapchat's private search. (Gasper's Br. 37.) As just explained, that understanding of *Jacobsen* is wrong. Gasper provides no additional argument to conclude otherwise.

Gasper may also be arguing that the CyberTip failed to establish a virtual certainty because it reported only "suspected" CSAM. (Gasper's Br. 35, 37–38.) He is wrong. The CyberTip reported "Apparent Child Pornography." (R. 38:1.) The use of "Apparent" is not an equivocation. It is a legal term of art. Federal law requires Snapchat to report an "apparent violation" of child pornography, 18 U.S.C. § 2258A(a)(2)(A), after obtaining "actual knowledge" of it, *id.*

§ 2258A(a)(1)(A)(i). Accordingly, "Apparent Child Pornography" meant that Snapchat believed that it had actual knowledge that the video in Gasper's account was CSAM, triggering its duty to report. "In the context of [Snapchat's] statutory obligations, . . . apparent is used synonymously with 'obvious.'" *United States v. Lowers*, 715 F. Supp. 3d 741, 754 n.4 (E.D.N.C. 2024).

* * *

Gasper's case presents "a fact pattern common in internet child pornography cases." *Silverstein*, 378 Wis. 2d 42, ¶ 5. The circuit court's private-search doctrine ruling would have two significant statewide consequences if adopted by this Court. First, it would lead to a dramatic increase in the number of search warrants sought by law enforcement just to view CSAM attached to CyberTips. Second, investigators may opt to proceed directly to obtaining a search warrant for the suspect's home and electronic devices based on the CyberTip without first viewing the reported file. Neither consequence is reasonable. Therefore, neither consequence is compelled by the Fourth Amendment.

III. Even if a Fourth Amendment violation occurred, the exclusionary rule should not apply.

If the State's two arguments fail, this Court should still reverse the suppression order because the exclusionary rule should not apply. 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.)[8]

[8] The State and circuit court referred to this issue as the "good faith exception," which is not uncommon. *State v. Burch*, 2021 WI 68, ¶ 21 n.6, 398 Wis. 2d 1, 961 N.W.2d 314. However, "[t]he Supreme Court's most recent cases do not use that phrase as a catchall for cases where exclusion is improper, and do not

"The fact that a Fourth Amendment violation occurred—i.e., that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rule applies." *Herring v. United States*, 555 U.S. 135, 140 (2009). "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.* at 144. The rule applies when the conduct is "deliberate, reckless, or grossly negligent" or the result of "recurring or systemic negligence." *Id.* "But when the police act with an objectively 'reasonable good-faith belief' that their conduct is lawful, or when their conduct involves only simple, 'isolated' negligence, the 'deterrence rationale loses much of its force', and exclusion cannot 'pay its way.'" *Davis v. United States,* 564 U.S. 229, 238 (2011) (citation omitted); *see State v. Burch*, 2021 WI 68, ¶¶ 16–18, 398 Wis. 2d 1, 961 N.W.2d 314. (discussing *Davis* and *Herring*).

This Court should decline to apply the exclusionary rule to Detective Schroeder's viewing of the CSAM video. At the time, the viewing of the video was not a Fourth Amendment violation because it had not been addressed by any Wisconsin court. *Reddick*, *Miller*, and several state courts had held that it was lawful to open the video. The only adverse authority was *Wilson*, and Detective Schroeder had been instructed at a training that he did not have to follow *Wilson* because it did not bind Wisconsin. (R. 60:154–55.) For these reasons, *Maher* concluded that the exclusionary rule should not apply. *Maher*, 120 F.4th at 321–23.

Because Detective Schroeder reasonably viewed a video based on his training in an area of unsettled law, "there is nothing concerning under Fourth Amendment doctrine with how [he] conducted [himself]." *Burch*, 398 Wis. 2d 1, ¶ 25. The

---

describe their conclusion that exclusion was inappropriate as applying a 'good faith' exception." *Id.*

societal cost of exclusion is disproportionate to the potential Fourth Amendment violation and therefore should not apply. *See id.*

Gasper contends that Detective Schroeder was trained to deliberately ignore binding Supreme Court law, but that assertion depends on his assumption that his case is a cell phone case. (Gasper's Br. 40–42.) It is not.

CONCLUSION

This Court should affirm the decision of the court of appeals reversing the circuit court's order granting suppression, and remand for further proceedings in the circuit court.

Dated this 1st day of July 2025.

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)
michael.conway@wisdoj.gov

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 10,951 words.

Dated this 1st day of July 2025.

Electronically signed by:

Michael J. Conway
MICHAEL J. CONWAY

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 this 1st day of July 2025.

Electronically signed by:

Michael J. Conway
MICHAEL J. CONWAY