**COURT OF APPEALS**
**DECISION**
**DATED AND FILED**

**October 30, 2024**

**Samuel A. Christensen**
**Clerk of Court of Appeals**



**Appeal No. 2023AP2319-CR** **Cir. Ct. No. 2023CF470**

**STATE OF WISCONSIN** **IN COURT OF APPEALS**
**DISTRICT II**

**STATE OF WISCONSIN,**

**PLAINTIFF-APPELLANT,**

**V.**

**MICHAEL JOSEPH GASPER,**

**DEFENDANT-RESPONDENT.**

APPEAL from an order of the circuit court for Waukesha County: SHELLEY J. GAYLORD, Reserve Judge. *Reversed and cause remanded*.

Before Gundrum, P.J., Neubauer and Lazar, JJ.

¶1 NEUBAUER, J. The State of Wisconsin appeals from an order granting Michael Joseph Gasper's motion to suppress. The primary issue is whether a law enforcement officer's warrantless inspection of a cyber tip digital

video file provided to the officer and identified as child pornography by a private internet service provider constituted an unreasonable search in violation of the Fourth Amendment. We conclude that Gasper did not have a reasonable expectation of privacy in the video, and thus, the officer's inspection was not a search subject to the Fourth Amendment. Accordingly, we reverse the suppression order and remand this matter for further proceedings consistent with this opinion.

## BACKGROUND

¶2 On January 13, 2023, the electronic service provider (ESP) Snapchat[1] submitted a report to the CyberTipline of the National Center for Missing and Exploited Children ("NCMEC"), as required by federal law.[2] Snapchat detected a child pornography video that had been "saved, shared, or uploaded" to Gasper's Snapchat account. The video was not made public, and no one else saw it. Snapchat detected the video using Microsoft's PhotoDNA program that scans files to determine if they are copies of known and reported

[1] Snapchat is a social media platform where users can "share text, photographs, and video recordings, collectively known as 'snaps.'" ***Commonwealth v. Carrasquillo***, 179 N.E.3d 1104, 1109 (Mass. 2022). While Snap, Inc. is the entity identified in Snapchat's terms of service and incorporation documents discussed herein, for ease of reading we refer to both the platform and entity as Snapchat.

[2] "In order to reduce ... and ... prevent the online sexual exploitation of children," federal law requires ESPs like Snapchat to report to NCMEC "any facts or circumstances from which there is an apparent violation of ... child pornography [statutes]" "as soon as reasonably possible after obtaining actual knowledge of any [such] facts or circumstances." 18 U.S.C. §§ 2258A(a)(1)(A)(i), (a)(2)(A), 2510(15), 2258E. The contents of that report are left to the discretion of the provider but may include, inter alia, email addresses, internet protocol (IP) addresses, geographic location information, and descriptions of the identified images. ***Id.*** § 2258A(b). NCMEC then forwards the CyberTip report to the appropriate law enforcement agency for possible investigation. ***Id.*** § 2258A(c).

child pornography based on their "hash values."[3] The submission to NCMEC indicated the presence of "Apparent Child Pornography" stored in the Snapchat user account and listed Gasper's subscriber information—his username, IP address, email address, and date of birth. That same day, Snapchat locked Gasper's account. No person from Snapchat or NCMEC opened the video.

¶3 NCMEC traced the IP address tied to Gasper's account to Wisconsin and thus sent the CyberTip report to the Wisconsin Department of Justice (DOJ). Other than the video, the CyberTip did not include any content from Gasper's account. A DOJ policy analyst opened the video and prepared and submitted an administrative subpoena to Gasper's internet service provider seeking the name and mailing address associated with Gasper's IP address.

[3] "A hash value is an algorithmic calculation that yields an alphanumeric value for a file." ***United States v. Stevenson***, 727 F.3d 826, 828 (8th Cir. 2013). We have described hash values as a "digital signature." ***State v. Baric***, 2018 WI App 63, ¶5, 384 Wis. 2d 359, 919 N.W.2d 221. The algorithm derives the hash value by analyzing all the "bits" of data in a particular file. Software programs can scan a file, derive its hash value, and compare that hash value to a database of hash values of known child pornography files. *See* ***id.***, ¶6 (describing such a program). PhotoDNA can detect slightly altered copies of known child pornography files. The CyberTip report indicated that the video linked to Gasper's Snapchat account was a hash match of a file containing child pornography.

As the federal district court in ***United States v. Lowers***, 715 F. Supp. 3d 741, 748 (E.D.N.C. Feb. 5, 2024), recently explained:

> As for a hash search's capacity to identify contraband, "hash searches are like dog sniffs but even better." Dennis Martin, *Demystifying Hash Searches*, 70 STAN. L. REV. 691, 717 (2018); *see also* Rebekah A. Branham, *Hash It Out: Fourth Amendment Protection of Electronically Stored Child Exploitation*, 53 AKRON L. REV. 217, 219 (2019) (citing evidence that the chance of two different files sharing the same hash value "is less than one in one billion").

¶4 Detective David Schroeder then received a copy of the CyberTip video. He opened the single video and confirmed that it depicted child pornography. Schroeder confirmed that Gasper occupied the residence connected to the IP address and that the available Wi-Fi networks outside Gasper's home were password protected and not publicly accessible. Using the information learned from the CyberTip video, Schroeder prepared and executed a search warrant at Gasper's home. Police seized electronic devices from Gasper's home and took him into custody. Gasper waived his ***Miranda***[4] rights and admitted that he had accessed additional child pornography files on his phone.

¶5 Gasper was charged with ten counts of possessing child pornography.[5] He filed a motion to suppress seeking exclusion of the Snapchat video because Schroeder opened it without a warrant or exception. He also sought to suppress the other child pornography evidence recovered from the search of his home as the fruit of a warrantless unconstitutional search of the Snapchat video.

¶6 Schroeder was the only witness to testify at the hearing on Gasper's motion to suppress. Schroeder described how PhotoDNA operates and recounted how he responded to the CyberTip. The State submitted into evidence Snapchat policies and guidelines that govern a user's use of Snapchat and that all users, including Gasper, must agree to upon creating a Snapchat account. These policies banned child pornography and informed users that Snapchat was actively scanning

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

[5] Gasper was also charged with nine counts of sexual exploitation of a child, although this appeal concerns only Gasper's claim that all child pornography evidence should be suppressed.

for child pornography and that Snapchat will report discovery of the same to NCMEC and law enforcement.

¶7 The circuit court granted Gasper's motion to suppress the video and all the child pornography evidence discovered pursuant to the warrant that relied on the video. The court determined that Gasper had a reasonable expectation of privacy because he used a cell phone to access Snapchat, citing ***Riley v. California***, 573 U.S. 373 (2014) and ***Carpenter v. United States***, 585 U.S. 296 (2018). The State appeals the order granting suppression.

## DISCUSSION

### Gasper Lacked a Reasonable Expectation of Privacy in a Child Pornography Video That He Uploaded to Snapchat in Violation of Its Terms of Service.

¶8 Gasper contends that the circuit court properly granted his motion to suppress because he had a reasonable expectation of privacy in the CyberTip video from his Snapchat account. The State contends that Gasper failed to show an objectively reasonable expectation of privacy sufficient to establish that the search violated his Fourth Amendment rights. As we now explain, we agree that Gasper failed to meet his burden to establish an objectively reasonable expectation of privacy in the video. Thus, Detective Schroeder's visual inspection of the video was not a search subject to the Fourth Amendment.

### I. Standard of Review

¶9 On review of a motion to suppress evidence, we uphold the circuit court's factual findings unless they are clearly erroneous. ***State v. Tentoni***, 2015 WI App 77, ¶6, 365 Wis. 2d 211, 871 N.W.2d 285. Whether the government conduct at issue constitutes a search, and if so, whether that search passes

constitutional muster, are questions of law to be decided de novo. ***Id.***; *see also* ***State v. Garcia***, 195 Wis. 2d 68, 73, 535 N.W.2d 124 (Ct. App. 1995).

## II. Fourth Amendment Principles: Reasonable Expectation of Privacy

¶10 The Fourth Amendment protects against unreasonable searches and seizures by the government. U.S. CONST. amend. IV; *see also* WIS. CONST. art. I, § 11.[6] Fourth Amendment rights are personal and may not be asserted vicariously. ***State v. Bruski***, 2007 WI 25, ¶22 n.3, 299 Wis. 2d 177, 727 N.W.2d 503. A search occurs for the purpose of the Fourth Amendment "when an expectation of privacy that society is prepared to consider reasonable is infringed." ***State v. Purtell***, 2014 WI 101, ¶21, 358 Wis. 2d 212, 851 N.W.2d 417 (quoting ***United States v. Jacobsen***, 466 U.S. 109, 113 (1984)). Thus, a person challenging a search bears the burden of establishing by a preponderance of the evidence that he or she has a reasonable expectation of privacy in the area or object of the challenged search. ***Tentoni***, 365 Wis. 2d 211, ¶7; ***Bruski***, 299 Wis. 2d 177, ¶22. The privacy interest is both subjective and objective: a defendant must show he or she subjectively expected privacy in the area or object, and the expectation is one that society recognizes as reasonable. ***Tentoni***, 365 Wis. 2d 211, ¶7. Failure to establish either defeats the defendant's motion to suppress. *See* ***State v. Baric***, 2018 WI App 63, ¶18 n.5, 384 Wis. 2d 359, 919 N.W.2d 221.

[6] The Wisconsin Supreme Court "generally follows the United States Supreme Court's interpretation of the search and seizure provision of the Fourth Amendment in construing Article I, Section 11 of the Wisconsin Constitution." ***State v. Bruski***, 2007 WI 25, ¶20 n.1, 299 Wis. 2d 177, 727 N.W.2d 503.

¶11 With regard to the objective prong, we consider the following nonexclusive factors in determining whether the totality of circumstances shows that a person has a reasonable 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). "[T]he reasonableness of an expectation of privacy in digital files shared on electronic platforms is determined by considering the same factors as in any other Fourth Amendment context." ***Baric***, 384 Wis. 2d 359, ¶19.

## III. Application to Gasper

¶12 As an initial matter, we note that the circuit court did not address either the subjective or the objective inquiries in regard to the video in Gasper's Snapchat account. Instead, the court relied on ***Riley*** (requiring a warrant to search arrestees' cell phones) and ***Carpenter*** (requiring probable cause to obtain cell-site records) to conclude that Gasper had a reasonable expectation of privacy in the video in his Snapchat account because he accessed it with his cell phone. However, Snapchat acquired the video from Gasper's Snapchat account, not his phone. That made Gasper's Snapchat account the relevant "area" that was searched. *See* ***State v. Bowers***, 2023 WI App 4, ¶¶26, 44-45, 405 Wis. 2d 716, 985 N.W.2d 123 (2022).

¶13 In ***Bowers***, we analyzed whether the defendant had a reasonable expectation of privacy in his Dropbox account, a cloud-based storage account that

he created with his work email address. ***Bowers***, 405 Wis. 2d 716, ¶¶1-3. We noted that the Dropbox account was a digital version of a physical storage container that could be accessed from "one device or a thousand devices." ***Id.***, ¶¶26- 27. That conclusion turned on the features of the Dropbox account, not the device that Bowers used to access it. *See* ***id.***, ¶¶20, 21-27, 40-42 ("We therefore address only whether Bowers' expectation of privacy *in his* [*a*]*ccount* was objectively reasonable" (emphasis added)). The Dropbox account was not tied to a "'physical device of any kind' and was not stored on county property or controlled by the county." ***Id.***, ¶27. Because the cloud-based storage center was password protected, and Bowers did not share the content of his account with anyone other than those he chose to, we concluded that Bowers had a reasonable expectation of privacy. *See* ***id.***, ¶¶21, 45.

¶14 As relevant here, we rejected the State's argument that because Bowers created the account with his county government email address and his employer could access the Dropbox account through the email address, Bowers lacked a reasonable expectation of privacy. ***Id.***, ¶¶22, 42. We explained that the county "did not search its own devices to access the information in Bower's [a]ccount; it used the internet as a tool to access the outside server on which the [a]ccount was located." ***Id.***, ¶42. Thus, the relevant "area" for purposes of determining whether Bowers had a reasonable expectation of privacy was the Dropbox account, not the device used by Bowers to access it. *See* ***id.***, ¶¶17, 20, 40.

¶15 This analysis applies here. Snapchat did not access the video in Gasper's account through his cell phone. Rather, the video was obtained directly from Gasper's Snapchat account. 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. Thus, the relevant question is whether Gasper had a reasonable expectation of privacy in the video in his Snapchat account.

¶16 He did not. As noted above, at the motion to suppress hearing, the State introduced three documents that show that Snapchat informed Gasper that it would be scanning and accessing his account for content that violated its terms of service (such as child pornography) and would report violations to law enforcement: (1) the "Snap Inc. Terms of Service"; (2) Snapchat's "Community Guidelines"; and (3) its "Sexual Content Community Guidelines Explainer Series" (the "Sexual Content Explainer").

¶17 The Terms of Service forbid using Snapchat "in any way not expressly permitted by these Terms or [the] Community Guidelines." They also forbid users from "violat[ing] any applicable law … in connection with [their] use of" Snapchat. By making an account, users specifically authorize Snapchat to "access, review, screen, and delete [their] content at any time and for any reason." The Terms of Service also contain a section entitled "Safety" that provides that if a user fails to comply with the Terms of Service, Snapchat "reserve[s] the right to remove any offending content, terminate or limit the visibility of your account, and notify third parties—including law enforcement—and provide those third parties with information relating to your account." At multiple points the Terms of Service contain a hyperlink to the Community Guidelines.

¶18 The Community Guidelines prohibit "any activity that involves sexual exploitation or abuse of a minor." They require that users "[n]ever post, save, send, forward, distribute, or ask for nude or sexually explicit content involving anyone under the age of 18." Snapchat explains that it will "report all instances of child sexual exploitation to authorities, including attempts to engage

in such conduct." The Community Guidelines refer users and provide a hyperlink to the Sexual Content Explainer "[f]or more information about sexual conduct and content that violates [the] Community Guidelines."

¶19 The Sexual Content Explainer restates Snapchat's prohibition on any content or activity related to the sexual exploitation of a child. It also has a paragraph describing how it scans user accounts and reports child pornography to NCMEC, just as it did in this case:

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

¶20 Gasper has failed to satisfy his burden to prove either his subjective or an objective expectation of privacy. First, as to any subjective expectation of privacy, 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.[7] Other than Schroeder's affidavit that established Gasper's Wi-Fi was password protected, there is no factual basis to conclude that Gasper had a subjective expectation of privacy in the video.

¶21 Even if Gasper had opted to testify to a subjective expectation, the Snapchat policies make it clear that any subjective expectation of privacy would be unfounded. This dooms Gasper's challenge. The evidence presented to the

[7] While Gasper submitted an affidavit, the circuit court ruled that it was inadmissible. Gasper does not challenge that ruling on appeal, and thus, has abandoned any effort to rely on the affidavit.

circuit court showed that Gasper agreed to terms that he violated by saving, sharing, or uploading a child pornography video to his account. Snapchat informed him that it would be scanning and accessing his account for content that violated the terms of service like child pornography and would report violations to NCMEC, as required by federal law, and to law enforcement. The terms to which Gasper agreed vitiate any claimed subjective expectation of privacy.

¶22 To further explain, even if Gasper had attested to a subjective expectation of privacy in the Snapchat video, that expectation would be objectively unreasonable given Snapchat's policies regarding sexual content in general and sexually explicit content involving children in particular. As to the first two factors identified in ***Bruski***, Snapchat's terms limited Gasper's property interest in his account, which prohibited him from saving, sharing, or uploading child pornography to his account. *See* ***Bruski***, 299 Wis. 2d 177, ¶27 (considering property interest in the object of the search). That conduct was obviously unlawful.

¶23 As to the third factor, Snapchat's Terms of Service, Community Guidelines, and Sexual Content Explainer limited Gasper's dominion and control over his account when it came to child pornography. *See* ***id.***, ¶¶27-28 (considering dominion, control, and the right to exclude others). Gasper agreed that Snapchat could monitor his account for content violations, and Snapchat reserved the right to access offending accounts, actively scan for child pornography, delete content and terminate his account, and advised that it would report child pornography to the authorities. Thus, Gasper could not exclude Snapchat from his account when it came to child pornography.

¶24 As to the fourth and fifth factors, even if his account were password protected, Gasper acknowledged that Snapchat expressly denied him permission, control, or privacy with respect to child pornography, no matter what precautions he took. *See* ***id.***, ¶¶24, 28 (considering "precautions customarily associated with those seeking privacy" and whether "property was put to some private use"). Finally, Gasper has failed to identify any historical notion of privacy for a child pornography video that has no lawful purpose. *See* ***id.***, ¶30 (considering historical notions of privacy).

¶25 While no Wisconsin court has addressed this issue, several federal district courts have determined that when a user agrees to an ESP's terms of service that advise that child pornography is prohibited content, the ESP would be scanning and accessing the account for violations of the terms, and the ESP would report violations to law enforcement, the user has no reasonable expectation of privacy in the child pornography in his or her account. *See, e.g.,* ***United States v. Lowers***, 715 F. Supp. 3d 741, 753-54 (E.D.N.C. Feb. 5, 2024) (collecting federal district court cases).

¶26 As one federal district court concluded, "given the prohibitions and reservations of rights in [Snapchat's] Terms of Service and Community Standards, even for the CyberTips involving uploaded images and videos whose contents were not 'publicly available,' a reasonable person would not have viewed files containing prohibited content as private." ***United States v. Tennant***, No. 23-CR-79, 2023 WL 6978405, at *9 (N.D.N.Y. Oct. 10, 2023) (denying motion to suppress child pornography recovered in searches of defendant's Snapchat and other social media accounts).

¶27 Another federal district court reached the same conclusion, reasoning that Yahoo's and Google's terms of service warned a defendant that he "risked being reported to law enforcement or NCMEC if either discovered that he sent, received, or distributed apparent child pornography. Even if Defendant believed that his [content was] private, society is not prepared to recognize that belief as reasonable given the Terms of Service …." ***United States v. Brillhart***, No. 22-CR-53, 2023 WL 3304278, at *8 (M.D. Fla. May 7, 2023) (denying motion to suppress evidence of child pornography recovered from defendant's Yahoo and Google accounts); *see also* ***United States v. Colbert***, No. 23-CR-40019, 2024 WL 2091995, **8-9 (D. Kan. May 9, 2024) (concluding that defendant lacked a reasonable expectation of privacy in child pornography on his Snapchat account because Snap, Inc.'s Terms of Service warned him that unlawful information related to his account could be released to law enforcement and its Community Guidelines warned him that child sexual exploitation would be reported to authorities); *but see* ***United States v. Coyne***, 387 F. Supp. 3d 387, 396 (D. Vt. 2018) (concluding that defendant retained a reasonable expectation of privacy in his Microsoft, Yahoo, and Chatstep accounts because the user agreements failed to specifically inform him that his content would be disclosed "to NCMEC and its law enforcement partners").

¶28 We agree with the conclusion reached in ***Lowers***, ***Tennant***, ***Brillhart***, and ***Colbert***. Gasper's agreement to Snapchat's Terms of Service, Community Guidelines, and Sexual Content Explainer vitiated any subjective expectation of privacy he might have had in the child pornography saved to his account. Even if he had testified to such a belief, that expectation is not objectively reasonable. Accordingly, Gasper has not met his burden in

demonstrating that any expectation of privacy in the video was either subjectively or objectively reasonable.

## CONCLUSION

¶29 Detective Schroeder's viewing of the video that accompanied the CyberTip did not constitute a search under the Fourth Amendment. Because the viewing of the video was not subject to the Fourth Amendment, the search warrant subsequently issued based on the video was also valid. The suppression order is therefore reversed, and this case is remanded for further proceedings consistent with this opinion.[8]

*By the Court*.—Order reversed and cause remanded.

Recommended for publication in the official reports

[8] Because we determine that no Fourth Amendment "search" occurred, we need not reach the additional grounds the State sets forth for reversal, including an exception to the warrant requirement based on a private party search conducted by Snapchat and the good faith exception to the exclusionary rule. *See* ***State v. Blalock***, 150 Wis. 2d 688, 703, 442 N.W.2d 514 (Ct. App. 1989) (cases should be decided on narrowest possible ground).