Appeal No. 2024AP469-CR **Cir. Ct. No. 2022CF495**

WISCONSIN COURT OF APPEALS
DISTRICT IV

STATE OF WISCONSIN,

PLAINTIFF-RESPONDENT,

V.

ANDREAS W. RAUCH SHARAK,

DEFENDANT-APPELLANT.

CERTIFICATION BY WISCONSIN COURT OF APPEALS

Before Kloppenburg, P.J., Graham, and Taylor, JJ.

Pursuant to WIS. STAT. RULE 809.61 (2021-22),[1] this appeal is certified to the Wisconsin Supreme Court for its review and determination.

Issues

This appeal broadly concerns whether Fourth Amendment safeguards are implicated when an electronic service provider (ESP) scans for and reviews digital files in an individual's account that are flagged as child pornography; and when law enforcement subsequently opens and views any flagged files that the ESP sent

[1] All references to the Wisconsin Statutes are to the 2021-22 version.

to the National Center for Missing and Exploited Children (NCMEC).[2] In a case involving similar facts, the Wisconsin Court of Appeals recently determined that the Fourth Amendment is not implicated because, based on the ESP's terms of service, the account holder has no reasonable expectation of privacy in any files in the account that contain child pornography. *See* ***State v. Gasper***, 2024 WI App 72, ___ Wis. 2d ___, ___ N.W.3d ___, petition for review pending (Appeal No. 2023AP2319-CR).

The ***Gasper*** decision has been published, and we are bound to follow it. However, while the ***Gasper*** court may have reached the right result (the file and derivative evidence should not be suppressed), we believe that it did so for the wrong reason (because the account holder has no reasonable expectation of privacy in the file based solely on the ESP's terms of service). In our view, the ***Gasper*** court's analysis of an account holder's reasonable expectation of privacy is not only contrary to existing precedent and legally incorrect, but it also undermines Fourth Amendment protections and falls short of providing a workable framework to guide future cases.

Therefore, we certify this appeal to the Wisconsin Supreme Court to address the following issues:

> 1. Whether a person who holds an electronic account with an ESP retains a reasonable expectation of privacy, as to the government, in files that the ESP obtains from the account, despite terms of service that provide that the ESP will scan the account for illegal content and may report such content to law enforcement.

[2] In addition to the Fourth Amendment of the United States Constitution, the arguments in this case also address Article I, Section 11 of the Wisconsin Constitution. However, for the sake of brevity, we refer exclusively to the Fourth Amendment throughout this certification.

> 2. Whether an ESP's scan and review of files in a person's electronic account constitute a private search or a government search under ***State v. Payano-Roman***, 2006 WI 47, 290 Wis. 2d 380, 714 N.W.2d 548.
>
> 3. Whether a law enforcement officer is required to obtain a warrant before opening and viewing any files that the ESP sent to NCMEC, which then sent the files to law enforcement.

This appeal provides an opportunity for the Wisconsin Supreme Court to establish a clear and cogent framework for addressing Fourth Amendment issues in this digital evidence context. Also, as part of its consideration of the second and third issues, this appeal provides the court with the opportunity to apply Wisconsin's private search doctrine in this context, and to clarify the holding of ***Payano-Roman*** in light of the many federal cases that address this topic.[3]

Rauch Sharak's Appeal

Google is an ESP, and Google Photos is one of the electronic services that it provides. Andreas Rauch Sharak, who is the defendant in this case, maintained a Google Photos account.

[3] *See, e.g.*, ***United States v. Cameron***, 699 F.3d 621, 637-38 (1st Cir. 2012) (concluding that an ESP's independent review of files in an individual's account was a private search); ***United States v. Richardson***, 607 F.3d 357, 363-67 (4th Cir. 2010) (same); ***United States v. Meals***, 21 F.4th 903, 907 (5th Cir. 2021) (same); ***United States v. Sykes***, 65 F.4th 867, 877 (6th Cir. 2023), cert. denied, 144 S. Ct. 576 (2024) (same); ***United States v. Berbis***, 4 F.4th 551, 561-62 (7th Cir. 2021) (same); ***United States v. Stevenson***, 727 F.3d 826, 828-30 (8th Cir. 2013) (same); ***United States v. Ringland***, 966 F.3d 731, 736-37 (8th Cir. 2020) (same). *But compare* ***United States v. Maher***, 120 F.4th 297, 312-20 (2d Cir. 2024) (the ESP's search was private, but law enforcement's subsequent search fell outside the private search exception); ***United States v. Wilson***, 13 F.4th 961, 971-75 (9th Cir. 2021) (same); *with* ***United States v. Reddick***, 900 F.3d 636, 638-40 (5th Cir. 2018) (the ESP's search was private, and law enforcement's subsequent search fell within the private search exception); ***United States v. Miller***, 982 F.3d 412, 422-26, 427-32 (6th Cir. 2020) (same).

Google automatically scans digital files that are uploaded by its users for certain "hash values." We have previously described hash values as "digital signatures" that can be used to identify known files of child pornography. *See* ***Gasper***, ___ Wis. 2d ___, ¶2 n.3 (citing ***State v. Baric***, 2018 WI App 63, ¶5, 384 Wis. 2d 359, 919 N.W.2d 221). When Google's scan detects a file with the same hash value as a known child pornography file, the file is flagged, and Google obtains the file from the user's account. On some occasions a Google employee may view a file that has been flagged to confirm that it contains apparent child pornography, and on other occasions the file may not be viewed by anyone at Google. Consistent with its terms of service, Google then sends the file, along with a "CyberTip" that is prepared by a Google employee, to NCMEC, which provides the CyberTip and the file to local law enforcement.[4]

Here, the parties agree that, in the course of scanning files that Rauch Sharak uploaded to his Google Photos account, Google's scan flagged several digital files with the same hash values as known child pornography files. Google obtained the files from Rauch Sharak's account, and it submitted a CyberTip to NCMEC along with the digital files and the name, mobile number, and email that were associated with the account. The CyberTip also identified the IP addresses that were associated with the uploads. It represented that a Google employee

[4] Rauch Sharak argues that the State failed to provide the terms of service that applied to his Google Photos account, but he does not meaningfully dispute that the terms prohibited users from "creat[ing], upload[ing], or distribut[ing] content that exploits or abuses children," including "all child sexual abuse materials." Nor does he meaningfully dispute that the terms of service provided that Google "will remove such content and take appropriate action, which may include reporting to [NCMEC], limiting access to product features, and disabling accounts."

"viewed the file[s] to the extent necessary to confirm that [they] contained apparent child pornography."[5]

NCMEC sent Google's CyberTip and the digital files that accompanied the CyberTip to the Wisconsin Department of Justice, which issued a WIS. STAT. § 165.505 administrative subpoena to the Internet Service Provider associated with the IP addresses identified in the CyberTip. The subpoena requested the names and addresses of the customers and subscribers associated with those IP addresses. The Internet Service Provider responded by providing Rauch Sharak's name and his address in Jefferson County, and the case was referred to the Jefferson County Sheriff's Office.

Following the referral, a Jefferson County detective opened the digital files that accompanied the CyberTip and visually confirmed that they contained apparent child pornography. The detective then applied for and obtained a warrant to search Rauch Sharak's residence, to seize any digital devices located at the residence, and to search and analyze those devices. Law enforcement executed the warrant and found more child pornography.

Rauch Sharak was charged with possession of child pornography. As relevant here, he moved to suppress "all evidence and any leads derived from the

[5] In this respect, the facts of this appeal differ from the facts in ***State v. Gasper***, 2024 WI App 72, ___ Wis. 2d ___, ___ N.W.3d ___. There, the file in question was scanned and obtained by Snapchat, but no person from Snapchat viewed the file before submitting the CyberTip and digital files to NCMEC. ***Id.***, ¶2. This distinction may matter for purposes of an analysis of the private search doctrine as applied to law enforcement's subsequent viewing of the file—there is a split of federal authority on that question. *Compare* ***Reddick***, 900 F.3d at 638-40; ***Miller***, 982 F.3d at 428-32; *with* ***Maher***, 120 F.4th at 312-20; ***Wilson***, 13 F.4th at 971-72. However, this distinction would not appear to make any difference to an analysis of whether the user has a reasonable expectation of privacy in files in the user's account, or to an analysis of whether the ESP's conduct constitutes a private or government search.

warrantless search of [his] digital files by … Google ….” After receiving the State’s response, the circuit court issued a thorough written decision. It rejected the State’s argument that Rauch Sharak lacks a reasonable expectation of privacy in the digital files in his account based on Google’s terms of service. The court nevertheless denied the motion to suppress, concluding that Google’s scan and review of the flagged files in Rauch Sharak’s account constituted a private search that was not subject to the Fourth Amendment. It further concluded that, although Rauch Sharak retains a reasonable expectation of privacy and the Fourth Amendment applies to the Jefferson County detective’s review of the files, the detective did not need a warrant to open and view the files under the private search doctrine.

On appeal, Rauch Sharak contends that the circuit court misapplied ***Payano-Roman***, which establishes the Wisconsin test for determining whether a search conducted by a private party should be deemed a government search. He argues that a web of federal laws and regulations amount to government encouragement and participation in Google’s search, such that it should be deemed a government search that is subject to the Fourth Amendment. Although every federal court to consider this precise question has concluded that an ESP’s scan of user content is a private search, Rauch Sharak contends that the test set forth in ***Payano-Roman*** compels a contrary result.

In its response, the State argues that the circuit court properly rejected Rauch Sharak’s argument that Google’s actions should be deemed a government search. In addition, the State seeks affirmance on an alternative ground—that

Rauch Sharak has no reasonable expectation of privacy in the digital files in his account that violate Google's terms of service.[6]

If we were not bound to follow ***Gasper*** and were instead writing on a blank slate, we would likely affirm the order denying the suppression motion based on the following conclusions. First, Google's actions (that is, scanning digital files that are uploaded to Google Photos accounts, obtaining and reviewing files that have the same hash values as known child pornography files, and sending such files to NCMEC) constituted a private search. In other words, Google's actions should not be deemed a government search, and were not subject to the Fourth Amendment. Second, although Rauch Sharak could not reasonably expect Google to refrain from sending the files to NCMEC based on the terms of service, he nevertheless retains a reasonable expectation of privacy as to the content of the files once they are in the hands of law enforcement. Therefore, the Jefferson County detective's warrantless visual review of the files was a "search" for Fourth Amendment purposes. Finally, the detective's warrantless search, which replicated Google's private search, fell within the private search doctrine, which is a recognized exception to the warrant requirement. Accordingly, the detective's actions did not violate the Fourth Amendment.

[6] In this appeal, as it did in ***Gasper***, the State also contends that the circuit court's order denying the motion to suppress could be affirmed on another alternative ground—the good faith exception to the exclusionary rule. *See* ***Maher***, 120 F.4th at 307-23 (concluding that the defendant retained a reasonable expectation of privacy as against the government in the suspected child pornography in his Google account, and that the law enforcement search was not exempted from the Fourth Amendment's warrant requirement because the law enforcement search did not merely replicate a prior private search, but nevertheless concluding that the evidence should not be suppressed based on the good faith exception to the exclusionary rule). We do not discuss the good faith exception further in this certification.

The Gasper Decision

As mentioned, the Wisconsin Court of Appeals recently issued a published decision that compels a different analysis. *See* ***Gasper***, ___ Wis. 2d ___. In that case, Gasper maintained an electronic account with Snapchat, which is an ESP. ***Id.***, ¶2. Like Google, Snapchat scans its users' accounts for files with the same hash values as known images of child pornography, and its scan flagged a video file in Gasper's account. ***Id.***, ¶2 & n.3. Without opening the file, a Snapchat employee sent a CyberTip with the file to NCMEC, which sent the tip and file to the Wisconsin Department of Justice. ***Id.***, ¶¶2-3. Through an administrative subpoena, the Department determined that the file had been uploaded from an IP address that was associated with Gasper's residence, and it provided that information, along with the file, to local law enforcement. ***Id.***, ¶¶3-4. A local law enforcement officer opened the file and confirmed that it contained suspected child pornography; the officer then applied for and obtained a warrant to search Gasper's residence. ***Id.***, ¶4. Gasper was criminally charged based on the evidence obtained in the search. ***Id.***, ¶5.

Gasper argued that the video file from Snapchat and all of the evidence obtained in the search of his residence should be suppressed because the law enforcement officer opened the file without a warrant. ***Id.***, ¶5. To support his motion to suppress, Gasper argued that he had uploaded the file to Snapchat from his cell phone, where he had a reasonable expectation of privacy. *See* ***id.***, ¶7. The circuit court granted the motion on the grounds that, under ***Riley v. California***, 573 U.S. 373 (2014), and ***Carpenter v. United States***, 585 U.S. 296 (2018), Gasper had a reasonable expectation of privacy in content he accessed from his cell phone. ***Gasper***, ___ Wis. 2d ___, ¶7. On appeal, the ***Gasper*** court reversed the order suppressing the evidence.

In its decision, the ***Gasper*** court first resolved a dispute about the "area" of the challenged search. *See* ***id.***, ¶10 (citing ***State v. Tentoni***, 2015 WI App 77, ¶7, 365 Wis. 2d 211, 871 N.W.2d 285, for the proposition that "a person challenging a search bears the burden of establishing … that he or she has a reasonable expectation of privacy in the area or object of the challenged search"). The court concluded that, because "Snapchat acquired the video from Gasper's Snapchat account," the account was the "relevant 'area' that was searched." ***Id.***, ¶12; *see also* ***id.***, ¶15 ("Snapchat did not access the video in Gasper's account through his cell phone. Rather, the video was obtained [by Snapchat] 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.").

Although it concluded that the account was the area that was searched, the ***Gasper*** court did not explicitly consider whether Gasper has a reasonable expectation of privacy in *his account*. Rather, the court considered whether he had a reasonable expectation of privacy in *the specific video file* that Snapchat obtained from the account and sent to NCMEC.[7]

To answer that question, the court considered Snapchat's terms of service. ***Id.***, ¶¶16-28. Those terms explicitly stated that Snapchat "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." ***Id.***, ¶16; *see also*

[7] It is established that users may have an objectively reasonable expectation of privacy in the accounts that they maintain with an ESP. *See* ***State v. Bowers***, 2023 WI App 4, ¶26, 405 Wis. 2d 716, 985 N.W.2d 123 (2022).

id., ¶¶17-19 (detailing the provisions of Snapchat's terms of service). More specifically, the terms provided: "We report violations of [Snapchat policies addressing child sexual exploitation] to [NCMEC], as required by law. NCMEC then, in turn, coordinates with domestic or international law enforcement, as required." ***Id.***, ¶19.

Based on those terms of service, the court determined that Gasper had no reasonable expectation of privacy in any file that he uploaded to his account that violated the terms of service, and that he could not reasonably expect that he could "exclude Snapchat from his account *when it came to child pornography*." ***Id.***, ¶23 (emphasis added). Throughout the decision, the ***Gasper*** court repeatedly emphasized that the reason Gasper lacked an expectation of privacy in the video file was based on the terms of service and the specific content of the video file.[8]

Although not directly stated by the ***Gasper*** court, we understand it to have concluded that, because Gasper could not reasonably expect to exclude *Snapchat* from his account when it came to child pornography, he also had no reasonable expectation of privacy *as to the government*. The court ultimately determined that the law enforcement officer's actions in opening and viewing the file "did not constitute a search under the Fourth Amendment." ***Id.***, ¶29.

[8] *See* ***Gasper***, ___ Wis. 2d ___, ¶22 ("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"); ***id.***, ¶23 ("Gasper could not exclude Snapchat from his account when it came to child pornography"); ***id.***, ¶24 ("Snapchat expressly denied him permission, control, or privacy with respect to child pornography"); ***id.***, ¶28 (the terms of service "vitiated any subjective expectation of privacy he might have had in the child pornography saved to his account").

We believe that the ***Gasper*** court's Fourth Amendment analysis is legally incorrect. Specifically, we conclude that the court erred in three respects.

First, the court's determination that the Snapchat account was the "relevant area that was searched" for Fourth Amendment purposes is inaccurate and could create confusion when applied in future cases. The Fourth Amendment applies to government actors, not to private entities. ***Payano-Roman***, 290 Wis. 2d 380, ¶17; *see also* ***State v. Cameron***, 2012 WI App 93, ¶23, 344 Wis. 2d 101, 820 N.W.2d 433. Yet no government official searched Gasper's account—it is undisputed that it was Snapchat, a private entity, that scanned the account for certain hash values and obtained the flagged video file from the account. ***Gasper***, ___ Wis. 2d ___, ¶¶2, 12. The law enforcement officer did not open and view the video file in question until Snapchat removed it from Gasper's account. ***Id.***, ¶4.[9]

[9] By concluding that the *account* was the relevant area that was searched, the ***Gasper*** court could be interpreted as having implicitly determined, without analysis, that Snapchat is acting as *an agent or instrumentality of the government* when it scans its users' accounts and reviews any flagged files. That implicit determination would follow because, without some government activity, the Fourth Amendment is not implicated and no further analysis is needed. *See* ***Payano-Roman***, 290 Wis. 2d 380, ¶19. In other words, there is no need to consider whether a search of an account violates the Fourth Amendment if the entity that searches the account is not acting as an agent or instrumentality of the government.

However, the issue of whether an ESP (Snapchat in ***Gasper*** and Google in this ***Rauch Sharak*** appeal) acts as an agent of the government when it scans and reviews files in a user's account is hotly contested in this ***Rauch Sharak*** appeal. Any implicit determination that the ***Gasper*** court might have made would be contrary to every federal decision cited by the parties that considered this issue. *See infra* n.1; *see also* ***United States v. Brillhart***, No. 2:22-CR-53-SPC-NPM, 2023 WL 3304278, at *5 (M.D. Fla. May 7, 2023); ***United States v. Tennant***, No. 5:23-CR-79 (BKS), 2023 WL 6978405, at *12 (N.D.N.Y. Oct. 10, 2023). Consider ***Maher***, which was released the same day as the ***Gasper*** decision. There, the court referred to "Google's private algorithmic search," ***Maher***, 120 F.4th at 301, and it emphasized that its decision "suggest[ed] no constitutional limitation on Google's own ability, as a private actor, to search for and remove child pornography on its platform," ***id.*** at 320.

Second, the ***Gasper*** court's determination that contract terms between private persons or entities (that is, Gasper and Snapchat) can eliminate a person's reasonable expectation of privacy against government action is concerning. If not corrected, the implications of the ***Gasper*** decision could be profound.

If the terms of service eliminated Gasper's reasonable expectation of privacy as to the government, it would seem to follow that law enforcement would be free to search his electronic account without obtaining a warrant. This could have far-reaching implications in the digital context, given the modern prevalence of using digital files and electronic accounts with third-party providers to manage a person's "houses, papers, and effects." *See* U.S. CONST. amend. IV. Moreover, such an analysis would not appear to be on firm footing in other non-digital contexts. Consider, as an example, an agreement to lease an apartment. Many leases prohibit the tenant from engaging in illegal activities on the premises and, as part of a lease, tenants often agree that the landlord can enter the premises under certain circumstances and may report illegal activity to law enforcement. Yet, we would not expect any court to conclude that, as a result of agreeing to those contract terms, tenants lose their reasonable expectation of privacy in the apartment as to the government, such that law enforcement officers could search the apartment without a warrant when no warrant exception applies.

We acknowledge the existence of some cases that could be read to suggest that a person loses the reasonable expectation of privacy when the person uploads files that violate an ESP's terms of service. *See* ***Gasper***, ___ Wis. 2d ___, ¶¶25-27 (citing several federal district court cases). Yet, most of these cases also address the private search doctrine, which authorizes a government actor to repeat a search that was previously conducted by a private party without securing a warrant. *See, e.g.*, ***United States v. Brillhart***, No. 2:22-CR-53-SPC-NPM, 2023 WL 3304278, at

5-7 (M.D. Fla. May 7, 2023). In such cases, it is the prior private search, not the terms of service, that result in the loss of a reasonable expectation of privacy. *See* ***id.* at *8 (citing ***United States v. Odoni***, 782 F.3d 1226, 1238 (11th Cir 2015), for the proposition that "[a]n individual does not have a reasonable expectation of privacy in an object to the extent the object has been searched by a private party"); *see also* ***id.*** at *7 (citing ***United States v. Jacobson***, 466 U.S. 109, 117 (1984), which first articulated the private search doctrine for the proposition that "[o]nce frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information").

As applied to the facts of ***Gasper***, we think that the legally correct Fourth Amendment analysis is as follows. Snapchat's search of Gasper's account for files containing hash values consistent with child pornography was a private search that did not implicate the Fourth Amendment. Law enforcement lawfully came into possession of the file (that is, it seized the file for Fourth Amendment purposes) because it lawfully received the file from Snapchat. The fact that Gasper entered into a contract stating that Snapchat could turn such files over to law enforcement did not eliminate Gasper's reasonable expectation of privacy, as to the government, in the content of the file. Law enforcement was required to obtain a warrant to search the files unless an exception to the warrant requirement applied. That determination should turn on the arguments about the private search doctrine that the parties raised in ***Gasper*** but that the ***Gasper*** court did not address.

Finally, we question the soundness of any analysis in which the reasonable-expectation-of-privacy determination depends on the specific content of a file. Although the ***Gasper*** court emphasizes that the reason Gasper did not have any expectation of privacy in a video file was based on its content, we cannot think of any other context in which the analysis of the existence of a reasonable

expectation of privacy depends on whether the item that is found in a search area is or is not contraband. And we question how, as a practical matter, a content-based distinction would work. Presumably, a person would maintain a reasonable expectation of privacy if the account does not contain any files that violate an ESP's terms of service, but one does not know whether the files in any account violate any terms of service unless and until the files are searched.

Accordingly, for these reasons, we certify this appeal to the Wisconsin Supreme Court.