FILED
06-13-2025
CLERK OF WISCONSIN
SUPREME COURT

STATE OF WISCONSIN

IN SUPREME COURT

Case No. 2024AP469-CR

STATE OF WISCONSIN,

Plaintiff-Respondent,

v.

ANDREAS W. RAUCH SHARAK,

Defendant-Appellant.

ON CERTIFICATION BY THE COURT OF APPEALS FROM DEFENDANT'S APPEAL OF A JUDGMENT OF CONVICTION ENTERED IN JEFFERSON COUNTY CIRCUIT COURT, THE HONORABLE WILLIAM F. HUE, PRESIDING

# BRIEF OF PLAINTIFF-RESPONDENT

JOSHUA L. KAUL
Attorney General of Wisconsin

MICHAEL J. CONWAY
Assistant Attorney General
State Bar #1134356

Attorneys for Plaintiff-Respondent

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

**Statutes**

**Other Authorities**

## INTRODUCTION

The State charged Andreas W. Rauch Sharak with possessing child pornography after Google detected files depicting child sexual abuse material (CSAM) in his Google Photos account and reported them. A detective viewed the files to confirm that they were CSAM. Rauch Sharak moved to suppress the CSAM. The circuit court denied the motion, and Rauch Sharak appealed.

This appeal primarily concerns dueling affirmative arguments. Rauch Sharak maintains that Google acted as a government agent and, thus, violated the Fourth Amendment by searching his account for CSAM without a warrant or warrant exception. The State disagrees, contending that Google acted as a private party. In addition, the State argues that Rauch Sharak lacked a reasonable expectation of privacy in the CSAM because he agreed to Google's Terms of Service, and those Terms deprived him of the right to exclude with respect to CSAM.

While Rauch Sharak's appeal was pending, the court of appeals accepted the State's reasonable-expectation-of-privacy argument in a different case that is now before this Court: *State v. Gasper*. A different panel of the court of appeals certified Rauch Sharak's appeal because it disagreed with *Gasper* but recognized that it was bound to apply it and, consequently, accept the State's reasonable-expectation-of-privacy argument. The panel certified three issues: (1) the State's reasonable-expectation-of-privacy argument; (2) Rauch Sharak's government-agent argument; and (3) whether a law enforcement officer may view CSAM files reported by an electronic service provider without a warrant. As he did in the court of appeals, however, Rauch Sharak does not address the third issue. While the third issue arises in *Gasper*, it is undisputed here that the detective could lawfully view the reported CSAM files pursuant to the private-search

doctrine—even if Rauch Sharak had a reasonable expectation of privacy in them. Rauch Sharak just disputes whether Google was, in fact, a private party.

This Court should bless *Gasper* and reject Rauch Sharak's arguments. Rauch Sharak cannot prove an objectively reasonable expectation of privacy in the CSAM from his Google Photos account because he agreed to terms that banned CSAM and provided for both the monitoring and reporting of CSAM within that account. Twenty courts have already rejected Rauch Sharak's government-agent argument because federal law specifically advises electronic service providers that they have no affirmative duty to search for CSAM on their platforms. This Court should therefore affirm.

## ISSUES PRESENTED

1. Did Rauch Sharak prove that he had a reasonable expectation of privacy in the CSAM files?

The circuit court answered: Yes.

This Court should answer: No.

2. Did Google act as a government agent when it scanned Rauch Sharak's account for CSAM?

The circuit court answered: No.

This Court should answer: No.

3. If a Fourth Amendment violation occurred, should the exclusionary rule apply?

The circuit court answered: Yes.

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 here.

## STATEMENT OF THE CASE

The material facts are undisputed. (R. 36:1–2.) Google sent a CyberTipline Report ("CyberTip") to the National Center for Missing and Exploited Children (NCMEC), reporting four CSAM videos that Rauch Sharak had uploaded to his Google Photos account. (R. 31:4–7, 39–42.)[1] A Google employee had opened the files and reviewed them "to the extent necessary to confirm that [they] contained apparent child pornography." (R. 31:6.) The IP address came from Palmyra, Wisconsin. (R. 31:8.) NCMEC referred the CyberTip to the Wisconsin Department of Justice (DOJ). (R. 31:13.)

DOJ issued an administrative subpoena to Rauch Sharak's internet service provider and assigned the CyberTip to the Jefferson County Sheriff's Office. (R. 31:14, 18–21.) The administrative subpoena returned an address where Rauch Sharak resided. (R. 31:23, 40.) A detective with the Jefferson County Sheriff's Office viewed the four videos attached to the CyberTip. (R. 31:14, 39–42.) He then prepared a search warrant for Rauch Sharak's residence and his personal digital devices. (R. 31:25–47.) Officers seized Rauch Sharak's smart phone, which contained 15 CSAM files. (R. 36:2.) The State charged Rauch Sharak with 15 charges of possessing child pornography. (R. 2:7–9.)

Rauch Sharak moved to suppress the CSAM. (R. 25.) He argued that Google acted as a government agent, which

[1] Google Photos "is a service that allows users to upload photos to a cloud storage account." *State v. Fristoe*, 489 P.3d 1200, 1202 n.1. (Ariz. Ct. App. 2021).

meant that Google had to comply with the Fourth Amendment. (R. 25:26–37.) While this claim raised an issue of first impression in Wisconsin, Rauch Sharak conceded that every other court to consider the issue had ruled contrary to his position in the same circumstances. (R. 25:30–31 & n.24.) These courts all deemed the electronic service providers (ESPs) private actors because federal law expressly provides that ESPs have no affirmative obligation to scan their platforms for CSAM. (R. 25:30 (citing 18 U.S.C. § 2258A(f).) Nonetheless, Rauch Sharak maintained that these courts had erred by failing to recognize that several other federal statutes "functionally compelled" Google to scan for CSAM. (R. 25:28.) Because Google lacked a warrant or warrant exception, Rauch Sharak maintained that the CSAM reported by Google had to be suppressed. (R. 25:38.)

The State countered that Rauch Sharak lacked a reasonable expectation of privacy in the CSAM files attached to the CyberTip. (R. 29:3–7.) The State cited to Google's Terms of Service and other policies that Rauch Sharak accepted by creating his Google Photos account. Those terms barred users from uploading CSAM to Google's platform, advised users that Google scans user accounts for content violations, and warned users that Google would remove CSAM and "take appropriate action," (R-App. 4), which included reporting to NCMEC and law enforcement, (R. 31:72–74, 81; R-App 3–4).[2] The State also argued that Google did not act as a government

[2] In the circuit court, the State erroneously submitted the "Abuse Program Policies and Enforcement" applicable to Google Drive rather than Google Photos. The State corrected the error in an appendix at the court of appeals because the "Child Sexual Abuse and Exploitation" policies for Google Drive and Google Photos are identical. (R. 31:72; R-App. 3–4.) The State again provides those terms in an appendix. Rauch Sharak has not disputed the content of any of Google's policies. (Certification 4 n.4.)

agent, and, even if it did, the exclusionary rule should not apply. (R. 29:9–12, 14–16.)

The circuit court denied Rauch Sharak's motion to suppress without a hearing. (R. 36.) The circuit court determined that Rauch Sharak had a reasonable expectation of privacy in the four files reviewed by law enforcement. (R. 36:7.) It concluded that Rauch Sharak had failed to prove that Google acted as a government agent. (R. 36:8–21.) While the court accepted that the federal laws cited by Rauch Sharak amounted to government encouragement for ESPs to search for CSAM, it nevertheless concluded that Google acted as a private entity under the totality of the circumstances. (R. 36:15–21.) It concluded that the detective lawfully viewed the CSAM files pursuant to the private-search doctrine because he viewed the files that a Google employee had already viewed. (R. 36:21–23.)

The circuit court also addressed the applicability of the exclusionary rule. It found that law enforcement reasonably relied on and conformed with existing caselaw outside of Wisconsin. (R. 36:26.) It found that there was no police misconduct. (R. 36:26.) Nevertheless, the circuit court stated that if its order denying suppression were reversed, then it would apply the exclusionary rule to address an issue of recurring or systemic negligence. (R. 36:26.)

Rauch Sharak subsequently pleaded guilty to 5 of the 15 counts. (R. 56:1.) The other 10 counts were dismissed and read in at sentencing. (R. 56:5.) The circuit court imposed an evenly bifurcated six-year sentence that it stayed for appeal. (R. 56:1–2.) Rauch Sharak appealed the denial of his suppression motion.

While Rauch Sharak's appeal was pending, the court of appeals issued and published *State v. Gasper*, 2024 WI App 72, 414 Wis. 2d 532, 16 N.W.3d 279, *review granted*, (2025 WI 16, Mar. 13, 2025). In *Gasper*, Snapchat detected a CSAM

video in the defendant's account and reported it to NCMEC, which forwarded it to Wisconsin law enforcement. *Id.* ¶¶ 2–4. A Wisconsin detective viewed the video before obtaining a search warrant that led to discovering CSAM on the defendant's electronic devices. *Id.* ¶ 4. The court of appeals concluded that Gasper did not have an objectively reasonable expectation of privacy in the CSAM file because Snapchat's policies explicitly barred CSAM and informed users that Snapchat scanned for and reported CSAM to NCMEC and law enforcement. *Id.* ¶¶ 8, 28.

After *Gasper*, a different panel of the court of appeals certified Rauch Sharak's appeal to this Court (the "Certification"). The Certification observed that it was bound to follow *Gasper* and, thus, affirm based on the State's reasonable-expectation-of-privacy argument. (Certification 2.) However, the Certification disagreed with *Gasper* because it concluded that Rauch Sharak "retains a reasonable expectation of privacy as to the content of the files once they are in the hands of law enforcement." (Certification 7.) The Certification would still have affirmed the order denying suppression because Google conducted a private search, and the detective's viewing of the CSAM fell within the private-search doctrine. (Certification 7.)

This Court granted certification.

## SUMMARY OF ARGUMENT

This Court should affirm the order denying suppression for two reasons.

First, Rauch Sharak lacked a reasonable expectation of privacy in the CSAM files because Google's Terms of Service deprived him of the right to exclude and other rights intrinsic to an expectation of privacy with respect to CSAM. The Terms required Rauch Sharak to agree to Google's prohibition on CSAM, consent to Google's monitoring of his account for

CSAM, and accept that Google would act on CSAM, which included reporting to NCMEC. Rauch Sharak cannot establish an objectively reasonable expectation of privacy in the CSAM files that the detective viewed after Google removed and reported them pursuant to the Terms. Similarly, even if Google acted as a government agent, Google did not intrude upon a reasonable expectation of privacy when it scanned Rauch Sharak's account because Rauch Sharak consented to monitoring by a government agent by agreeing to the Terms. Contrary to the Certification's concern, this result is consistent with other cases that have used property law to evaluate the reasonableness of an expectation of privacy. Rauch Sharak created a bailment with Google by uploading files to his account. Since bailments are governed by contract, Google's Terms of Service inform the reasonableness of Rauch Sharak's claim of privacy.

Second, Google acted as a private party when it searched Rauch Sharak's account. Twenty courts have already rejected Rauch Sharak's contrary argument. He nevertheless asks this Court to become a conspicuous outlier based on his theory that a web of federal statutes implicitly encouraged Google to search for CSAM. However, he fails to acknowledge that federal law specifically tells ESPs that they have no duty to search for CSAM. Rauch Sharak cannot reconcile his theory of implicit encouragement with this explicit disclaimer, nor does he attempt to. Instead, he claims that the circuit court was bound to apply a strict three-factor test rather than evaluate the totality of the circumstances. This Court's precedent, however, unambiguously directs courts to consider the totality of the circumstances.

This Court can affirm the order denying suppression for either of these two reasons. Because Rauch Sharak cannot prove a reasonable expectation of privacy, no Fourth Amendment search occurred, and it is immaterial whether Google acted as a government agent. Alternatively, even if

Rauch Sharak had a reasonable expectation of privacy, he failed to prove that Google acted as a government agent. Because Rauch Sharak does not challenge the circuit court's application of the private-search doctrine to the detective's viewing of the CSAM files, his failure to establish that Google acted as a government agent ends the analysis. The State encourages this Court to address both issues anyway because they recur in CSAM prosecutions.

Finally, even if Rauch Sharak 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. Rauch Sharak lacked a reasonable expectation of privacy in the four flagged CSAM files.

The Fourth Amendment to the United States 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 a reasonable expectation of privacy in the area searched. *Id.* ¶¶ 22–23. Rauch Sharak failed to prove that he had an objectively reasonable expectation of privacy in the four CSAM videos.

### A. Rauch Sharak lacked an objectively reasonable expectation of privacy in the CSAM files viewed by the detective because Google's Terms deprived him of the right to exclude with respect to CSAM.

This Court has identified the following, non-exclusive factors to help determine 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 a digital "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. *Gasper* correctly recognized that this expectation of privacy does not necessarily extend to individual files viewed outside the account. The court correctly concluded that defendant Gasper lacked an objectively reasonable expectation of privacy in a CSAM video that a detective viewed outside of Gasper's account after Snapchat reported it pursuant to its policies. *Gasper*, 414 Wis. 2d 532, ¶¶ 16, 22, 28.

Three of Snapchat's user policies animated *Gasper*'s ruling. 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 that violates Snapchat's content policies or the law. *Id.* ¶ 17 (alteration in original). Second, the Snapchat Community Guidelines expressly prohibited all content involving sexually explicit content with a minor and informed users that Snapchat reports such content to law enforcement. *Id.* ¶ 18. Third, the Sexual Content Explainer reiterated Snapchat's prohibition on CSAM and stated that Snapchat

reports all CSAM to NCMEC. *Id.* ¶ 19. Given these policies, any subjective expectation of privacy would have been "objectively unreasonable." *Id.* ¶ 22.

Snapchat's terms deprived Gasper of the property interests underlying the *Bruski* factors. Snapchat's terms "limited Gasper's property interest in his account which prohibited him from saving, sharing, or uploading child pornography." *Gasper*, 414 Wis. 2d 532, ¶ 22. The terms limited Gasper's right to exclude, dominion, and control because they allowed Snapchat to monitor and access Gasper's account for CSAM. *Id.* ¶ 23. Snapchat's policies barred Gasper from taking precautions consistent with a privacy interest to secure CSAM. *Id.* ¶ 24. Rather, Snapchat retained the right to circumvent 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 user policies, the legal conclusion rests on how those policies restricted Gasper's right to exclude. A property-law analogue for the relationship between an individual user and an ESP 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 relationship between an individual user and an ESP is akin to a 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 with 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 a person'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 previously considered bailment law 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 the 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, just like the relationship between an individual and the purveyor of a safety deposit box. *See* D'Onfro, *supra*, at 128. Moreover, Gasper allowed Snapchat to secure and 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 the Terms of Service—to determine the scope of Gasper's right to exclude and, thus, his reasonable expectation of privacy. The Terms of Service required Gasper to relinquish his right to exclude Snapchat from CSAM and agree to having Snapchat scan for and report CSAM. Stated another way, Snapchat refused to facilitate the storage or transmission of CSAM in its role as bailee. By holding that Gasper lacked an objectively reasonable expectation of privacy in the CSAM video viewed by law enforcement, the court of appeals merely gave effect to the bailment as defined by the express contract. *See Toyota Motor*, 332 Wis. 2d 201, ¶ 11.

*Gasper* applies to Rauch Sharak. Rauch Sharak created a bailment with Google by storing files within a Google Photos account. Google's Terms of Service governed the bailment. Just as in *Gasper*, the Terms required Rauch Sharak to relinquish his right to exclude with respect to CSAM and to consent to having his account monitored for CSAM. Google retained the right to remove content that violated its terms or the law, including "child pornography," specifically. (R. 31:59, 67.) Google's Privacy Policy instructed Rauch Sharak that Google would "analyze [his] content to help [Google] detect abuse such as spam, malware, and illegal content." (R. 31:81.) Google's policy on "Child Sexual Abuse and Exploitation" provided: "Do not create, upload, or distribute content that exploits or abuses children," which "includes all child sexual abuse materials." (R. 31:72; R-App. 3.) Google stated further: "We will remove such content and take appropriate action, which may include reporting to the [NCMEC]." (R. 31:73; R-App. 4.)

In this light, all six *Bruski* factors weigh against Rauch Sharak. When it came to the CSAM files, Rauch Sharak lacked a property interest, could not exclude, and could not exercise dominion and control. *See Bruski*, 299 Wis. 2d 177, ¶ 24 (factors one and three). He accepted that he could not

take precautions to exclude Google from his CSAM or 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)). Thus, Rauch Sharak lacked an objectively reasonable expectation of privacy in the four CSAM files viewed by the detective.

Rauch Sharak argues that *Gasper* improperly "federalizes" private contracts. (Rauch Sharak's Br. 18–19.) He overlooks *Byrd*. A reasonable expectation of privacy is not "a brooding omnipresence in the sky." *S. Pac. Co. v. Jensen*, 244 U.S. 205, 222 (1917) (Holmes, J., dissenting). It is derived from "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). An ESP's terms directly inform whether an individual's claimed expectation of privacy is rooted in personal property law or societal understandings.

Moreover, *Gasper*'s reliance on Snapchat's written policies protects ESP users from government overreach. *Gasper* does not necessarily extend to *any* content disclosed by an ESP to the government—either negligently or intentionally. "A bailee who uses the item in a different way than he's supposed to, or against the bailor's instructions, is liable for conversion." *Carpenter*, 585 U.S. at 399 (Gorsuch, J., dissenting). For example, if an individual entrusted a dog to a neighbor for care while traveling, it would be a breach for "the neighbor to put Fido up for adoption." *Id.* It follows that an ESP's disclosure of data not addressed by the terms of service or in violation of those terms would not necessarily deprive the user of a reasonable expectation of privacy in that

data. In this way, Snapchat's Terms of Service cabined *Gasper*'s scope.

Accordingly, Rauch Sharak lacked a reasonable expectation of privacy in the four CSAM files viewed by the detective. 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 act 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. *Gasper* applies with equal force to Google's search of Rauch Sharak's account if Google acted as a government agent.

Because Rauch Sharak lacked a reasonable expectation of privacy in the CSAM reported in the CyberTip, the detective's viewing of those files did not constitute a search under the Fourth Amendment. *See Gasper*, 414 Wis. 2d 532, ¶¶ 28–29. However, unlike in *Gasper*, Rauch Sharak raises another potential Fourth Amendment event—Google's search of his account. While this wrinkle requires additional analysis, it does not lead to a different result. Even if Google acted as a government agent, Rauch Sharak lacked a reasonable expectation of privacy in the CSAM files in his account pursuant to Google's Terms of Service.

If Google acted as a government agent, then its Terms of Service constituted a government policy that explicitly restricted Rauch Sharak's expectation of privacy in his account. Several courts have held that public employees subject to computer-use policies that allow the government employer to access the computer and bar unauthorized activity lack a reasonable expectation of privacy in the computer. *See United States v. Thorn*, 375 F.3d 679, 683 (8th Cir. 2004) (collecting cases) *vac'd on other grounds*, *Thorn v.*

*United States*, 543 U.S. 1112 (2005). If Google acted as a government agent, then Rauch Sharak similarly allowed a government agent to access his account to enforce its CSAM ban. (R. 31:72–74, 81; R-App 3–4.) "He chose to trade some privacy for a [Google Photos account]." *Medlock v. Trs. of Ind. Univ.*, 738 F.3d 867, 872 (7th Cir. 2013). Therefore, Rauch Sharak cannot prove that Google infringed a reasonable expectation of privacy in his account by scanning it for CSAM, even if Google acted as a government agent. Indeed, it appears that Rauch Sharak has argued himself into a corner. If Google acted as a government agent, then Rauch Sharak consented to that government agent scanning and accessing his account.

### C. The Certification has not identified flaws in *Gasper*'s reasoning.

The Certification disagreed with *Gasper*'s reasoning for three reasons. (Certification 11.) None of them call *Gasper* into doubt.

First, the Certification faulted *Gasper* for characterizing the Snapchat account as the "relevant area" that was "searched" but concluding that Gasper lacked a reasonable expectation of privacy in the CSAM video reviewed by the detective. (Certification 11.) The Certification erroneously collapsed two separate issues into one.

The "relevant area" presented a threshold issue. Gasper argued that he had a categorical reasonable expectation of privacy in the CSAM because he accessed Snapchat exclusively through his cell phone. *Gasper*, 414 Wis. 2d 532, ¶¶ 7, 12. That line of reasoning would render Snapchat's Terms of Service immaterial. *See id.* ¶ 12. *Gasper* rejected that argument because Snapchat detected the CSAM video by scanning Gasper's account, not his cell phone. *Id.* ¶ 15. That meant the "relevant area" was Gasper's Snapchat account, not his cell phone. *Id.*

After rejecting the cell phone argument, *Gasper* determined that Gasper lacked a reasonable expectation of privacy in the *video* viewed by the detective, holding that "[the detective's] *viewing of the video* that accompanied the CyberTip did not constitute a search under the Fourth Amendment." *Gasper*, 414 Wis. 2d 532, ¶ 29 (emphasis added). *Gasper* did *not* address Gasper's expectation of privacy in his Snapchat account because no government agent ever accessed it. *See id.* ¶¶ 3–4.[3]

Second, the Certification argued that *Gasper* ruled contrary to law by holding that private terms of service can void a person's expectation of privacy in a protected space. (Certification 12–13.) The Certification asserts that *Gasper* allows law enforcement to search an ESP user's account or a person's rented apartment without a warrant based on the ESP's terms of service or the tenant's lease. (Certification 12.) Rauch Sharak agrees. (Rauch Sharak's Br. 19.) Neither scenario will come to pass under *Gasper*.

Conceptually, these two examples are distinct from *Gasper*. In these two examples, law enforcement intrudes on a space that is unquestionably protected by the Fourth Amendment and finds contraband. *See Bowers*, 405 Wis. 2d 716, ¶ 26 (electronic account); *Florida v. Jardines*, 569 U.S. 1, 6 (2013) (home). The government then attempts to retroactively justify that intrusion by citing to a contract that generally prohibits illegal conduct. *See, e.g.*, *United States v. Washington* 573 F.3d 279, 284 (6th Cir. 2009). In *Gasper*, the inverse occurred. The detective never accessed Gasper's Snapchat account. *Gasper*, 414 Wis. 2d 532, ¶¶ 3–4. Instead,

---

[3] The Certification's related concern that *Gasper* could be construed as implicitly holding that Snapchat acted as a government agent is unnecessarily alarmist. (Certification 11 & n.9.) *Gasper* did not even consider—let alone decide—whether Snapchat acted as a government agent.

he viewed a single video of contraband attached to the CyberTip after Snapchat had already removed it from Gasper's account and then obtained a warrant for Gasper's home and devices. *Id.* ¶¶ 2–4. Had the detective wished to access Gasper's Snapchat account, he would have needed a warrant or warrant exception. *See Bowers*, 405 Wis. 2d 716, ¶ 45.

*Gasper* is consistent with how other cases have managed the intersection between a defendant's privacy interest and a third-party's property interest. In *United States v. Cunag*, 386 F.3d 888 (9th Cir. 2004), a police officer discovered drugs in the defendant's hotel room while accompanying a hotel employee. *Id.* at 890–91. The hotel employee had called the police and locked the defendant out of the room because he suspected the defendant of procuring the room through credit card fraud. *Id.* at 890. The Ninth Circuit concluded that the defendant's expectation of privacy in the hotel room had been extinguished by the hotel's "affirmative steps to repossess" and "assert dominion and control" over the room. *Id.* at 895. These "private acts of dominion" deprived the defendant of the right to exclude from the room. *Id.* (citation omitted). Here, Google's Terms of Service constituted private acts of dominion that deprived Rauch Sharak of a reasonable expectation of privacy in CSAM.

The Seventh Circuit considered similar principles in *United States v. Thomas*, 65 F.4th 922 (7th Cir. 2023). There, the defendant leased a condo in Georgia under a false identity while a fugitive. *Id.* at 923. The Seventh Circuit stated that "using an alias to sign a lease . . . does not by itself deprive a tenant of a legitimate expectation of privacy." *Id.* On the other hand, the landlord "retained an ownership interest in the property and was entitled to protect her interest from a fugitive." *Id.* at 924. 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"). *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.

Third, the Certification questioned how the reasonable expectation of privacy analysis could turn on the content of a file. (Certification 13–14.) The Certification states: "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." (Certification 14.) Rauch Sharak raises an almost identical concern. (Rauch Sharak's Br. 18.) These doubts arise from conflating the reasonable expectation of privacy in an ESP account with the reasonable expectation of privacy in an isolated CSAM file. *Gasper* did not hold that Gasper lost his reasonable expectation of privacy in his Snapchat account because it contained CSAM. Rather, it held that Gasper lacked a reasonable expectation of privacy "in the video" viewed by the detective. *Gasper*, 414 Wis. 2d 532, ¶ 28.

### D. Rauch Sharak's alternative argument is unpersuasive.

Rauch Sharak argues in the alternative that Google's Terms of Service were too vague to deprive him of a reasonable expectation of privacy in the CSAM. (Rauch Sharak's Br. 20.) He derives this argument from *United States v. Maher*, 120 F.4th 297 (2d Cir. 2024). There, the Second Circuit held that Google's then-existing terms did not deprive the defendant of a reasonable expectation of privacy in CSAM because the terms regarding the monitoring and reporting of CSAM were too equivocal. *Maher*, 120 F.4th at 307–09. In *Maher*, the Terms of Service stated that Google "'may' report 'illegal content' to 'appropriate authorities.'" *Id.* at 307 (citation omitted). They also stated that Google "does not necessarily . . . review content." *Id.* at 308–09 (alteration in original). However, *Maher* declined to "draw any categorical conclusions about how terms of service affect a user's expectation of privacy," limiting its holding to "Google's particular Terms of Service." *Id.* at 308.

Rauch Sharak acknowledges that he was subject to more specific terms than those in *Maher*. (Rauch Sharak's Br. 21.) The Terms of Service apprised Rauch Sharak that Google retained the right to remove "child pornography." (R. 31:67.) Google's Privacy Policy informed Rauch Sharak that Google would use "automated systems" to "detect abuse" like "illegal content." (R. 31:81.) Google's Child Sexual Abuse and Exploitation policy stated unambiguously: "Do not create, upload, or distribute content that exploits or abuses children," including "all child sexual abuse materials." (R. 31:72; R-App. 3.) Google then stated: "We will remove such content and take appropriate action, which may include reporting to the [NCMEC]." (R. 31:73; R-App. 4.)

Rauch Sharak claims that Google's use of "may" before "reporting to the [NMEC]" compels the same result as *Maher*. (Rauch Sharak's Br. 22.) He invests this single "may" with too

much significance. Google clearly stated that it "will remove [CSAM] and take appropriate action." (R. 31:73; R-App. 4.) One such "appropriate action" was filing a report with NCMEC. (R. 31:73; R-App. 4.) The fact that Google reserved the right to take actions other than or in addition to reporting to NCMEC did not render its commitment to "tak[ing] appropriate action" equivocal.

Rauch Sharak also claims that Google will take "appropriate action" only when it is "notified of unlawful activities," (Rauch Sharak's Br. 22 (quoting R. 31:73)), which implies that it may not report contraband found from its own investigation, (Rauch Sharak's Br. 22). This reading is strained. Nothing in the statement precludes Google from becoming "notified of unlawful activities" from its own investigation. (R. 31:73.)

* * * * *

The Certification and Rauch Sharak appear to fault *Gasper* for enabling law enforcement to invade private spaces without regard for the Fourth Amendment so long as law enforcement recovers contraband. *Gasper*, however, held only that an individual does not have a reasonable expectation of privacy in an individual CSAM file removed from an ESP account and sent to law enforcement when the ESP's user agreement banned CSAM, deprived the individual of the right to exclude with respect to CSAM, and advised the user that CSAM would be subject to action including reporting to the authorities. That holding reflects a considered application of *Bruski*. *Gasper*'s reasoning also applies to Rauch Sharak even if Google acted as a government agent because that means Rauch Sharak consented to a government agent monitoring his account for CSAM and acting on it. These limited conclusions do not compromise an individual's general expectation of privacy in an ESP account.

## II. Google did not act as a government agent.

### A. Rauch Sharak does not dispute the circuit court's application of the private-search doctrine to the detective's viewing of the CSAM.

The private-search doctrine is an exception to the Fourth Amendment's warrant requirement. 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.

Here, a Google employee viewed the CSAM files before reporting them. (R. 36:21.) When an employee of the ESP views a CSAM file before reporting it, federal courts agree that an investigator may view the same file without a warrant pursuant to the private-search doctrine. *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). The circuit court followed this consensus in concluding that the private-search doctrine applied to the detective's viewing of the CSAM files reported by Google that a Google employee had already viewed. (R. 36:21–23.)

Rauch Sharak does not challenge the application of the private-search doctrine to the detective. Instead, he argues that Google was a government agent, not a private actor. (Rauch Sharak's Br. 23–35.) Rauch Sharak's argument lacks merit.

### B. This Court should join other courts in concluding that an ESP acts as a private party when voluntarily searching its platform for CSAM.

Rauch Sharak bears the burden of proving that Google conducted a government search. *State v. Payano-Roman*, 2006 WI 47, ¶ 23, 290 Wis. 2d 380, 714 N.W.2d 548. All courts that have considered whether an ESP acts as a government agent when reporting CSAM discovered on its platform have held that the ESP acted in a private capacity.

Eight federal appellate circuits have reached this conclusion. *See United States v. Cameron*, 699 F.3d 621, 637–38 (1st Cir. 2012); *United States v. Richardson*, 607 F.3d 357, 366–67 (4th Cir. 2010); *United States v. Meals*, 21 F.4th 903, 907 (5th Cir. 2021); *United States v. Sykes*, 65 F.4th 867, 877 (6th Cir. 2023), *cert. denied*, 144 S. Ct. 576 (2024); *United States v. Miller*, 982 F.3d 412, 424–25 (6th Cir. 2020); *United States v. Bebris*, 4 F.4th 551, 561–62 (7th Cir 2021); *United States v. Ringland*, 966 F.3d 731, 736–37 (8th Cir. 2020); *United States v. Stevenson*, 727 F.3d. 826, 828–30 (8th Cir. 2013); *United States v. Rosenow*, 50 F.4th 715, 729–31 (9th Cir. 2022), *cert. denied*, 143 S. Ct. 786 (2023); *United States v. Rosenschein*, 136 F.4th 1247, 1254–55 (10th Cir. 2025). *United States v. Ackerman*, 831 F.3d 1292, 1306 (10th Cir. 2016) (Gorsuch, J.).

Six published federal district court opinions have reached this conclusion. *See United States v. Clark*, 673 F. Supp. 3d 1245, 1255 (D. Kan 2023); *United States v. Bohannon*, 506 F. Supp. 3d 907, 914–15 (N.D. Cal. 2020);

*United States v. Coyne*, 387 F. Supp. 3d 387, 398 (D. Vt. 2018); *United States v. Stratton*, 229 F. Supp. 3d 1230, 1238 (D. Kan. 2017); *United States v. Keith*, 980 F. Supp. 2d 33, 40 (D. Mass. 2013); *United States v. Green*, 857 F. Supp. 2d 1015, 1018–19 (S.D. Cal. 2012).

Two state supreme courts and four intermediate state appellate courts have reached this conclusion. *See State v. Pauli*, 979 N.W.2d 39, 51–52 (Minn. 2022); *State v. Lizotte*, 197 A.3d 362, 372 (Vt. 2018); *State v. Ingram*, 662 S.W.3d 212, 228 (Mo. Ct. App. 2023); *State v. Fristoe*, 489 P.3d 1200, 1205 (Ariz. Ct. App. 2021); *People v. Wilson*, 270 Cal. Rptr. 3d 200, 218 (Cal. Ct. App. 2020); *Burwell v. State*, 576 S.W.3d 826, 832 (Tex. Ct. App. 2019).

The cornerstone of this universal holding is 18 U.S.C. § 2258A(f)(3), which states that ESPs are not legally required to "affirmatively search, screen, or scan for facts or circumstances" of CSAM. *See, e.g.*, *Meals*, 21 F.4th at 907 (concluding that "this forceful statutory disclaimer" belied the defendant's claim that ESP was "a mandatory government agent"). The law requires that ESPs report "[a]pparent violations" of child pornography laws, 18 U.S.C. § 2258A(a)(2)(A), only after "obtaining actual knowledge" of the violations, 18 U.S.C. § 2258A(a)(1)(A)(i). All courts have concluded that this reporting requirement does not transform ESPs into government agents. *See, e.g.*, *Rosenow*, 50 F.4th at 730–31 (collecting cases). In fact, this statutory scheme incentivizes ESPs *not* to search for CSAM because intentional ignorance avoids triggering the reporting requirement. *See Ringland*, 966 F.3d at 736.

These courts have all ruled consistently with *Skinner v. Ry. Execs. Ass'n*, 489 U.S. 602, 614–15 (1989). *Skinner* held that federal regulations effectively mandating drug tests for employees of private railroads turned those private drug tests into government action. *Id.* at 615–16. The regulations achieved this effect by removing "all legal barriers to testing."

*Id.* at 615. Specifically, the regulations preempted any collective bargaining agreement that did not provide for the drug tests, prohibited railroads from negotiating the drug tests away, mandated discipline for employees who refused a drug test, and authorized the government to obtain the results of any drug test. *Id.*

The coercive elements of the regulations in *Skinner* are not replicated in 18 U.S.C. § 2258A. *See Rosenow*, 50 F.4th at 730–31 (collecting cases rejecting the comparison to *Skinner*). Federal law does not invest ESPs with authority that they otherwise lacked to scan their users' accounts. *Stevenson*, 727 F.3d at 830. The reporting requirement does not preempt terms of service that forbid such scans, bar ESP's from negotiating away the right to conduct scans, or dictate consequences for users who refuse to submit to scans. *Id.* Most importantly, the same statute that sets forth the reporting obligation also states that ESPs are not required to search for CSAM in the first place. 18 U.S.C. § 2258A(f)(3).

This Court need not belabor this analysis. All other courts have correctly concluded that ESPs do not act as government agents when they choose to scan their platforms for CSAM. This Court should join them and conclude that Google was a private actor in this case.

### C. *Payano-Roman* directs courts to consider the totality of the circumstances.

Rauch Sharak steers clear of the one-sided weight of authority. Instead, he argues that *Payano-Roman* bound the circuit court to deem Google a government actor based on a strict three-factor test. (Rauch Sharak's Br. 24–29.) This argument is meritless.

*Payano-Roman* clearly states that "[t]he question of whether a search is a private search or a government search is one that must be answered taking into consideration *the totality of the circumstances*." *Payano-Roman*, 290 Wis. 2d

380, ¶ 21 (emphasis added). *Payano-Roman* derived this rule from *Skinner* and the Seventh Circuit. *See id. Skinner* stated that "[w]hether a private party should be deemed an agent or instrument of the Government for Fourth Amendment purposes" presents "a question that can only be resolved '*in light of all the circumstances*.'" *Skinner*, 489 U.S. at 614 (emphasis added) (citation omitted). The Seventh Circuit similarly declared that the "analysis is made 'on a case-by-case basis and *in light of all the circumstances*.'" *United States v. Shahid*, 117 F.3d 322, 325 (7th Cir. 1997) (emphasis added) (citation omitted).

Unsurprisingly, *Payano-Roman* based its holding on all the facts and even listed every relevant fact. *Payano-Roman*, 290 Wis. 2d 380, ¶ 27. "Taking all of these circumstances into account," this Court concluded that the defendant had proven that a private party conducted a government search. *Id.* ¶ 28. This Court then reiterated that this holding arose from "consider[ing] all the circumstances of this case." *Id.* ¶ 29. *Payano-Roman* could not be clearer that determining whether a private actor was a government agent turns on the totality of the circumstances.

Rauch Sharak reads *Payano-Roman* differently by fixating on a single paragraph. He asserts that *Payano-Roman* adopted a strict three-factor test from a court of appeals decision, *State v. Rogers*, 148 Wis. 2d 243, 435 N.W.2d 275 (Ct. App. 1988). (Rauch Sharak's Br. 25.) Those three factors are:

> (1) the police may not initiate, encourage or participate in the private entity's search; (2) the private entity must engage in the activity to further its own ends or purpose; and (3) the private entity must not conduct the search for the purpose of assisting governmental efforts.

*Payano-Roman*, 290 Wis. 2d 380, ¶ 18 (quoting *Rogers*, 148 Wis. 2d at 246). According to Rauch Sharak, because the

circuit court concluded that federal law encouraged Google's search under factor one (R. 36:15–16), it was bound to deem Google a government agent, (Rauch Sharak's Br. 28–29). He insists that the "totality of the circumstances" statements describe how to apply the *Rogers* test. (Rauch Sharak's Br. 25.)

Rauch Sharak ignores *Payano-Roman*'s substance. This Court observed that "*Rogers* stated three requirements that must be met for a search to be a private search." *Payano-Roman*, 290 Wis. 2d 380, ¶ 18. That observation was not an endorsement. To the contrary, this Court focused on the totality of the circumstances and never referred to *Rogers*'s test again. *See id.* ¶¶ 21–29. *Payano-Roman* could hardly have elevated the *Rogers* test to the exclusive test for a private party's search without even applying it.

Rauch Sharak's argument reveals that this Court should jettison *Rogers*'s test. This Court does not need a special justification to do so because *Rogers* is a court of appeals decision. *Evers v. Marklein*, 2024 WI 31, ¶ 25, 412 Wis. 2d 525, 8 N.W.3d 395. Nonetheless, two justifications for departing from *stare decisis* apply to *Rogers*. *Rogers* "has become detrimental to coherence and consistency in the law" and is "unworkable in practice." *State v. Johnson*, 2023 WI 39, ¶ 20, 407 Wis. 2d 195, 990 N.W.2d 174 (citation omitted).

First, *Payano-Roman*'s quotation of *Rogers* appears to have led to a covert split in authorities in the court of appeals that undermines coherence and consistency in the law. Two decisions read *Payano-Roman* as adopting *Rogers*'s three "requirements" for a private actor's search to be a private search. *State v. Berggren*, 2009 WI App 82, ¶ 14, 320 Wis. 2d 209, 769 N.W.2d 110; *State v. Cameron*, 2012 WI App 93, ¶¶ 24–25, 344 Wis. 2d 101, 820 N.W.2d 433. Another decision accurately described *Payano-Roman* as articulating an inquiry based on the "totality of the circumstances" without mentioning *Rogers*. *State v. Cole*, 2008 WI App 178, ¶¶ 12, 19,

315 Wis. 2d 75, 762 N.W.2d 711. Still another decision read *Payano-Roman* as stating that a private search could be attributed to the government *either* through *Rogers or* by showing that the search was a "joint endeavor." *State v. Butler*, 2009 WI App 52, ¶ 13, 317 Wis. 2d 515, 768 N.W.2d 46 (citation omitted). These decisions reveal that *Rogers* has distracted litigants and courts from the totality of the circumstances. Overruling *Rogers*'s test would dispel this ambiguity.

Second, *Rogers*'s test is unsound in principle because no authorities support it. Most importantly, it is contrary to *Skinner*. *See Johnson*, 407 Wis. 2d 195, ¶ 24 (deeming prior decision "unsound in principle" because it incorrectly applied a U.S. Supreme Court decision). *Rogers* attributed its test to *State v. Bembenek*, 111 Wis. 2d 617, 331 N.W.2d 616 (Ct. App. 1983). *See Rogers*, 148 Wis. 2d at 246–47. However, *Bembenek* did not articulate a test of any kind. Rather, *Bembenek* clearly considered the totality of the circumstances. *See Bembenek*, 111 Wis. 2d at 631–34. *Rogers*'s first factor merely repeats *Bembenek*'s summation sentence in its concluding paragraph. *See id.* at 633–34. *Rogers*'s second and third factors have no relation to any reasoning in *Bembenek*. *See id.* at 631–34.

*Rogers*'s test is also unsound in principle on its own terms. By framing the inquiry as three factors that must be satisfied before a private party's search is legally a private search, *Rogers* implicitly imposes a presumption that the private search is a government search. That presumption is wrong. *Payano-Roman*, 290 Wis. 2d 380, ¶ 23. The three factors are also useless. The first factor is a legal conclusion disguised as an inquiry. *See Bembenek*, 111 Wis. 2d at 633–34. The second and third factors are redundant to each other. While the second factor asks whether the private party conducted the search for its own purposes, the third factor asks whether the private party conducted the search to assist the government. *Payano-Roman*, 290 Wis. 2d 380, ¶ 18. Those

are two sides of the same coin—the purpose of the private party's search.

For these reasons, this Court should retire *Rogers*'s three-pronged test. As the First Circuit has explained, it is imprudent to encumber a totality-of-the-circumstances inquiry with an arcane multi-factor test: "Because we see little upside in endorsing one multi-factor test or another, and still less in inventing a new one, we think it unnecessary to festoon the easily understood 'totality of the circumstances' standard with any multi-factor trappings." *Doe v. Mass. Inst. of Tech.*, 46 F.4th 61, 70 (1st Cir. 2022).

### D. The totality of the circumstances reveals that Google did not act as a government agent.

#### 1. Rauch Sharak misapplies the standard of review.

Initially, Rauch Sharak misapplies the standard of review. He treats the circuit court's interpretation of federal statutes as factual findings subject to clear error review. (Rauch Sharak's Br. 29–30.) However, it is well-established that questions of statutory interpretation are issues of law reviewed *de novo*. *State v. Stewart*, 2018 WI App 41, ¶ 18, 383 Wis. 2d 546, 916 N.W.2d 188. Rauch Sharak's position would threaten legal instability. The clearly erroneous standard affirms factual findings "even if contrary findings could also reasonably be made based on the same evidence." *Hennessy v. Wells Fargo Bank, N.A.*, 2020 WI App 64, ¶ 16, 394 Wis. 2d 357, 950 N.W.2d 877. Applying this standard of review to statutory interpretations would allow for two different circuit court judges to reach "contrary" interpretations of the same statute and yet both be affirmed, leading to equally valid but

contradictory interpretations.[4] Rauch Sharak cannot usurp this Court's role to determine what the law says by labeling the circuit court's legal conclusions as factual findings.[5]

### 2. Federal law did not encourage Google to search Rauch Sharak's account.

Rauch Sharak argues that a constellation of federal statutes implicitly compels ESPs to search for CSAM. (Rauch Sharak's Br. 29–35.) Incredibly, he never acknowledges that 18 U.S.C. § 2258A(f)(3) expressly relieves ESPs of a duty to "affirmatively search, screen, or scan" for CSAM. Rauch Sharak's argument lacks merit because he fails to address 18 U.S.C. § 2258A(f)(3) and mischaracterizes the federal laws that he does cite.

Rauch Sharak begins by arguing that section 230 of the Communications Decency Act of 1996 (47 U.S.C. § 230), incentivizes ESPs to search for CSAM by immunizing them from publisher liability in defamation suits. (Rauch Sharak's Br. 13–14, 30, 33.) The provisions of section 230 "bar plaintiffs from holding [ESPs] legally responsible for information that third parties created and developed." *Johnson v. Arden*, 614 F.3d 785, 791 (8th Cir. 2010); *see* 47 U.S.C. § 230(c)(1). Two purposes animated this immunity. First, the immunity aimed "to maintain the robust nature of Internet communication, and, accordingly, to keep government interference in the medium to a minimum." *Zeran v. America Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997). Second, the immunity promotes "self-regulation" by eliminating "the specter of liability" that

---

[4] The Supreme Court has "consistently held that state courts have inherent authority, and are thus presumptively competent, to adjudicate claims arising under the laws of the United States." *Tafflin v. Levitt*, 493 U.S. 455, 458 (1990).

[5] Regardless, Rauch Sharak's statutory argument fails under either a *de novo* or clear error standard.

would "deter service providers from blocking and screening offensive material." *Id.* at 331, 333.

Rauch Sharak's claim that section 230 encourages ESPs to search for CSAM does not square with section 230's two primary effects. Keeping "government interference . . . to a minimum" runs counter to a government directive to search for CSAM. *Zeran*, 129 F.3d at 330. To be sure, section 230 does not condone the distribution of CSAM or alter criminal law. 47 U.S.C. § 230(e). However, a statute designed to discourage restrictive content moderation does not meaningfully encourage ESPs to search for CSAM. In addition, "self-regulation" is, by definition, not directed by the government. *Zeran*, 129 F.3d at 331, 333. That lack of government involvement is confirmed by the fact that ESPs have no legal obligation to search for CSAM. 18 U.S.C. § 2258A(f)(3). For these reasons, federal courts have already considered and rejected Rauch Sharak's section 230 argument. *See Richardson*, 607 F.3d at 367; *Children's Health Defense v. Facebook Inc.*, 546 F. Supp. 3d 909, 932 (N.D. Cal. 2021).

Rauch Sharak next argues that the Victims of Trafficking and Violence Protection Act of 2000 (TVPA), Pub. L. No. 106-386, 114 Stat. 1464, 1466–91 (codified as amended at 22 U.S.C. § 7101–10 and in scattered sections of 18 U.S.C.), encourages ESPs to search for CSAM by expanding the definition of human trafficking to include participating ESPs. (Rauch Sharak's Br. 14, 30, 33.) However, criminal consequences for ESPs that participate in human trafficking do not encourage law-abiding ESPs to monitor their users for CSAM. Complying with criminal law obviously cannot render a private actor a government agent. Otherwise, all law-abiding private actors would be government agents.

Rauch Sharak asserts that the Protect Our Children Act of 2008, Pub. L. No. 110–401, 122 Stat. 4229 (codified as amended in scattered sections of 18 and 47 U.S.C.), "granted NCMEC sweeping new powers, funding, and responsibilities."

(Rauch Sharak's Br. 32.) That fact is a non-sequitur because NCMEC did not scan Rauch Sharak's Google Photos account. More importantly, that Act enacted 18 U.S.C. § 2258A(f)(3)—the provision that tells ESPs that they do not have to search for CSAM. Protect Our Children Act, Pub. L. No. 110–401 § 501, 122 Stat. at 4244. The Act can hardly have encouraged ESPs to search for CSAM by assuring them that they had no legal obligation to do so. *See Rosenow*, 50 F.4th at 730 ("[T]he Protect Our Children Act disclaims any governmental mandate to search.").

Rauch Sharak nevertheless uses NCMEC as a red herring, recounting NCMEC's history to suggest that NCMEC's powers and responsibilities turned Google into a government agent. (Rauch Sharak's Br. 31–33.) His claim, however, is that Google acted as a government agent. NCMEC merely forwarded the files flagged by Google to Wisconsin law enforcement without viewing them. (R. 31:9–13.) The history of NCMEC is therefore irrelevant. *See Bebris*, 4 F.4th at 558 (noting that whether NCMEC was a government agent was immaterial since NCMEC only forwarded images flagged by an ESP to law enforcement without viewing them).

Rauch Sharak also relies on the circuit court's assertion that "Google's search would not be possible without access to NCMEC's hash lists." (R. 36:15; *see* Rauch Sharak's Br. 33.) On this record, that finding is clearly erroneous since the circuit court did not hold a suppression hearing. The CyberTip states only that Google reported the CSAM after an employee manually reviewed the four files and confirmed that they depicted CSAM without disclosing how Google became aware of the files. (R. 31:5–6; 36:1.) Google did not need any assistance from NCMEC to have an employee view four files. Moreover, even if Google used a hash list provided by NCMEC, Google would remain a private actor. Once again, Rauch Sharak gives 18 U.S.C. § 2258A(f)(3) short shrift. Even if NCMEC provided Google a list of known CSAM files with

their hash values, Google would still be legally entitled not to search for CSAM.

Finally, Rauch Sharak argues that the Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (FOSTA), Pub. L. No. 115–164, 132 Stat. 1253–56 (codified at 18 U.S.C. §§ 1, 2421A, and 47 U.S.C. § 230), mandated that ESPs search for CSAM by amending section 230 of the Communications Act. (Rauch Sharak's Br. 13, 30, 33.) He is wrong. FOSTA clarified that section 230 "was never intended to provide legal protection to websites that unlawfully *promote and facilitate* prostitution" or sex trafficking. FOSTA, Pub. L. No. 115–164, § 2(1), 132 Stat. at 1253 (emphasis added). As with his TVPA argument, Rauch Sharak erroneously conflates consequences for ESPs that engage in criminal conduct with encouragement for law-abiding ESPs to search for CSAM. They are not equivalent. *See Does 1–6 v. Reddit, Inc.*, 51 F.4th 1137, 1145 (9th Cir. 2022) ("FOSTA requires that a defendant-website violate the criminal statute by directly sex trafficking or, with actual knowledge, 'assisting, supporting, or facilitating' trafficking, for the immunity exception to apply.").

Ultimately, Rauch Sharak cannot reconcile his position with the fact that 18 U.S.C. § 2258A(f)(3) relieves ESPs of an affirmative duty to search for CSAM. His web of statutes does not justify disregarding that clear provision and departing from every other court. Had Congress wished to require ESPs to scan for CSAM, it would have done so expressly, not secretly through a patchwork of statutes. *See Whitman v. American Trucking Assns.*, 531 U.S. 457, 468 (2001) ("Congress . . . does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions—it does not, one might say, hide elephants in mouseholes.").

### 3. Google had a private purpose to search for CSAM.

Rauch Sharak also declares that Google's search of his account was solely to aid the government in prosecuting child pornography. (Rauch Sharak's Br. 34–35.) He ignores Google's obvious private purpose in scanning for CSAM.

Google scans for CSAM to provide its users an optimal experience and, thus, succeed commercially by attracting users. The Terms of Service require users to "comply with applicable laws" so that Google can "maintain a respectful environment for everyone." (R. 31:59.) Google reports content to law enforcement to "[p]rotect against harm to the rights, property or safety of Google, [Google's] users, or the public." (R. 31:87.) The Abuse Policy states that "[t]he policies play an important role in maintaining a positive experience for everyone using Google products." (R-App. 3.) An ESP's desire for a positive user experience is a private purpose. *See Rosenow*, 50 F.4th at 734 ("[T]he ESPs' desire to purge child pornography from their platforms and enforce the terms of their user agreements is a legitimate, independent motive apart from any interest that the ESPs had in assisting the government."). A positive user experience free from CSAM makes it more likely that Google will retain and attract users. *See Fristoe*, 489 P.3d at 1205; *Stevenson*, 727 F.3d at 830. The Sixth and Eighth Circuits have already concluded that Google, specifically, acts on this commercial interest in scanning for CSAM. *Miller*, 982 F.3d at 425; *Ringland*, 966 F.3d at 736.

* * * * *

Rauch Sharak's argument depends on tying this Court's hands. He can prevail only if this Court binds itself both to *Rogers*'s misbegotten three-factor test and to accepting the circuit court's flawed statutory analysis as a set of factual findings. In this way, he dodges the overwhelmingly one-sided

authority against him and the federal law that expressly relieves ESPs of a duty to search for CSAM. The Certification disregarded Rauch Sharak's gambit to conclude that Google acted in a private capacity. (Certification 7.) This Court should do the same.

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

Even if Rauch Sharak suffered a Fourth Amendment violation, this Court should decline to apply the exclusionary rule.

"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. Thus, 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*).[6]

[6] The decision not to exclude evidence is frequently called "the 'good faith' exception to the exclusionary rule." *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

This Court should decline to apply the exclusionary rule here. The Jefferson County detective had an objectively reasonable belief that no Fourth Amendment violation had occurred. Wisconsin courts have not yet addressed whether an ESP acts as a government agent when scanning a user's account for CSAM. Every other court to consider the issue has concluded that the ESP is not a government agent in these circumstances. *See* pages 34–35, *supra*. The detective could reasonably assume that Google conducted a private search based on the law at the time. The circuit court also found that there was no law enforcement misconduct. (R. 36:26.) Given the silence of Wisconsin courts, the completely one-sided weight of authority from other jurisdictions, and the lack of misconduct, "there is nothing concerning under Fourth Amendment doctrine with how [the detective] conducted [himself]." *Burch*, 398 Wis. 2d 1, ¶ 25. Accordingly, the societal cost of exclusion is too steep a price to pay. *See id.*

Both the circuit court and Rauch Sharak believe that failing to suppress the evidence would allow for "government/society to be aware of and remedy a tremendous harm to the justice system, *i.e.* the superseding of the Fourth Amendment through legislation converting private searches into government searches." (Rauch Sharak's Br. 36; R. 36:26). This statement is difficult to parse, but it is clearly not directed at the exclusionary rule's purpose of deterring "*police* misconduct." *Burch*, 398 Wis. 2d 1, ¶ 17 (emphasis added). The exclusionary rule does not apply to raise awareness or precipitate legislative change. In addition, this statement does not identify any supposed recurring or systemic negligent practice that exclusion would rectify. If anything, the circuit court and Rauch Sharak have only highlighted the

---

a catchall for cases where exclusion is improper, and do not describe their conclusion that exclusion was inappropriate as applying a 'good faith' exception." *Id.*

novelty of the issue under Wisconsin law, which weighs against exclusion.

## CONCLUSION

This Court should affirm the judgment of conviction because the circuit court correctly denied Rauch Sharak's suppression motion.

Dated this 13th day of June 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-Respondent

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 10,979 words.

Dated this 13th day of June 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 13th day of June 2025.

Electronically signed by:

Michael J. Conway
MICHAEL J. CONWAY