FILED
05-27-2025
CLERK OF WISCONSIN
SUPREME COURT

No. 2024AP469-CR

STATE OF WISCONSIN
SUPREME COURT OF WISCONSIN

STATE OF WISCONSIN,
Plaintiff-Respondent,

vs.

ANDREAS W. RAUCH SHARAK,
Defendant-Appellant.

On Certification
Appeal from the Circuit Court for Jefferson County
The Honorable Judge William F. Hue Presiding
Case No. 2022CF495

BRIEF OF DEFENDANT-APPELLANT

BRADLEY W. NOVRESKE
State Bar No. 1106967

Attorney for Defendant-Appellant

NOVRESKE LAW OFFICE, LLC
13422 W. Prospect Pl.
New Berlin, WI 53151
(414) 502-7558
brad@novreskelaw.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

UNITED STATES SUPREME COURT

WISCONSIN CASES

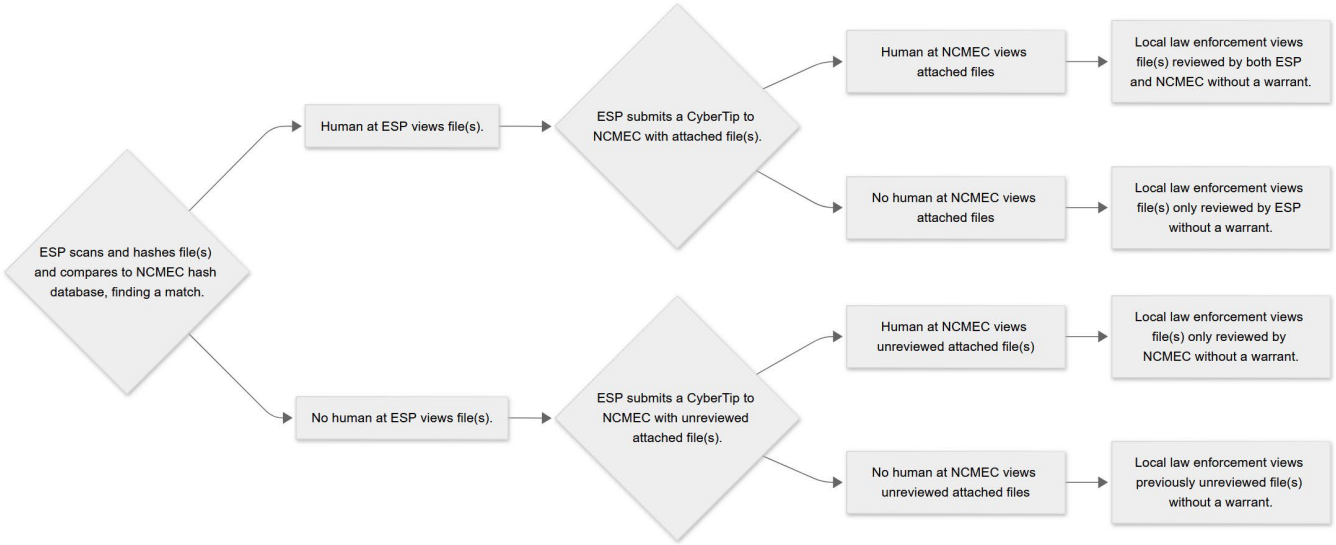
FEDERAL APPELLATE CASES

FEDERAL STATUTES

WISCONSIN STATUTES

INTRODUCTION

This case, as well as *State v. Gasper*, Case No. 2023AP2319-CR, 2024 WI App. 72, 414 Wis.2d 532, 16 N.W.3d 279, presents this Court with a complex Fourth Amendment issue of first impression in Wisconsin. These cases address a common fact pattern that proceeds along one of four possible paths:



1. A user creates an account on an app, social media platform, email provider, or similar website (often referred to as Electronic Service Providers (ESPs) or Interactive Computer Services (ICSs)) accepting the ESP's Terms of Service (Terms) often without reading them, and then uploads, stores, or transmits data or communications over the ESP's platform.

2. The ESP, using proprietary software, scans the contents of all data and communications uploaded, stored, or transmitted over the platform, calculating "hash values" for image and video contents. The ESP then compares those hash values to databases of hash values maintained by the National Center for Missing and Exploited Children (NCMEC) which contain hash values of images and videos that have previously been categorized as child sexual abuse materials (CSAM), also referred to as child pornography (CP).

3. Anytime a user's data and communications is scanned and flagged as a match to a hash value in one of NCMEC's databases, the ESP is required by federal law to submit specific details about the data, the user, and subscriber details to NCMEC in a report called a CyberTipline Report (CyberTip). The suspected files are always attached to the CyberTip.

   a. Sometimes, but not always, a human employee or contractor of the ESP opens and views the file(s) to verify that the contents appear to be CSAM.

   b. Often, the ESP creates and submits the CyberTip to NCMEC without any human ever viewing the files.

4. Once NCMEC receives a CyberTip, an analyst compiles additional information about the user/subscriber based on the information provided by the ESP. This includes approximate geolocation data for the IP address(es), the Internet Service Provider that issued the IP address to the user, and an internal check for any prior CyberTips that might be associated with the current CyberTip based on IP address, email address, phone number, user name, or other biographical data provided by the ESP. This information is compiled into sections of the CyberTip.

a. Sometimes, but not always, a human employee of NCMEC opens and views the file(s) to verify that the contents appear to be CSAM.

b. Often, particularly where no human review was done by the ESP, NCMEC will compile the CyberTip without any human ever viewing the files. This was the case in *Gasper*.

5. NCMEC is then required by federal law to transmit the CyberTip and its attachments to the local law enforcement agency (often, but not always, WIDOJ's Department of Criminal Investigation in Wisconsin) believed to have jurisdiction based on the geolocation of the IP address used.

6. Local law enforcement receives the CyberTip and opens and views the attached files without a warrant. When WIDOJ is the agency that receives the CyberTip, a "designee" opens and views the attachments and issues an administrative subpoena to the Internet Service Provider that owns the IP address identified in the CyberTip for subscriber data for that IP address. The CyberTip is then forwarded to the county or municipal police department with jurisdiction over the address provided by the Internet Service Provider.

7. A search warrant is subsequently sought by the county or municipal police department for the suspect's home and electronic devices based on the contents of the CyberTip and any additional investigation conducted by local law enforcement prior to seeking a warrant.

This recurring fact pattern raises several important questions that are not settled, some of which are presented to the Court by *Rauch Sharak* and *Gasper* based on the path that applies to each case:

- Does a user of an ESP's platform have a reasonable expectation of privacy vis-à-vis the government regardless of the ESP's Terms?

- If no, what must the Terms Service contain to effectuate a knowing and voluntary relinquishment of the expectation of privacy for the user's data and communications over the ESP's platform vis-à-vis the government?

- Assuming a reasonable expectation of privacy, does an ESP perform a search as understood by the Fourth Amendment by relying on proprietary software to scan and calculate hash values for all user data and communications on the platform? Does an ESP perform a search when a human employee or contractor opens and views the contents of the data or communications? Is there a difference in scope between the two searches?

- Under this Court's precedent in *State v. Payano-Roman*, 2006 WI 47, 290 Wis.2d 380, 714 N.W.2d 548, is the ESP's search (whether hash-only or viewed by a human) considered government action given the encouragement and participation of the government in performing the searches?

- If no, is NCMEC acting as an agent or instrumentality of the government or otherwise performing a "government function" when acting in its congressionally mandated role as the national clearinghouse for the investigation and identification of CSAM?

- If no human employee of the ESP views the file(s) and no human analyst of NCMEC views the file(s), can local law enforcement open and view the files without a warrant under the private search doctrine based only on the ESP's use of hash-matching? (Path 4 applicable to *Gasper*)

- To what extent can the Government circumvent the protections of the Fourth Amendment by outsourcing its investigation and surveillance to private-sector entities, allowing the government access to second-by-second intimate personal data about any individual that would be impossible to obtain through traditional policing methods?

- Assuming a Fourth Amendment violation, is suppression an appropriate remedy?

ISSUES PRESENTED

1. Did Mr. Rauch Sharak have a reasonable expectation of privacy in the contents of his data and communications in his Google Photos account?

2. Did the trial court incorrectly apply the appropriate legal standard when it explicitly acknowledged that under the controlling precedent, *Rogers*, as adopted by *Payano-Roman*, Mr. Rauch Sharak proved that Google's actions were a government search for Fourth Amendment purposes, but rejected that precedent in favor of a totality of the circumstances multifactor balancing test not supported by any authority?

3. Did Mr. Rauch Sharak prove by a preponderance of the evidence that Google searched the contents of his electronic data and communications as an agent or instrumentality of the government?

4. Should the evidence obtained through Google's search and any derivative evidence be suppressed?

SUMMARY OF ARGUMENTS

Mr. Rauch Sharak had a reasonable expectation of privacy in his data and communications while using the Google platform. Google's Terms did not extinguish Mr. Rauch Sharak's reasonable expectation of privacy vis-à-vis the government. This case turns on whether Google was acting as an agent or instrumentality of the government when it searched Mr. Rauch Sharak's electronic communications and data. If Google's search was government action for Fourth Amendment purposes, Mr. Rauch Sharak is entitled to suppression of the evidence discovered by Google. If the search was merely a "private search," Mr. Rauch Sharak would not be entitled to suppression. Three requirements must be met for a search to be considered a "private search." These three requirements were identified in *Rogers*, 148 Wis.2d 243, and adopted as the controlling analysis by this Court in *Payano-Roman*, 2006 WI 47.

All three requirements must be met before a court can conclude that a challenged search was a "private search" not subject to the Fourth Amendment. In this case, the trial court held that Mr. Rauch Sharak disproved the first of the three requirements. The trial court further held that Mr. Rauch Sharak met his burden of proof establishing that Google was acting as an agent or instrumentality of the government under *Rogers* and *Payano-Roman* because all three requirements for the search to be a "private search" could not be met once Mr. Rauch Sharak disproved the first requirement.

However, discontent with that result, the trial court explicitly rejected *Payano-Roman*'s clear holding that all three *Rogers* requirements must be met for a search to be a "private search." The trial court instead substituted its own totality of the circumstances, multifactor balancing test, asserting that *Payano-Roman*'s analysis seemed counterintuitive. The trial court held that Google's search was a "private search" despite not meeting all three *Rogers* requirements and denied Mr. Rauch Sharak's motion. Nevertheless, to prevent the need for a remand should the Court of Appeals disagree with the trial

court's abandonment of the clear holding in *Payano-Roman*, the trial court made findings as it relates to suppression and ultimately held that suppression was necessary if the Court of Appeals (or this Court) decides that Google acted an agent or instrumentality of the government for purposes of the search.

The trial court went rogue. It rejected the clear, unequivocal rule announced by *Payano-Roman*, a case which has been the controlling precedent on the private search doctrine in Wisconsin for nearly 20 years. The court acknowledged that *Rogers* and *Payano-Roman* required the court to conclude that Google's search was government action for purposes of the Fourth Amendment and explicitly rejected that result and substituted its own analysis to reach the opposite conclusion.

Unlike the not-infrequent scenario in which a trial court mistakenly applies the wrong legal standard or omits a critical step in its analysis, in this case the trial court performed the correct analysis, reached the correct conclusion under that analysis, and explicitly rejected that result. It opted to create its own test divorced from the requirements imposed by *Payano-Roman*. There was no mistake, no inadvertence, and no confusion. It was the wholesale rejection of controlling Wisconsin Supreme Court precedent. The trial court held that Mr. Rauch Sharak met his burden of proof under the controlling legal standard. The trial court held that suppression was the appropriate remedy. Mr. Rauch Sharak respectfully asks this court to reverse the trial court insofar as its analysis went beyond those two holdings and order the suppression of any evidence discovered by Google or derived therefrom.

STATEMENT OF THE CASE

I. Factual Background.

The facts are undisputed. Google, an Electronic Services Provider[1] ("ESP"), proactively scans all content uploaded to or transmitted through Google services by a subscriber or user. This process is done automatically using proprietary software such as MD5 hashing (which is used in virtually every case often in conjunction with a second software) and PhotoDNA, which was developed by Microsoft and made available to ESPs and the National Center for Missing and Exploited Children ("NCMEC"). Unlike MD5 hashing, PhotoDNA tries to identify photos that are visually highly similar to previously identified images classified as CSAM despite the photos not being identical at the bit level such that there would be matching MD5 hash values. Similar proprietary software has been developed by Google and YouTube to perform the same function as PhotoDNA. ESPs use one or several of these options to automatically scan the electronic data and communications of the ESP's users, calculate a cryptographic hash value of any uploaded files, and compare each file's hash value to a database of hash values associated with previously identified child sexual abuse materials ("CSAM") maintained and distributed to ESPs by NCMEC.

If a match is found, the ESP is mandated by federal law to submit a report to NCMEC providing detailed information about the individual who uploaded or received the content. Attached to each report are the actual files which were uploaded or transmitted. Often, but not always, a staff member of the ESP views the files prior to submitting them to NCMEC to confirm that the images contain suspected CSAM. Often, but not always, a staff member at NCMEC

[1] "Electronics Service Provider is a broad, catchall term for providers of interactive computer services as defined by Section 230. The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions. Internet Service Providers (ISPs) are one type of ESP.

views the files attached to the report. Ultimately, NCMEC gathers additional information about the user and transmits the report and attachments to local law enforcement in the jurisdiction in which the user is believed to reside. Upon receiving the report, law enforcement reviews the report and views the attached files.

In this case, on August 17, 2021, Google submitted a CyberTipline Report ("CyberTip") to NCMEC indicating that suspected CSAM had been uploaded to Google. (R36/1; A-App. 1). The CyberTip indicated that four specific files containing suspected CSAM had been identified. (*Id.*). The CyberTip indicated that "A person at Google viewed the file to the extent necessary to confirm that it contained apparent child pornography concurrently to or immediately preceding the sending of the CyberTip." (*Id.*). The CyberTip included the names of the files uploaded as well as the IP addresses associated with the uploads. (*Id.*). It also included a "geo lookup" for the IP addresses associated with the uploads which indicated that the ISP was maintained by Spectrum (formerly Charter) and U.S. cellular. (*Id.*).

On August 17, 2021, NCMEC staff downloaded and viewed the suspected CSAM files attached to the CyberTip and compiled additional geolocation and subscriber data. The CyberTip was then forwarded to WIDOJ on September 15, 2021. On October 28, 2021, Policy Analyst McCarty opened and viewed the attachments to the CyberTip without a warrant. On November 1, 2021, the Office of the Wisconsin Attorney General issued an administrative subpoena to Charter Communications, pursuant to Wis. Stat. § 165.505. (*Id.*). The subpoena requested that Charter provide the name(s) and address(es) of the customer(s) and/or subscriber(s) associated with the IP addresses listed in the CyberTip. (*Id.* at 2; A-App. 2). Charter provided the name of the subscriber and the address associated with the IP addresses. (*Id.*). The case was then referred to the Jefferson County Sheriff's Office for investigation. (*Id.*). Det. McIntyre of the Jefferson County Sheriff's Office opened the files attached to the CyberTip without a warrant and viewed them. (*Id.*).

After reviewing the files, Det. McIntyre applied for a search warrant. (*Id.*). A warrant was obtained for the residence, authorizing the Jefferson County Sheriff's Office to seize any digital devices located at the residence and authorized their search and analysis. A Samsung Galaxy S7 was seized, belonging to Mr. Rauch Sharak. Det. McIntyre reviewed 15 files located on that phone and determined that they contained child pornography. (*Id.*).

II. Procedural History.

Mr. Rauch Sharak was charged on November 14, 2022 with 15 counts of possession of child pornography contrary to Wis. Stat. § 948.12(1m). (R2; A-App. 34). On July 6, 2023, Mr. Rauch Sharak filed a motion to suppress evidence obtained after Google searched his digital files and communications, the subsequent warrantless search of those files by NCMEC, and finally the warrantless search of those files by Det. McIntyre. (R25; A-App. 43). Mr. Rauch Sharak argued that Google was an agent or instrumentality of the government for purposes of the search because Google is functionally compelled to carry out the search by the interplay between several federal regulatory regimes: the Protect Our Children Act, § 230 of the Communications Decency Act ("Section 230"), and the allow States and Victims to Fight Online Trafficking Act of 2017 ("FOSTA"). (R36/11; A-App. 11).

The State argued that Mr. Rauch Sharak did not have a reasonable expectation of privacy in the contents of his electronic communications and data uploaded to Google because the uploaded content violated Google's terms and services. The trial court held that Mr. Rauch Sharak had a reasonable expectation of privacy in the contents of his electronic communications and data uploaded to Google, and that Google's Terms did not diminish Mr. Rauch Sharak's expectations of privacy. (*Id.* at 5; A-App. 5).

The trial court made several findings of fact as they relate to the regulations relevant to the inquiry. The court found that these regulations (1) developed in response to congressional dissatisfaction with ESPs not being willing sufficiently in the opinion of Congress to engage in any form of content

moderation and especially not willing to do so through affirmative efforts, perhaps, as articulated by Congress, out of fear of liability; (2) were intended to specifically shield ESPs from liability if they choose to engage in moderating activities; (3) specifically defined the type of content that was being targeted – "materials that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable;" (4) specifically shielded ESPs from liability for targeting this type of content "whether or not such material is constitutionally protected;" (5) limited the scope of Section 230 immunity for ESPs that published content promoting or facilitating prostitution and sex trafficking creating liability for ESPs that do not affirmatively search out and remove such content; (6) expanded the definition of human trafficking under the Trafficking Victims' Protection Act ("TVPA") to more explicitly cover ESPs that "benefit from participation in a venture which has engaged in sex trafficking," which did not necessarily require knowledge of the content or direct participation in its creation in order to be found to be criminally liable under that law; and (7) were introduced explicitly to remove what lawmakers believed to be federal impediments on local law enforcement actions against ESPs. (*Id.* at 11-13; A-App. 11-13).

The trial court also found that Google, as an ESP, is required by federal law to provide information to the CyberTipline maintained by NCMEC regarding any apparent violations of federal statutes criminalizing acts related to sexual exploitation of children and/or child pornography if Google obtains actual knowledge of facts or circumstances regarding such violations. (*Id.* at 13; A-App. 13). Regarding NCMEC, the court found that NCMEC is federally mandated to maintain and operate the CyberTipline as a clearinghouse for the collection of reports of child sexual exploitation, and that NCMEC is statutorily required to make CyberTipline Reports generated by ESPs and compiled by NCMEC available to federal, state, and local law enforcement agencies. (*Id.*).

Considering the three requirements identified in *Rogers* as adopted by *Payano-Roman* which must be met for the court to conclude a search was

private, the court first held that law enforcement encouraged and participated in Google's search. The court found that Google's search would not be possible without access to NCMEC's hash lists, and that Google utilizes these hash lists in its search and then reports the results from those searches to NCMEC, which then makes the results available to law enforcement. As such, the court found that law enforcement was participatory in the search and government regulations/statutes certainly encouraged the search. (R36/15-16; A-App. 15-16).

Considering the second requirement, the court held that Google's search was based on private, non-law enforcement ends based on the immunity provided through engaging in the proactive screening, flagging, and reporting to NCMEC, as Google had the option to make a business decision as to whether that endeavor when weighed against potential legal liability is worthwhile. (*Id.* at 16).

Considering the third requirement, the court held that Google's decision to search was motivated by a desire to achieve protection (by regulation granted immunity) from civil and criminal liability and that those concerns are legitimate business purposes separate and distinct from assisting governmental efforts, "which admittedly is a natural consequence of the decision to scan." (*Id.* at 16-17; A-App. 16-17).

It was at this point that the trial court's analysis forked:

> Of note though is what expectation the Court has of the party with the burden of production/proof and what expectation the independently assessing Appellate Court has of the Trial Court in the application of fact to the three factors identified or law (the Court's ultimate conclusion), when the burden of proof/persuasion is assigned to Defendant. The three requirements that must be met under *State v. Rogers*, 148 Wis.2d 243 (Ct. App. 1988) for a search to be a <u>private search</u> have been set forth herein multiple times. Because the Defendant, who has no incentive to establish a private search, is assigned the burden of persuasion/production by *Rogers* and *Payano-Roman*, this Court concludes that Defendant establishing even one factor negates the possibility of a Court finding all three, all of which seemingly must be met for a Court to find that the search was private under *Rogers* and *Payano-Roman* by definition. That being the case,

> Defendant will have met its burden to prove government action.
>
> But, that can't be so because it is so counterintuitive as to process and analysis. Consequently, this Court concludes that the Trial Court is not required to engage in a draconian endeavor to "check boxes" as it relates to the three factors. This Court concludes that when its factual findings as to the factors are mixed, the Court will consider the totality of the circumstances in applying the 3-factor test (facts to law) and then will weigh them and articulate a result, subsequently tested independently by superior Courts again, under the totality of the circumstances.

(*Id.* at 18-19; A-App. 18-19).

Proceeding in that manner, the court concluded that Mr. Rauch Sharak did not meet his burden to satisfy the court, by a preponderance of the evidence, that Google's search was a government as opposed to private search. (*Id.* at 19; A-App. 19).

However, anticipating the possibility of being overturned on appeal and hoping to avoid the need to remand the case to the trial court, the court expressed concern that failing to suppress evidence in this case would foster "recurring or systemic negligence." The court held that "should it be determined either that Google's search initially, or NCMEC's search subsequently, constituted a government search, then there is and will be recurring or systemic negligence that must be remedied and in order for it to be remedied, evidence must be suppressed in individual cases in order 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 to government searches. This is true even if the underlying legislation could be challenged as unconstitutional (violative of the Fourth Amendment)." (*Id.*)

Ultimately, the court concluded that "in weighting the potential of 'letting guilty and possibly dangerous Defendants go free' through suppression, a costly toll, admittedly, against the systemic reckless disregard of Fourth Amendment requirements within the legislative scheme determined by a superior Court to have converted a private search to a government search, demands, in this Court's opinion, suppression because society's cost (the

virtual destruction of Fourth Amendment protections under such circumstances) 'pays its way' even as weighed against the costly toll of letting guilty and possible dangerous Defendants go free," and that the court, "under those circumstances, would suppress the evidence and any physical evidence further derived from the illegal search(es)". (*Id.* at 26-28; A-App. 26-28).

STANDARDS OF REVIEW

This Court applies a two-step standard of review when reviewing the mixed question of law and fact of whether a search is a private search or a government search. *Payano-Roman*, 290 Wis.2d at 389. The trial court's findings of evidentiary or historical fact will be upheld unless clearly erroneous. *Id.* This Court must independently review the ultimate question of whether the search was a government search or a private search. *Id.* The same two-step standard applies to the questions of a defendant's reasonable expectation of privacy and the reasonableness of a search. *Id.* Whether the trial court applied the appropriate and applicable law is a question of law that this Court reviews independently. *State v. Popenhagen*, 2008 WI 55, ¶ 24, 309 Wis.2d 601, 749 N.W.2d 611. The application of the good faith exception to the exclusionary rule is an issue of law which this Court reviews independently. *State v. Scull*, 2015 WI 22, ¶ 17, 361 Wis.2d 288, 862 N.W.2d 562.

ARGUMENT

A. Mr. Rauch Sharak had a reasonable expectation of privacy in the contents of his data uploaded to Google that was not negated by Google's Terms.

To establish that a search occurred which implicates the Fourth Amendment, Mr. Rauch Sharak must establish that he had a reasonable expectation of privacy in the contents of his data uploaded to Google. *State v. Bruski*, 2007 WI 25, ¶22, 299 Wis.2d 177, 727 N.W.2d 503. A person has a reasonable expectation of privacy if they have (1) an actual or subjective expectation of privacy in the place searched and the item seized; and (2) that expectation is objectively reasonable, i.e., it is one that society is prepared to

recognize as reasonable. *Id*. at ¶23. In this case, the trial court held that Mr. Rauch Sharak had a reasonable expectation in the contents of his data and communications on his Google accounts based on federal precedents such as *United States v. Miller*, 982 F.3d 412, 426-27 (6th Cir. 2020). (R36/5).

The State argued that Mr. Rauch Sharak did not have a reasonable expectation of privacy because he violated Google's Terms by uploading illegal images of child pornography. In other cases, the State has argued that regardless of the Terms an individual never has an expectation of privacy in contraband. Indeed, the Court of Appeals in *Gasper* appears to have held that Gasper had no reasonable expectation of privacy in the contents he sent over Snapchat because even if he had a subjective expectation of privacy in CSAM images, that belief was not objectively reasonable. *Gasper*, 414 Wis.2d at ¶28. Because there was no expectation of privacy in the CSAM, the *Gasper* court reasoned, law enforcement did not conduct a search for Fourth Amendment purposes by viewing the attachments to the CyberTip. *Id.* at ¶29.

The *Gasper* court's approach is troubling and analytically unsound in two regards. First, it is impossible to determine whether a user's uploaded data violates an ESPs Terms without first knowing the contents of that data by searching it. A content-based distinction that can only be applied after the fact is unworkable in practice. Presumably, a person would maintain a reasonable expectation in privacy if the user's data does not contain any files that violate the Terms of that ESP, but would not for any files that violate the ESP. In effect, this approach would eliminate the Fourth Amendment protections for those individuals most likely to become criminal defendants (assuming the content in violation of the Terms carries criminal liability) while preserving it for those individuals who are unlikely to become defendants.

Second, the *Gasper* court effectively federalizes contract terms between private persons or entities (the user and the ESP) by construing any action that a user takes in violation of the Terms as an action for which the user could not have an objective expectation of privacy. "To further explain, even if Gasper

had attested to a subjective expectation of privacy in the Snapchat video, that expectation would be objectively unreasonable given Snapchat's policies regarding sexual content in general and sexually explicit content involving children in particular." *Id.* at ¶22. Any user data that violates an ESP's terms would lack a reasonable expectation of privacy as a matter of law under this approach, regardless of whether the public is willing to recognize the user's subjective expectation of privacy as reasonable but for the violation of the Terms.

This Court should start from the well-established premise that a user of an ESP's platform has a reasonable expectation of privacy in the contents, data, and private communications that take place on the platform. From there, there are two analytical approaches that this Court could take with regard to the impact of Terms on a user's reasonable expectation of privacy. First, this Court could hold that an ESP's terms never extinguish a user's reasonable expectation of privacy as to the government. Second, this Court could hold that an ESP's terms *could* extinguish a user's reasonable expectation of privacy as to the government if the Terms are explicit enough.

The first approach is the best approach and was the approach advocated for by Mr. Rauch Sharak and adopted by the trial court. It is a clear bright-line rule that is content-neutral in its application. It promotes a consistent, predictable application by eliminating the need for every court to examine the Terms of a given ESP as of the date of the user's account creation or the date of the violation. It is consistent with the treatment of private use contracts in other contexts (car rentals, hotel rentals, storage unit rentals, etc.). And it has a well-established carve out for government ESPs that recognizes Terms as an explicit agreement outlining the rights, responsibilities, and expectations between the user and that particular government entity which does implicate a user's reasonable expectations of privacy as to the government. Under the first approach, Mr. Rauch Sharak had a reasonable expectation of privacy in the contents of his Google account and the only question remaining is whether

Google's search of his account was a private search or a government search under *Payano-Roman*.

Under the second approach, an ESP's Terms *could* extinguish a user's reasonable expectations of privacy depending on the specificity of those Terms as it relates to disclosure to the government. This is the approach that was taken by *United States v. Maher*, released the same day as *Gasper*. 120 F.4th 297 (2d Cir. 2024). The *Maher* court, following *United States v. Warshak* (*Warshak III*), 631 F.3d 266 (6th Cir. 2010), acknowledged that there might be a case where an ESP's Terms pertaining to content review "might ever be so broadly and emphatically worded as to categorically extinguish internet service users' reasonable expectations of privacy in the contents of their emails, even as against the government." *Maher* at 309. The *Maher* court held that Google's Terms, "repeatedly qualifying the content review that the company 'may' conduct, do not effect such a complete extinguishment." *Id.*

This approach is most consistent with the approach taken by the *Gasper* court, but focusing on the contents of the Terms as it relates to disclosure to the government of user data instead of focusing on whether the user's data itself violates the Terms. For example, compare the Terms at issue in *Gasper* with the Terms in *Maher*. In *Gasper*, the Snapchat Terms explicitly informed the user that Snapchat would scan and access all content on his account for content that violates the Terms and would report violations to law enforcement. For example, by making a Snapchat account, the user specifically authorized Snapchat to "access, review, screen, and delete [their] content at any time and for any reason." *Gasper* at ¶17.

Snapchat's Terms also inform users that Snapchat "reserves the right to remove any offending content, terminate or limit the visibility of your account, and notify third parties – including law enforcement – and provide those third parties with information relating to your account." *Id.* Additionally, the Terms prohibit "any activity that involves sexual exploitation or abuse of a minor;" requires that users "never post, save, send, forward, distribute, or ask for nude

or sexually explicit content involving anyone under the age of 18;" and explains that Snapchat will "report all instances of child sexual exploitation to authorities, including attempts to engage in such content." *Id.* at ¶18.

Finally, Snapchat's Community Guidelines (incorporated into its Terms) states: "Preventing, detecting, and eradicating Child Sexual Abuse Material (CSAM) on our platform is a top priority for us, and we continuously evolve our capabilities to address CSAM and other types of child sexually exploitative content. We report violations of these policies to NCMEC, as required by law. NCMEC then, in turn, coordinates with domestic or international law enforcement, as required." *Id.* at ¶19.

Google's Terms in effect prior to February 2021 were discussed in *Maher*. At that time, the Terms advised that Google "may review content" on its platform "to determine whether it is illegal or violates our policies" and "may remove or refuse to display content that we reasonable believe violates our policies or the law." *Maher* at 302. But, in the very next sentence, the Terms state: "But that does not necessarily mean that we review content, so please don't assume that we do." *Id.* The terms also state that Google "may … report a detected violation of law or its policies to appropriate authorities." And later, the Terms state that Google "will share personal information outside of Google" where necessary to "meet any applicable law ... or enforceable governmental request." *Id.*

Google's Terms as amended in February 2021 eliminated much of the qualified uncertain language but still fall far short of the specificity of Snapchat's Terms:

> **Child Sexual Abuse and Exploitation**
>
> Do not create, upload, or distribute content that exploits or abuses children. This includes all child sexual abuse materials. To report content on a Google product that may exploit a child, click "Report abuse." If you find content elsewhere on the internet, please contact the appropriate agency in your country directly.
>
> More broadly, Google prohibits the use of our products to endanger children. This includes but is not limited to predatory behavior towards

> children as:
>
> 'Child Grooming' (for example, befriending a child online to facilitate, either online or offline, sexual contact and/or exchanging sexual imagery with that child); 'Sextortion' (for example, threatening or blackmailing a child by using real or alleged access to a child's intimate images); Sexualization of a minor (for example, imagery that depicts, encourages, or promotes the sexual abuse of children or the portrayal of children in a manner that could result in the sexual exploitation of children; and Trafficking of a child (for example, advertising or solicitation of a child for commercial sexual exploitation).
>
> We will remove such content and take appropriate action, which *may* include reporting to the National Center for Missing & Exploited Children, limiting access to product features, and disabling accounts.
>
> Do not use this product to engage in illegal activities or to promote activities, goods, services, or information that cause serious and immediate harm to people or animals. While we permit information for educational, documentary, scientific, or artistic purposes about this content, we draw the line when the content directly facilitates harm or encourages illegal activity. We will take appropriate action *if we are notified of unlawful activities* which *may* include reporting you to the relevant authorities, removing account access to some of our products, or disabling your Google account. (emphasis added).

Additionally, in its Privacy Policy, users are informed Google will review user content:

> We use different technologies to process your information for these purposes. We use automated systems that analyze your content to provide you with things like customized search results, personalized ads, or other features tailored to how you use our services. And we analyze your content to help us detect abuse such as spam, malware, and illegal content. We also use algorithms to recognize patterns in data. For example, Google Translate helps people communicate across languages by detecting common language patterns in phrases you ask it to translate.

Like the pre-2021 Terms, Google's latest Terms include the same qualified "may" language that led the *Maher* court to conclude that the Terms did not extinguish the defendant's reasonable expectation of privacy. The result should be the same in Mr. Rauch Sharak's case under the second approach, particularly because the latest Terms suggest that Google may report users to the relevant authorities only "if [Google is] notified of unlawful activities," implying that Google will not report users to the relevant authorities when Google itself searches and monitors user content.

Like the *Gasper* court's approach, this second approach is not content-neutral as disclosure to law enforcement only occurs if the content violates the law. The only difference between this approach and the *Gasper* approach is that the operative question is not whether the content violates the Terms (as it is in *Gasper*) but whether the content violates the law and triggers the disclosure described by the Terms. In practice, there is little meaningful difference between the two.

This Court should adopt the first approach and establish a bright-line rule that an ESP's Terms do not negate a user's reasonable expectations of privacy on the platform as to the government. This appropriately shifts the focus from parsing Terms on a case-by-case basis to determine whether a challenged search implicates the Fourth Amendment to a much narrower focus on the application of the private search doctrine to the search in question.

B. The trial court held that Mr. Rauch Sharak prevailed under *Rogers* and *Payano-Roman*, and so the court invented a new test in order to deny Mr. Rauch Sharak's motion.

"Privacy is not insignificant; it is not something to be taken for granted; and even as it diminishes as our world becomes more interconnected and dangerous, privacy must not become a legal fiction." *State v. Subdiaz-Osorio*, 2014 WI 87, ¶ 40, 357 Wis.2d 41, 849 N.W.2d 748. Advances in technology have made it easier than ever for citizens to be surveilled without their consent or realization. With an "increasingly busy intersection" between the Fourth amendment protections and the constant advancements and use of technology, it is critical that our privacy law keep pace." *Id.* at ¶ 2. Courts must not allow privacy to be eviscerated to accommodate innovation. *Id.* at ¶ 43. In fact, the United States Supreme Court has recognized that a "central aim" of the Framers was to "place obstacles in the way of a too permeating police surveillance." *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018).

The Fourth Amendment to the United States Constitution and Article I, §

11 of the Wisconsin Constitution[2] guarantee the right to be free from "unreasonable searches and seizures." The Fourth Amendment regulates only governmental action; it does not protect against intrusive conduct by private individuals acting in a private capacity. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). The Constitution does, however, "constrain governmental action by whatever instruments or in whatever modes that action may be taken." *Lebron v. Nat'l R.R. Passenger Corp.*, 513 U.S. 374, 392 (1995) (cleaned up). Thus, a private search or seizure may implicate the Fourth Amendment where the private party acts "as an agent of the Government or with the participation or knowledge of any government official." *Id.* at 113; *Payano-Roman*, 2006 WI 47 at ¶¶ 17-19.

Warrantless searches are *per se* unreasonable and subject to a few "jealously and carefully" delineated exceptions. *State v. Young*, 2006 WI 98, ¶ 54, 294 Wis.2d 1, 717 N.W.2d 729, *Arizona v. Gant*, 556 U.S. 332, 338 (2009); *Coolidge v. New Hampshire*, 403 U.S. 443, 455 (1971). The burden falls upon the party seeking an exception to the warrant requirement to establish that a search is reasonable because it falls into one of the few exceptions to the general rule. *Coolidge*, 403 U.S. at 455. However, a defendant challenging a search conducted by a private party bears the burden of showing the search was governmental action. *Payano-Roman*, 290 Wis.2d at 23.

It is well settled that private searches are not subject to the Fourth Amendment's protection because the Fourth Amendment applies only to government action. *Id.* at ¶ 17. "*Payano-Roman* is the leading decision in Wisconsin on whether the government was sufficiently involved with what a private party did to implicate the Fourth Amendment." *State v. Butler*, 2009

[2] This Court has traditionally understood the Wisconsin Constitution's provision on search and seizure, Article I, § 11, to be coextensive with the Fourth Amendment. *State v. Houghton*, 2015 WI 79, ¶ 49, 364 N.W.2d 234, 868 N.W.2d 143. For simplicity, unless otherwise specified any reference to the Fourth Amendment will refer to both the Fourth Amendment to the U.S. Constitution and Article I, § 11 of the Wisconsin Constitution.

WI App. 52, ¶ 13, 317 Wis.2d 515, 768 N.W.2d 46. In *Payano-Roman*, this Court held:

> The court of appeals in *Rogers* stated three requirements that must be met for the Court to find/conclude that a search is a private search: (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 purposes; and (3) the private entity must not conduct the search for the purpose of assisting governmental efforts. Similarly, a search may be deemed a government search when it is a "joint endeavor" between private and government actors: "Courts which have considered combined efforts of a government official and a private person in a search hold that a search is subject to the fourth amendment prohibition against an unreasonable search if the search is a joint endeavor involving a private person and a government official."

Payano-Roman, 290 Wis.2d at ¶ 18-19 (cleaned up). However, the mere presence of a government official will not necessarily transform a private search into government action. *Id.* at ¶ 20.

In no uncertain terms, this Court previously stated that the three *Rogers* requirements *must be met* for a court to find/conclude that a search is a private search. *Id.* at ¶ 18 (emphasis added). Stated differently, when a defendant disproves even one of the *Rogers* requirements, a court cannot find/conclude that a search is a private search. While the analysis the court performs to determine if any of the *Rogers* requirements have been met considers the totality of the circumstances, *Rogers* and *Payano-Roman* dictate that once a court concludes that one or more of the *Rogers* requirements has been disproven by the defendant, the search is subject to the Fourth Amendment's prohibition against unreasonable searches. In this case, the trial court acknowledged as much: "Because the Defendant, who has no incentive to establish private search, is assigned the burden of persuasion/production by *Rogers* and *Payano-Roman*, this Court concludes that Defendant establishing even one factor negates the possibility of a Court finding all three, all of which seemingly must be met for a Court to find that the search was private under *Rogers* and *Payano-Roman* by definition." (R36/18; A-App. 18).

Instead, the trial court concluded that following the clear language of

Rogers and *Payano-Roman* was counterintuitive and opted to perform a multifactor balancing test to determine whether Google's search should be considered private or government action despite Mr. Rauch Sharak establishing that the government participated in and encouraged the search. This is directly contrary to *Rogers* and *Payano-Roman* and functionally eliminates the category of searches referred to as "joint endeavors" by the *Payano-Roman* court in which law enforcement participates and encourages the search but the private party and government have different independent motivations for performing the search.

Payano-Roman involved an individual being treated in the hospital believed to have ingested a baggie or balloon containing narcotics. The search at issue involved the medical team and police administering oral laxatives to recover the baggie of drugs both for the purpose of ensuring that it was expelled without rupturing and to collect it for evidence. In *Payano-Roman*, this Court, applying the *Rogers* requirements, found that (1) Agent Parker directly participated in the search and was not just "merely present" for the search; (2) the doctors had an independent medical purpose for the search; and (3) implicitly, because the purpose of the search from the standpoint of the medical team was medical treatment, the search was not conducted for the purpose of assisting government efforts. *Payano-Roman*, 290 Wis.2d at ¶¶ 26, 28-29. Nevertheless, this Court held that "when we consider all the circumstances of this case, we conclude that the medical purpose of the procedure cannot insulate the simultaneous evidence-gathering purpose from Fourth Amendment scrutiny," and that "the police and medical staff were engaged in a joint endeavor with a dual purpose: medical treatment and the recovery of evidence of a crime." *Id.* at ¶ 26. Payano-Roman disproved the first *Rogers* requirement for a search to be considered private, and this Court held that this precluded a finding that the search was private even though the medical team had an independent purpose for engaging in the search. *Id.* at ¶ 29.

In this case, like in *Payano-Roman*, the trial court found that the

government participated in and encouraged Google's search. Like in *Payano-Roman*, the trial court found that "Google engaged in the activity to further its own ends or purposes as opposed to government ends." And like in *Payano-Roman*, the trial court found that Google's search was not done for the purpose of furthering the government investigation but rather from the separate and distinct legitimate business purpose of shielding itself from civil and criminal exposure where it otherwise could potentially be liable. Unlike in *Payano-Roman*, however, in this case the trial court concluded that Google's independent purpose (avoiding the liability created by the government to induce Google to perform the search at issue) could "insulate the simultaneous evidence-gathering purpose from Fourth Amendment scrutiny."

Whether Google's search in this case was a private search should be answered the same as whether the medical team's search in *Payano-Roman* was a private search. In both cases, there was government involvement and encouragement of the search, dual purposes behind the search (i.e., medical treatment and evidence gathering in *Payano-Roman* and avoiding civil and criminal liability and evidence gathering in this case), and in both cases the private party did not conduct its search for the purpose of assisting governmental efforts. The Supreme Court of Wisconsin held that this scenario should be considered a "joint endeavor" and that such a joint endeavor was government conduct for purposes of the Fourth Amendment's state action requirement. Indeed, *Payano-Roman* defines "joint endeavors" as a search involving both a private person and a government official and acknowledges that such a search will be deemed subject to Fourth Amendment restrictions. It categorizes "joint endeavors" separately from the requirements of *Rogers*, explicitly only requiring the participation of both a private person and government and emphasizing that participation means something more than the mere presence of a government official. *Id.* at ¶ 19-20. If a "joint endeavor" is found any time a search is conducted by a private actor with the participation of the government, any case in which the defendant disproves the first *Rogers*

requirement involves a government search by definition regardless of the court's holding on the second and third *Rogers* requirements. That is precisely what occurred in this case.

The trial court, after acknowledging that *Rogers* and *Payano-Roman* required that same result if applied, opted instead to engage in a totality of the circumstances multifactor balancing test unsupported by any authority, but based on this approach being "what the Court has been trained to do," and what the court "has decades of experience doing."

Simply put, the trial court went rogue. It did not apply the law as stated by this Court in *Payano-Roman* which adopted the Court of Appeal's analysis in *Rogers*. The trial court acknowledged so explicitly. It correctly recognized that under *Rogers* and *Payano-Roman*, Mr. Rauch Sharak met his burden of proof, precluding a finding that Google's search was government action for purposes of the Fourth Amendment. Ultimately, the court concluded that suppression was warranted in this case to address systemic and repeated negligence that undermined the protections of the Fourth Amendment systemically. That should have been the end of the analysis.

Instead, for reasons unknown, the trial court embarked on its own path, casting off the controlling precedent of this Court in favor of an approach that focused almost exclusively on whether the regulations at issue in this case mirrored those in *Skinner v. Ry. Lab. Execs.' Ass'n,* 489 U.S. 602, 614-15 (1989), the United States Supreme Court precedent which was cited in *Payano-Roman* along with *United States v. Shanid*, 117 F. 3d 322 (7th Cir. 1997). Both of these cases were considered by this Court in deciding *Payano-Roman*, and to the extent that *Payano-Roman* differs from the approaches taken in *Skinner* or *Shanid*, it reflects a determination by this Court that Wisconsin's lower courts should follow the guidance provided in *Payano-Roman* and not attempt to independently apply *Skinner* or *Shanid*.

The trial court did not do so. Or, more accurately, the trial court *did* do so, acknowledged that doing so would result in Mr. Rauch Sharak meeting his

burden of proof precluding the court from finding that Google's search was private, and pivoted to an analysis that allowed the court to reach the opposite conclusion and deny Mr. Rauch Sharak's motion. This Court should reverse the trial court's analysis to the extent it went beyond the determination that that Mr. Rauch Sharak prevailed under *Rogers* and *Payano-Roman*. The trial court was correct in recognizing that *Rogers* and *Payano-Roman* precluded a finding that Google's conduct was a private search and the analysis that the trial court performed to avoid that conclusion had no basis in law and was contrary to this Court's precedent.

C. Mr. Rauch Sharak proved by a preponderance of the evidence that Google performed the search in this case as an agent or instrumentality of the government under *Rogers* and *Payano-Roman*.

Mr. Rauch Sharak does not dispute the trial court's findings of evidentiary and historical facts, as recited above. Mr. Rauch Sharak had a reasonable expectation of privacy in the contents of his Google account and data. He uploaded content to that account which Google automatically scanned, calculated a hash value for each file, and compared those hash values to databases maintained by NCMEC. Upon finding matches, someone at Google visually reviewed each file. Google, as required by federal law, then submitted a CyberTip to NCMEC attaching the uploaded files. Staff at NCMEC reviewed those files and forwarded the report and additional data gathered by NCMEC to the Jefferson County Sheriff's Office. Det. McIntyre opened the attachments to the CyberTip and viewed them. He did not obtain a warrant to do so.

As it relates to Google, the court found that Google, as an ESP, is required by federal law to provide information to the CyberTipline maintained by NCMEC regarding any apparent violations of federal statutes criminalizing acts related to sexual exploitation of children and/or child pornography if Google obtains actual knowledge of facts or circumstances regarding such violations. Regarding NCMEC, the court found that NCMEC is federally mandated to maintain and operate the CyberTipline as a clearinghouse for the

collection of reports of child sexual exploitation, and that NCMEC is statutorily required to make CyberTipline Reports generated by ESPs and compiled by NCMEC available to federal, state, and local law enforcement agencies.

The court also found that the Protect Our Children Act, Section 230, and FOSTA (1) developed in response to congressional dissatisfaction with ESPs not being willing sufficiently in the opinion of Congress to engage in any form of content moderation and especially not willing to do so through affirmative efforts, perhaps, as articulated by Congress, out of fear of liability; (2) were intended to specifically shield ESPs from liability if they choose to engage in moderating activities; (3) specifically defined the type of content that was being targeted – "materials that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable;" (4) specifically shielded ESPs from liability for targeting this type of content "whether or not such material is constitutionally protected;" (5) limited the scope of Section 230 immunity for ESPs that published content promoting or facilitating prostitution and sex trafficking creating liability for ESPs that do not affirmatively search out and remove such content; (6) expanded the definition of human trafficking under the Trafficking Victims' Protection Act ("TVPA") to more explicitly cover ESPs that "benefit from participation in a venture which has engaged in sex trafficking," which did not necessarily require knowledge of the content or direct participation in its creation in order to be found to be criminally liable under that law; and (7) were introduced explicitly to remove what lawmakers believed to be federal impediments on local law enforcement actions against ESPs.

These facts are not clearly erroneous. Applying *Payano-Roman* to these facts leads to the conclusion that Google's search was a government search for purposes of the Fourth Amendment. *Payano-Roman* instructs that for a search to be private, the court must find that all three *Rogers* requirements are met. In this case, none of the three are met.

The first *Rogers* requirement for a search to be considered private is that

the police may not initiate, encourage, or participate in the private entity's search. Mr. Rauch Sharak agrees with the trial court's analysis on this point—while the police did not actively participate in Google's search of Mr. Rauch Sharak's files in the sense than an officer was on scene at the time Google's software scanned the data and Google's employees reviewed the contents of the data that was flagged as a hash match to images identified as CSAM, Google's ability to engage in the search required the participation of NCMEC which is a government agency for purposes of the Fourth Amendment when engaging in its function as a national clearinghouse for the investigation and identification of CSAM. *United States v. Ackerman*, 831 F. 2d 1292 (10th Cir. 2016).

NCMEC was created in 1984, ostensibly as a non-profit organization founded by private advocates. Despite the private nature of NCMEC, it is inextricably connected to the United States Government since its inception. The center was launched on June 13, 1984 with the U.S. Attorney General and members of Congress in attendance.[3] Then-President Ronald Reagan gave the introductory remarks.[4] And after the 1984 "Missing Children's Assistance Act" established a national resource center and clearinghouse on missing and exploited children,[5] Congress designated NCMEC to fill that role. Congress also allocated financial support for NCMEC, which it continues to the present. In fact, while NCMEC may dispute the exact figure since it doesn't take into account the "in-kind" donations from private parties, approximately 70-75% of NCMEC's budget comes from federal funds.[6]

---

[3] *See Remarks at a White House Ceremony Marking the Opening of the National Center for Missing and Exploited Children*, by President Ronald Reagan, June 13, 1984, Ronald Regan Presidential Library and Museum, available at: http://www.reaganlibrary.gov/archives/speech/remarks-white-house-ceremony-marking-opening-national-center-missing-and-exploited.

[4] *Id.*

[5] PL 98-473, SEC 403, October 12, 1984, 98 Stat 1937.

[6] Brief for the National Center for Missing and Exploited Children as Amicus Curiae, p. 8, *United States v. Ackerman*, 831 F. 3d 1292 (10th Cir. 2016).

With the advent of the internet and more recently with the advancements in technology that have resulted in near-universal adoption of smartphones and other internet-connected devices, NCMEC has taken on more law enforcement responsibilities especially as it relates to attempts to enforce laws criminalizing the possession and distribution of CSAM. For example, in 2008 Congress enacted the "Protect Our Children Act," which granted NCMEC sweeping new powers, funding, and responsibilities, as well as imposing duties on private actors (ISPs and ESPs) to report conduct to NCMEC, who would then distribute information on that conduct to other appropriate government agencies.

Today, NCMEC possesses both duties and powers that far exceed that of a private citizen or corporation. Federal law mandates that NCMEC collaborate with federal and state law enforcement agencies in over a dozen ways. *Ackerman*, 831 F.3d at 1296-98. Federal law continues to designate NCMEC as the national clearinghouse for information on missing or exploited children. *Id.* Federal law requires that NCMEC alone operate the official electronic tip-line for ISPs to report potential child exploitation violations; federal law mandates these reporting obligations. *Id.* Federal law requires ISPs to report any known child pornography violations to NCMEC, and federal law requires that an ISP treat any report of known child pornography to NCMEC as a request to preserve evidence issued *by the government itself*. *Id.* Federal law requires that NCMEC provide training and technical assistance to other law enforcement agencies for assistance in executing its statutory functions (e.g., 18 U.S.C. § 3056(f) authorizes the U.S. Secret Service to provide 'at the request of' NCMEC, "forensic and investigative assistance in support of any investigation involving missing or exploited children."). *Id.*

Perhaps most tellingly, NCMEC, unlike private citizens who only have immunity from suit when they unintentionally discover contraband and immediately report it and follow preservation instructions from law enforcement, NCMEC enjoys immunity from prosecution when it knowingly

and intentionally possesses CSAM in furtherance of its statutory duties.

Because Google's search would not be possible without NCMEC and because the regulations which create and limit civil and criminal liability for Google at a minimum encourage Google to engage in the search activity, in this case the government encouraged and participated in the search, precluding a court from finding that the first requirement of *Rogers* is met.

The second *Rogers* requirement is that the private entity must engage in the activity to further its own ends or purposes. In this case, it cannot be said that Google's activities furthered its own ends or purposes *such that the activities would have taken place but for the government's regulatory actions to incentivize compliance and punish non-compliance.* The trial court's analysis was framed too narrowly. This distinction is important. In *Payano-Roman*, for example, the medical team's purpose was to provide medical treatment. The purpose of the police officer participating in the search was the collection of evidence. The medical team would have performed the search *regardless of the government's participation or evidence-gathering purpose.* Administering laxatives to Payano-Roman would have been done as a part of the medical care provided by the doctors due to the danger of the baggie of heroin that Payano-Roman ingested rupturing while traversing his digestive system. The medical team was not motivated by potential civil and criminal liability created by the government should the team decline to administer laxatives.

This is a crucial difference between *Payano-Roman* and this case. In this case, as the trial court found, Google's purpose in performing the search was to shield itself from the potential civil and criminal liability that the government created through the regulatory regime in response to ESPs not being willing to engage in the desired searches. Prior to the creation and expansion of this potential liability, ESPs avoided engaging in proactive content moderation. Unlike *Payano-Roman*, but for the government's regulatory efforts, fine-tuned over several amendments, Google would not be engaging in the proactive scanning and searching of its users' electronic data.

That is evidenced in the February 2021 amendment to Google's Terms that eliminated much of the qualifying language including Google's reassurance that their Terms "[do] not necessarily mean that we review content, so please don't assume that we do."

If Google's desire to avoid the civil and criminal liability created by the government for the purpose of pressuring Google to engage in searches of private data is considered a legitimate independent business purpose, the Fourth Amendment's protections are all but meaningless. The same could be said of the regulatory regime in *Skinner*, as the railroad companies at issue in that case could have incurred the risks and expenses associated with non-compliance, which the trial court in this case points to as the alternative option available to Google. It is always true that a private entity can refuse to comply with a governmental regulation or demand and face the consequences of doing so. Here, Google would not have engaged in the search but for the government creating new civil and criminal liability that made the risk of non-compliance untenable. As such, there was not an independent legitimate business purpose behind Google's actions such as there was behind the medical team's actions in *Payano-Roman*.

Finally, *Rogers* requires that the private entity must not conduct the search for the purpose of assisting governmental efforts. In this case (and in *Payano-Roman*), this analysis is largely the same as the analysis of the second *Rogers* requirement. In *Payano-Roman*, the medical team engaged in the search for the purpose of medical treatment due to the risk of severe harm or death if the baggie of heroin ruptured inside Payano-Roman. It is clear in such a case that the search was not conducted for the purpose of assisting governmental efforts, even if the search did in fact assist governmental efforts. Here, in contrast, the search served exclusively to further the government's interest in collecting evidence for the prosecution of individuals who possess or disseminate CSAM. There is no other purpose for screening for CSAM than to identify CSAM, and Google is required by federal law to report the CSAM that is discovered. There

is no universe in which Google conducts the search and locates CSAM but does not convey that evidence to NCMEC to be routed for prosecution to the applicable law enforcement agency. In *Payano-Roman*, had law enforcement not been present, the substance in the baggie would have been discarded, not turned over to law enforcement. Google's search in this case was conducted solely for the purpose of assisting governmental efforts to gather evidence and prosecute the possession and distribution of CSAM.

Viewed together, and taking into account the totality of the circumstances, none of the three *Rogers* requirements are met in this case. All three are required for the court to conclude that Google's search was private. As such, Mr. Rauch Sharak has demonstrated by a preponderance of the evidence that Google's search was subject to the requirements of the Fourth Amendment.

D. Suppression is warranted.

Mr. Rauch Sharak agrees with the trial court's analysis as it relates to suppression. The exclusionary rule is a judicially created rule "designed to safeguard Fourth Amendment rights generally through its deterrent effect." *United States v. Calandra*, 414 U.S. 338, 348 (1974). In Wisconsin, "the exclusionary rule is premised on suppressing evidence that is in some sense the product of illegal government activity." *State v. Knapp*, 2005 WI 27, ¶ 22, 285 Wis.2d 86, 700 N.W.2d 899 (cleaned up). However, "to the extent that application of the exclusionary rule could provide some incremental deterrent, that possible benefit must be weighed against the substantial social costs exacted by the exclusionary rule." *Id.* (quoting *Illinois v. Krull,* 480 U.S. 340, 352-53 (1987)).

"Although rooted in the Constitution, the exclusionary rule is a judge-made one in furtherance of conduct that courts have considered to be in the public interest and to suppress conduct that is not. It has also been said that the exclusionary rule applies only in contexts where its remedial objectives are thought most efficaciously served." *Id.* (cleaned up). Specifically, "the exclusionary rule serves to deter deliberate, reckless, or grossly negligent

conduct, or in some circumstances recurring or systemic negligence." *Herring v. United States*, 555 U.S. 135, 144 (2009). In this case, failing to suppress the evidence would foster "recurring or systemic negligence." The searches at issue in this case is one of countless searches conducted by ESPs for the purpose of locating CSAM and reporting it to NCMEC for investigation and prosecution on behalf of the government. The recurring or systemic negligence must be remedied, and in order for it to be remedied, evidence must be suppressed in individual cases in order 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.

In assessing this issue, the *Herring* court held that the Court analyzing the issue should balance the cost (suppression as it relates to the prosecution of any individual criminal case) versus the benefit of deterrence (would suppression in any individual case positively impact behavior globally or cause systemic change?). The *Herring* court held:

> The benefits of deterrence must outweigh the costs. We have never suggested that the exclusionary rule must apply in every circumstance in which it might provide marginal deterrence. To the extent that the application of the exclusionary rule could provide some incremental deterrent, that possible benefit must be weighed against its substantial social costs. The principal cost of applying the rule is, of course, letting guilty and possibly dangerous defendants go free—something that offends basic concepts of the criminal justice system. The rule's costly toll upon truth-seeking and law enforcement objectives presents a high obstacle for those urging its application.

The trial court correctly recognized that suppression in this case is necessary to prevent recurring or systemic negligence. Mr. Rauch Sharak maintains that suppression is both warranted and necessary in this case.

CONCLUSION

Mr. Rauch Sharak met his burden of proof under *Rogers* and *Payano-Roman* to establish that Google's search was a government search for purposes of the Fourth Amendment. Conceding that but dissatisfied with an analysis

that the trial court felt was counterintuitive, the court disregarded *Rogers* and *Payano-Roman* and embarked on an analysis contrary to both. Google searched Mr. Rauch Sharak's electronic communications and data as an agent or instrumentality of the government, and did so without a warrant. Suppression is warranted. Mr. Rauch Sharak respectfully requests that this Court reverse the trial court's analysis to the extent that it went beyond a determination that Mr. Rauch Sharak prevails under *Rogers* and *Payano-Roman*, and orders the suppression of all evidence derived from Google's search.

Dated at New Berlin, Wisconsin this 27th day of May, 2025.

NOVRESKE LAW OFFICE, LLC

Electronically signed by
BRADLEY W. NOVRESKE
State Bar No. 1106967

13422 W. Prospect Pl.
New Berlin, WI 53151
(414) 502-7558
brad@novreskelaw.com

CERTIFICATE OF COMPLIANCE

I hereby certify that this brief conforms to the rules contained in Wis. Stat. § 809.19(8)(b), (bm) and (c) for a brief. The length of this brief is 10842 words as calculated by Microsoft Word's word count feature.

I further certify that filed with this brief is an appendix that complies with § 809.19(2)(a) and that contains, at a minimum: (1) a table of contents; (2) the findings or opinion of the circuit court; (3) a copy of any unpublished opinion cited under § 809.23(3)(a) or (b); and (4) portions of the record essential to an understanding of the issues raised, including oral or written rulings or decisions showing the circuit court's reasoning regarding those issues.

I further certify that if this appeal is taken from a circuit court order or judgment entered in a judicial review of an administrative decision, the appendix contains the findings of fact and conclusions of law, if any, and final decision of the administrative agency.

I further certify that if the record is required by law to be confidential, the portions of the record included in the appendix are reproduced using one or more initials or other appropriate pseudonym or designation instead of full names of persons, specifically including juveniles and parents of juveniles, with a notation that the portions of the record have been so reproduced to preserve confidentiality and with appropriate references to the record.

Dated at New Berlin, Wisconsin this 27th day of May, 2025.

Electronically signed by
BRADLEY W. NOVRESKE
State Bar No. 1106967

APPENDIX TABLE OF CONTENTS