STATE OF WISCONSIN
SUPREME COURT

STATE OF WISCONSIN,

Plaintiff-Appellant,

-v- Appeal No. 2023-AP-2319 - CR

MICHAEL JOSEPH GASPER,

Defendant-Respondent-Petitioner.

On Review Of The Published Wisconsin Court Of Appeals District II Decision Issued October 30, 2024, Reversing An Order Suppressing Evidence Obtained By Warrantless Search Of Internet Account Data Entered In The Circuit Court For Waukesha County Case No. 23-CF-000470, The Honorable Shelley J. Gaylord Presiding

---

DEFENDANT-RESPONDENT-PETITIONER'S BRIEF

ATTORNEYS FOR DEFENDANT-RESPONDENT-PETITIONER,
MICHAEL J. GASPER

Law Offices of Joseph F. Owens, LLC
2665 S. Moorland Road, Suite 200
New Berlin, WI 53151
Phone: (262) 785-0320
By: **JOSEPH F. OWENS**
State Bar No. 1016240

Law Offices of Debra K. Riedel
2665 S. Moorland Road, Suite 200
New Berlin, WI 53151
Phone: (414) 277-7818
By: **DEBRA K. RIEDEL**
State Bar No. 1002458

TABLE OF CONTENTS

OVERVIEW

This case squarely places front and center the Fourth Amendment rights of all members of the public to their private cyberdata from their cellphones to "the Cloud". The Court of Appeals in this published decision adopted two fundamentally flawed propositions urged upon the Court by the Wisconsin Attorney General's Office:

Government Proposition 1. A person cannot have either an objective or subjective "reasonable expectation of privacy" protected by the Fourth Amendment in cyberdata placed by that person on an Electronic Service Provider's (ESP) platform in their private account when it contains criminally proscribed contraband.

> ¶ 25 While no Wisconsin court has addressed this issue, several federal district courts have determined that when a user agrees to an ESP's terms of service that advise that child pornography is prohibited content, the ESP would be scanning and accessing the account for violations of the terms, and the ESP would report violations to law enforcement, the user has no reasonable expectation of privacy in the child pornography in his or her account. (emphasis added.)
>
> [Court of Appeals Slip Opinion, October 30, 2024, p. 12., R-App. 12.]

Government Proposition 2. The terms of private commercial adhesion agreements between an ESP and persons utilizing the ESP's platforms operate to waive the Fourth Amendment rights of those persons against governmental warrantless searches and seizures of their cyberdata stored in their private account with the ESP.

> Gasper's agreement to Snapchat's Terms of Service, Community Guidelines, and Sexual Content Explainer vitiated any subjective expectation of privacy he might have had in the child pornography saved to his account. Even if he had testified to such a belief, that expectation is not objectively reasonable. (emphasis added.)
>
> [Court of Appeals Slip Opinion, October 30, 2024, ¶ 28, p. 13. R-App. 13.]

Under the Wisconsin Department of Justice officially adopted regimen, law enforcement agents are instructed to open and view without a warrant, "Suspected

Child Sexual Abuse Material" (SCSAM) cyberdata forwarded to DOJ as a CyberTip from the National Center for Missing and Exploited Children (NCMEC).

Under this process, when a proprietary software filter employed by an Electronic Service Provider (ESP), such as Snapchat, Facebook, Instagram, etc., detects SCSAM, the ESP is required by 18 U.S.C. 2258A to forward that data in the form of a "CyberTip" containing computerized "hash values" to NCMEC. The software used by each ESP differs from one to the other. In the typical case, neither the ESP nor NCMEC open and view the SCSAM data. NCMEC, using the user's Internet Protocol (IP) address, then locates the user's geographic locale.

In this case, the geographic locale of the user's IP address was within the State of Wisconsin, so the Wisconsin Attorney General was sent an unopened computer coded "CyberTip" by NCMEC. The Attorney General, then utilized an "Administrative Subpoena" process to identify the internet customer's identity and address. It is further undisputed that under the Wisconsin Attorney General's official protocol, previously unviewed CyberTip "hash" data is first opened and physically viewed without a warrant by a Department of Justice administrative bureaucrat. The uncontroverted fact of this deliberate systemic governmental action by Wisconsin Attorney General personnel was scrupulously avoided by the State in its Appellant's Brief in the Court of Appeals, and thereafter conceded in its Reply Brief, but was nevertheless ignored by the Court of Appeals in its October 30, 2024 Opinion.

The Wisconsin Court of Appeals decision here posits that if an ESP private computerized data filter program detects potential contraband in the form of "suspected" child pornographic content (SCSAM) in a customer's account, the simple use of the ESP's servers and the adhesion terms of service with the private ESP, operate to forfeit any Fourth Amendment protection against a governmental warrantless search and seizure of that content.

If that is to be the considered law of Wisconsin - we all need to know that fact - because the rules governing what privately stored information is "contraband"

on one day, can morph overnight into other forms of "contraband," simply by legislative fiat (e.g., material sympathetic to the Communist Party during the 1950's; intoxicating liquor during the Prohibition Era of the 1920's, and, in today's volatile political environment, legislatively outlawed information relating to obtaining health related pregnancy termination medical services).

The ramifications of the Court of Appeals holding in this case represents a frightening departure from settled U.S. Supreme Court Fourth Amendment precedent in the fields of car rental contracts, telephone company contracts, hotel contracts and apartment leasing, where breach of contractual provisions prohibiting illegal conduct or contraband do not operate to waive the Fourth Amendment warrant requirement applicable to governmental searches and seizures.

It is undisputed that under the Wisconsin Attorney General's system, the previously unviewed CyberTip image data is first opened and physically viewed, without a warrant, by a Department of Justice agent, not local law enforcement. The Department of Justice then determines which local law enforcement agency has jurisdiction over the user's place of residence and forwards the CyberTip to that agency. In this case, that was the Waukesha County Sheriff's Department, where Detective David Schroeder, who, following the Wisconsin Attorney General's required protocol, opened and viewed the CyberTip data image again without a warrant.

Both of these acts of law enforcement opening and viewing the previously unopened CyberTip image data were warrantless "searches" by government agents at the state and local levels. *Schneckbloth v. Bustamonte,* 412 U.S. 218 (1973); *State v. Denk*, 315 Wis.2d 5, 758 N.W.2d 775, 2008 WI 130 ¶36. It is black letter law that a warrantless search by a government agent is presumed to be "unreasonable" under the Fourth Amendment unless the government shows by "clear and convincing evidence" that its conduct falls into one of the narrow exceptions to the warrant requirements of the Fourth Amendment. *State v. Matejka*, 241 Wis.2d 52, 621 N.W.2d 891, 2001 WI 5 ¶17.

This case raises the threshold issue of whether a search warrant is required for law enforcement to open and view the content of cellphone data uploaded from a person to their private ESP account, which content ostensibly matched the CyberTip's imagery to the ESP's proprietary database of imagery through its computerized scanning program. The integrity of Snapchat's underlying imagery database was never identified, and the State misrepresented to the circuit court that "PhotoDNA" was the scanning software utilized by the ESP's filter process - which it was not. The ESP's scanning software was "MD5", which the circuit court's independent review of professional literature cited by the State in its trial court brief was shown to be unreliable. Based upon this factual foundation, the circuit court applied the U.S. Supreme Court holdings in *Carpenter v. United States*, 585 U.S. 296, 138 S.Ct. 2206 (2018), *Riley v. California*, 573 U.S. 373, 134 S.Ct. 2473 (2014) and *U.S. v. Wilson*, 13F.4th 961 (9th Cir. 2021) to grant the defense motion to suppress.

The problem is <u>not</u> that compliance with the Fourth Amendment warrant requirements is unattainable in the context of obtaining a warrant to review ESP customer account cellphone data by law enforcement agencies. The problem is that the Wisconsin Attorney General's Office is not willing to conform its procedures to meet the fundamental requirements of the Fourth Amendment when seeking to intrude into a private citizen's cyberdata. Instead, they turn to the judiciary and propose exception after exception to avoid compliance with the Fourth Amendment. It was this propensity that led Chief Justice John Roberts in *Carpenter* and *Riley* to unequivocally identify the exclusionary rule as the only effective enforcement mechanism to be applied by courts in Fourth Amendment cellphone data search cases as a matter of public policy - a decision which the trial court followed and the Court of Appeals deliberately avoided.

TABLE OF AUTHORITIES CITED

CASES **Page No.**

CASES **Page No.**

CASES **Page No.**

STATUTES CITED

OTHER AUTHORITIES

STATEMENT OF ISSUES

I. WHETHER GASPER WAS ENTITLED TO A "REASONABLE EXPECTATION OF PRIVACY" IN DATA UPLOADED TO HIS SNAPCHAT ACCOUNT FROM HIS CELLPHONE.

Answered By The Trial Court: In The Affirmative.

The trial court found that Gasper had a "reasonable expectation of privacy" in the data content of his cellphone and suppressed all evidence resulting from the warrantless cellphone search, citing *Riley v. California*, 573 U.S. 373, 134 S.Ct. 2473 (2014), *Carpenter v. United States*, 585 U.S. 296, 138 S.Ct. 2206 (2018), *U.S. v. Wilson*, 13 F.4th 961 (9th Cir. 2021), and referencing multiple law review articles in footnote 2. of its Decision and Order [R-App. 2].

Answered By The Court Of Appeals: In The Negative, stating:

> We conclude that Gasper did not have a reasonable expectation of privacy in the video, and thus, the officer's inspection was not a search subject to the Fourth Amendment. (emphasis added.)
>
> [Court of Appeals Slip Opinion pp. 1-2; R-App. 1-2.]

II. WHETHER THE WARRANTLESS VIEWING BY LAW ENFORCEMENT OF THE SNAPCHAT CYBERTIP SATISFIES THE THIRD PARTY OR "PRIVATE SEARCH" EXCEPTIONS TO THE FOURTH AMENDMENT.

Answered By The Trial Court: In The Negative.

> However, current SCOTUS cases do not allow for the government's proposed expansion of the private party search doctrine. That doctrine demands that a human being actually view *defendant's* image. Because SNAPCHAT did not view Gasper's video, current law means law enforcement needed a warrant before viewing it.
>
> [R-App. 16.]

Not Addressed By The Court Of Appeals, which expressed the following rationale set forth in footnote 8. on p. 14 of the Slip Opinion: [R-App. 14.]

> [8] Because we determine that no Fourth Amendment "search" occurred, we need not reach the additional grounds the State set forth for reversal . . . .

III. WHETHER THE "GOOD FAITH EXCEPTION" TO THE EXCLUSIONARY RULE APPLIES TO OBVIATE THE CONSTITUTIONAL VIOLATIONS OF THE FOURTH AMENDMENT WARRANT REQUIREMENTS IN THIS CASE.

Answered By The Trial Court: "*Not argued in Gasper*" by the State. "*Good faith unlikely in Gasper's case given the split in court decisions*." [R-App. 19; Trial Court Decision and Order R-56, p. 4.]

Not Answered By The Court Of Appeals, which expressed the following rationale set forth in footnote 8. on page 14 of the Slip Opinion [R-App. 14.]

> [8] Because we determine that no Fourth Amendment "search" occurred, we need not reach the additional grounds the State set forth for reversal . . . .

The circuit court ruling indicating abdication by the State was raised by the State in its Appellant's Brief in the Court of Appeals on pages 41-43.

STATEMENT ON ORAL ARGUMENT AND PUBLICATION

The Defendant-Respondent-Petitioner, Michael J. Gasper, maintains that oral argument is absolutely necessary to address the issues presented in this case, which involve complicated technology and are of statewide import.

Resolution of the case by the Supreme Court does warrant publication because it will expand the published body of case law on Fourth Amendment search and seizure of cellphone data.

STATEMENT OF THE CASE

A. Nature of the Case.

This is a criminal case which presents fundamental constitutional issues under the Fourth Amendment with respect to warrant requirements restricting law enforcement access to a person's data uploaded from their cellphone to their user account in an Electronic Service Provider (ESP) data storage system.

B. Procedural History.

On March 20, 2023, Waukesha County Circuit Court Judge Paul Bugenhagen issued a Search Warrant of the defendant, Michael J. Gasper's residence to seize all electronic devices, including cellphones. [R-6, pp. 4-6; R-App. 43-45.]

This Search Warrant was based upon an application for a Search Warrant by Waukesha County Sheriff's Detective David Schroeder, dated March 20, 2023, (misnomered in its heading as a "Search Warrant") [R-6, pp. 9-23; R-App. 46-60]. The application for Search Warrant was predicated upon assertions made by Detective Schroeder [R-6, pp. 20-22 ¶¶27-38; R-App. 57-59] in which he stated that he had opened and reviewed a video contained in a Snapchat CyberTip report of "apparent child pornography" from the National Center for Missing and Exploited Children (NCMEC) via CyberTip #152547912. In doing so, he had physically viewed the video included in the CyberTip without a warrant, which he perceived as depicting sexual intercourse between an adult male and a prepubescent light skinned female. [R-6, p. 21 ¶31; R-App. 58.]

On March 22, 2023, the Waukesha County District Attorney's Office filed the Criminal Complaint in this matter based on this information, first obtained by the Wisconsin Department of Justice by opening and viewing the content of the CyberTip from the National Center for Missing and Exploited Children (NCMEC) without a warrant, and then by the Waukesha County Sheriff's Department, which also opened and viewed the content of the CyberTip from the NCMEC without a warrant.

On May 10, 2023, Gasper filed a Motion to Suppress Evidence and Derivative Fruits of Search of Premises and Electronic Devices [R-23, pp. 1-20; R-App. 87-106].

On May 11, 2023, Gasper filed a separate Motion to Suppress Statements and Fruits of Illegal Arrest. [R-24, pp. 1-3.]

On October 2, 2023, the circuit court conducted an evidentiary hearing on both Motions to Suppress.

On October 30, 2023, the circuit court issued a Decision and Order granting Gasper's Motions to Suppress. [R-56, pp. 1-6; R-App. 16-21.]

On December 8, 2023, the State filed a Notice of Appeal from the October 30, 2023 circuit court Decision and Order granting Gasper's Motions to Suppress. [R-61, p. 1.]

On February 16, 2024, the circuit court entered a signed formal Order granting Gasper's Motions to Suppress. [R-73, p. 1; R-App. 22.]

On October 30, 2024, the Wisconsin Court of Appeals, District II, issued the Decision in this case reversing the circuit court order which had granted Gasper's Motions to Suppress. [R-81, pp. 1-15; R-App. 1-15.]

C. <u>Statement of Facts.</u>

The Court of Appeals' Opinion recites the salient background facts upon which it relied in its Opinion in ¶¶ 2-7, inclusive, and in footnotes 1, 2 and 3. [R-81, pp. 2-5; R-App. 2-5.]

In short, on January 13, 2023, the defendant uploaded cyberdata from his cellphone to his private account at Snapchat. A CyberTip generated by Snapchat and reported to the National Center for Missing and Exploited Children (NCMEC) as Suspected Child Sexual Abuse Material (SCSAM), consisted of CyberTip #152547912, describing the upload of a 16 second video on January 13, 2023 by a Snapchat username "mike_g6656", with an IP address of 184.100.214.42, which is linked to the defendant, Michael Gasper's name and address. [R-38, p. 3; R-App. 25.]

It is uncontroverted that every charge against Gasper came exclusively from use of Gasper's cellphone. [R-60, p. 96; R-App. 142.]

The Court of Appeals' Opinion at ¶20 recognized that access to the defendant's internet service, including his Snapchat user account, was password protected. [R-81, p. 10; R-App. 10.]

The Court of Appeals' Opinion in ¶12 reversed the circuit court which had found that, pursuant to the U.S. Supreme Court cases of *Riley v. California*, 573 U.S. 373, 134 S.Ct. 2473 (2014) and *Carpenter v. United States*, 585 U.S. 296, 138 S.Ct. 2206 (2018), Gasper had a reasonable expectation of privacy in his Snapchat account, including the video uploaded on January 13, 2023 from his cellphone. [R-App. 7.] The Court of Appeals' Opinion in ¶15 recites that Snapchat internally obtained the subject video by scanning its servers. [R-App. 8-9.]

The Court of Appeals' Opinion in ¶¶16-19 identified the Snapchat documents it deemed relevant to its decision as consisting of three unilateral commercial documents issued by Snapchat to its users, only one of which was identified as having been received by Gasper in a sworn declaration that the circuit court refused to admit into evidence. That document was the November 2021 "Snap, Inc. Terms of Service". There was no evidentiary foundation as to when the January 2023 Snapchat's "Community Guidelines" and Snapchat's January 2023 "Sexual Content Community Guidelines Explainer Series" was adopted or disseminated by Snapchat to its users. [R-App. 9-10.] Gasper's cellphone upload occurred on January 13, 2023.

The Court of Appeals' Opinion in ¶2 is factually incorrect when it states that Snapchat detected the subject video using a Microsoft Photo DNA program to scan user files. [R-App. 2-3.] As pointed out in detail in Gasper's Respondent's Brief in the Court of Appeals, the actual language of the CyberTip document itself references Snapchat scanning by an MD-5 program, not Microsoft's Photo DNA program, despite Detective Schroeder's verbal testimony that he believed Snapchat

had used "Photo DNA". [R-38; R-App. 23-30; R-60, pp. 23-27; 30-35; 37-41; 150-151; R-App. 118-128; 130-134; 171-172.]

The Court of Appeals' Opinion in ¶20 and in footnote 7 on p. 10 of its Opinion, refused any consideration of Gasper's Affidavit in support of the Motion to Suppress, which set forth his subjective expectations of privacy as an offer of proof. [R-App. 10.]

Gasper's Affidavit was placed in the trial court record at the motion hearing pursuant to an offer of proof following the trial court denial of admission of it into evidence as "self-serving". [R-54, p. 1; R-App. 107; R-60, pp. 140-146; R-App. 164-170.] Contrary to the Court of Appeals' Opinion, the relevance and admissibility of this Affidavit as an offer of proof was preserved and addressed in Gasper's Respondent's Brief filed in the Court of Appeals at pages 21-22.

The State's Appellant's Brief recited multiple times on multiple pages that Microsoft's PhotoDNA computer program was used to scan the video uploaded to Gasper's Snapchat account. This assertion is disingenuous and not supported by the record because Snapchat and Waukesha County Sheriff Detective David Schroeder actually used a different algorithm hash program known as "MD5" (Message Digest 5) - not PhotoDNA, to a computerized review of the hash data contained in the CyberTip. [R-60 pp. 23-27; 30-35; 137-140; 150-151; R-App. 118-128; 161-164; 171-172; R-38 p. 3; R-App. 25.]

The circuit court asked Detective Schroeder the following question:

> Q. That's why I asked, does PhotoDNA, within it, have a database of suspected child sexual abuse material?
>
> A. That would be my understanding because their software is scanning it. It has to know something to say it's a match.
>
> The Court: That's an assumption. You don't know.
>
> Mr. Owens: Speculation.

[R-60, pp. 36-37, R-App. 129-130.]

On direct examination, Detective Schroeder was asked:

> Q. In your experience, is PhotoDNA accurate in locating images images of suspected pornography?
>
> A. I don't know if any of my software I am currently using was specifically PhotoDNA. I'm not sure I can answer that.

[R-60, p. 68; R-App. 141.]

These facts become important because the circuit court itself actually researched the State's assertions of the "virtual certainty" of the MD5 algorithm made by the State to the circuit court in footnote 4 on page 5 of the State's circuit court Brief in Response to Defendant's Motion to Suppress. [R-30 p. 5.] The circuit court found those assertions by the State not credible. On page 5 of the circuit court's decision [R-App. 20-21] the court stated:

> Even if this court adopted the broader view, the facts don't support a warrantless search. Photo DNA assigned Gasper's video a hash value that starts with "MD5." (See item 30(b) in Detective Schroeder's affidavit attached to the house warrant request.) If the "MD5" is unreliable, it will create a "collision." A "collision" means that the suspected image may contain innocuous material, which is beyond the scope of the private search doctrine. Here the government's brief cited a web page in support of the reliability of the hash program at p 5, fn. 4: https://www.okta.com/identity-101/md5.) That website, contrary to Plaintiffs assertions of astronomically high reliability of PhotoDNA hash programming, states that MD5 hashes have been "broken cryptographically" for over a decade, meaning it is not secure. The web site adds MP5 should not be used when "collision verification is important." Collision verification is clearly important in the private party search doctrine. With MD5 specifically at issue in Gasper's case, it should not be relied upon as some federal courts have done. This, on its own, supports the motions to suppress.
>
> (emphasis added.)

The hearing transcript and the CyberTip report itself marked as Trial Exhibit 3 [R-38, pp. 1-8; R-App. 23-30] reflect that algorithm program "MD5" was used by Snapchat in the scanning of the image extracted from Gasper's cellphone upload into his account, not PhotoDNA. Detective Schroeder testified that he believed that

PhotoDNA was used by Snapchat because he interpreted the word "No" in the "Uploaded File Information" section of the CyberTip, to be the same as the word "False" in the definition key in the CyberTip. The relevant section of the CyberTip report reads in pertinent part:

Uploaded File Information

Filename: *mike_g6656-None-a2ab49c0-4899-54d4-87b4-c37f6ab6585b~2066-4acd140950.mp4*

MD5: *4083423d0a4c7c4cd8c67e5c114214af*

Did Reporting ESP view entire contents of uploaded file? *No*

Were entire contents of uploaded file publicly available? *No*

The headnote at the top of page 2 of the CyberTip itself states:

CyberTipline Report 152547912 | 2

Additional Information: *2023-01 -13T07:46:09Z this timestamp is when the user saved, shared, or uploaded this media file. fileViewedByEsp = <u>False indicates that the reported media was detected by PDNA hash matching technology</u> and was reported without review by a Snap team member.* (emphasis added.)

Careful visual review of the CyberTip report itself which was marked Trial Exhibit 3 [R-38, pp. 1-8; R-App. 23-30] shows that program "MD5" was used. In addition, the key word "*<u>False</u>*" does not appear anywhere in that document - the presence of which word, according to the above-referenced underlined language of the CyberTip line report, "… *indicates that the reported media was detected by PDNA hash matching technology* …". Thus, absence of the word "*False*" in the CyberTip report therefore shows that the reported SCSAM was <u>not</u> detected by PhotoDNA.

The State's Court of Appeals Brief accurately recited that Snapchat reported its own unopened algorithm data identified as "Unconfirmed" and "apparent child

pornography" *via* CyberTip to the National Center For Missing and Exploited Children (NCMEC). The CyberTip provided NCMEC the username of "mike g6656", an associated email address, an incorrect date of birth of 04-06-1971, and an "IP address" of "184.100.214.42."[1] [R-60, pp. 156-159; R-App. 177-180.]

The NCMEC then used a Geo-Lookup internet site to learn that the device associated with the IP address was located within the State of Wisconsin and was served by Century Link. All of this information was then provided by the NCMEC to the Wisconsin Department of Justice.

Notably, the State's Appellant's Brief in the Court of Appeals completely avoided informing the Court that the CyberTip was first opened and viewed without a warrant by Wisconsin Department of Justice "designee", Matthew Lochowitz, the first warrantless search by the State. According to the State Attorney General's investigating protocol, Mr. Lochowitz then issued an "Administrative Subpoena" to Century Link to obtain the individual subscriber name(s) and geographic address associated with the IP Address. [R-60, pp. 38-41; R-App. 131-134; R-60, pp. 96-99; R-App. 142-145; R-60, pp. 100-101; R-App. 146-147.] This constitutionally suspect "Administrative Subpoena" is issued pursuant to Wis. Stat. §165.505(2) without "probable cause" and is issued by a non-judicial officer. [R-39, pp. 1-3; R-App. 40-42.] The defendant, Michael Gasper, was identified by Century Link as a "subscriber" of the IP address and his home address was provided by Century Link to the Wisconsin Department of Justice. This information and the uploaded video in the CyberTip file was then sent by the DOJ to the Waukesha County Sheriff's Department.

It is uncontroverted that upon receipt of the foregoing information and media file, Waukesha County Sheriff's Department Detective, David Schroeder, on March 2, 2023, opened and viewed the Snapchat "apparent child pornography"

---

[1] "An IP Address is a unique address that identifies a device on the Internet." *State v. Baric*, 384 Wis.2d 359, 919 N.W. 2d 221, 2018 WI App 63 at ¶4.

media file, also without a search warrant. This conduct was the second warrantless search by the State.

On March 20, 2023, Detective Schroeder prayed for and obtained a search warrant of the defendant's residence, vehicles and person based upon his warrantless March 2, 2023 opening and viewing of the subject Snapchat media file. [R-60, pp. 106 - 111; R-App. 148-153.] The precatory recitations in Detective Schroeder's 15 page notarized search warrant application included a lengthy and broad description of items requested to be seized, including the content and data of all phones, mobile electronic devices, computers, routers, modems, network equipment, software.

However, the operative portion of the three page Search Warrant itself, "particularly" describes its scope as not reaching the contents of electronic devices and is limited to seize "things," providing as follows:

> *NOW, THEREFORE, in the name of the State of Wisconsin, you are commanded forthwith to search the said premises for said things, and if the same or any portion thereof is found, to bring the same and the person, if ordered, in whose possession the same are found and return this warrant within Forty-Eight (48) hours before said Court, to be dealt with according to law.*
>
> (emphasis added.)

[R-45, p. 3.]

The Search Warrant was exhibited and executed on March 21, 2023 at 5:33 a.m. by Detective Schroeder and members of the Waukesha County Sheriff Tactical Enforcement Unit at the Gasper residence on Lisa Lane in the Town of Ottowa, Waukesha, County, Wisconsin. [R-60, pp. 125-129; R-App. 154-158.] Detective Schroeder confirmed that official reports filed by Detective Knipfer and Deputy Thompson state that they preemptively drew their firearms without provocation and pointed them at the 71 year-old defendant, Michael Gasper, as he opened the door of his home in his underwear, compliantly responding to their knocking. Detective Knipfer also preemptively pointed his drawn firearm without provocation at Mary

Gasper's person within the home. [R-60, pp. 127-128; R-App. 156-157.] The defendant, Michael Gasper, without an arrest warrant, was immediately handcuffed and placed into a sheriff's vehicle, his cellphone was seized and he was transported in custody to the Waukesha County Sheriff's Department for interrogation and a complete vetting of Gasper's cellphone contents after being informed by Detective Schroeder that the search warrant applied to a search of the content of his cellphone. [R-60, pp. 131-132; R-App. 159-160.]

ARGUMENT

I. Gasper Was Entitled To A "Reasonable Expectation of Privacy" In Data Uploaded To His Snapchat Account From His Cellphone.

A. Cellphone Content Is Categorically Granted A Reasonable Expectation Of Privacy By The U.S. Supreme Court.

The Fourth Amendment of The Constitution of the United States provides as follows:

Amendment IV.

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. (emphasis added.)

Article I, Section 11. of the Wisconsin Constitution utilizes identical language.

Both the Fourth Amendment to the United States Constitution and Article I, Section 11 of the Wisconsin Constitution protect against unreasonable searches and seizures. *State v. Tullberg*, 2014 WI 134, ¶27, 359 Wis. 2d 421, 857 N.W. 2d 120. Moreover, the Wisconsin Supreme Court is explicit in its remonstrance to the bench and bar in our state that a warrantless seizure is presumed to be constitutionally "unreasonable":

> "A seizure conducted without a valid warrant is presumptively unreasonable" *State v. Brereton*, 2013 WI 17, ¶24, 345 Wis. 2d 563, 826 N.W.2d 369.

This case presents the Court with a classic unconstitutional warrantless search by two levels of government agencies in the investigative process which

resulted in the criminal charges being preferred against Michael Gasper. These agencies were: (a) the Wisconsin Attorney General's Office; and (b) the Waukesha County Sheriff's Office. These unconstitutional warrantless searches led to the issuance of the search warrant executed on March 21, 2023 of Michael Gasper's residence as to which Michael Gasper was compelled to cooperate. [*Bumper v. North Carolina*, 391 U.S. 543, 548, 885 S.Ct. 1788 (1968); *U.S. v. Nafzger*, 965 F.2d 213 (7th Cir. 1992).]

Notably, it is uncontroverted that the alleged contraband imagery in this case identified as constituting the basis for the criminal charges filed against Michael Gasper, was solely from his cellphone. [R-60, p. 96; A-App. 142.] No other electronic device is involved. This fact has major significance here because the fundamental privacy rights of persons to their cellphone content impacts the Fourth Amendment obligations imposed on law enforcement.

In *Riley v. California*, 573 U.S. 373, 134 S.Ct. 2473 (2014), the Supreme Court explains in detail why it was granting "categorical" recognition of a "reasonable expectation of privacy" in cellphones and their content under the Fourth Amendment:

> The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information - an address, a note, a prescription, a bank statement, a video - that reveal much more in combination than any isolated record. (emphasis added.)
>
> *Riley, supra*, 573 U.S. at 394, 134 S.Ct. at 2498.

> Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives - from the mundane to the intimate.
>
> *Riley, supra*, 573 U.S. at 395, 134 S.Ct. at 2490.

The Court of Appeals' opinion recites that Gasper was required to prove up a reasonable expectation of privacy in the specific suspected contraband video before he would have standing to challenge it as a governmental search. That is not

the correct focal point for addressing a cellphone user's "reasonable expectation of privacy".

The Court of Appeals' opinion in this case appears to recognize that the U.S. Supreme Court decisions in *Riley v. California*, 573 U.S. 373, 134 S.Ct. 2473, 189 L.Ed.2d 432 (2014) and *Carpenter v. U.S.*, 585 U.S. 296, 138 S.Ct. 2206 (2018) announced a public policy decision that in today's world cellphone users have a constitutionally protected expectation of privacy in the data content of their cellphones. The Court of Appeals nevertheless appears to narrowly construe the reach of the Supreme Court public policy decisions in *Riley* and *Carpenter* as being limited to the internal memory of the cellphone device itself. This strained analysis ignores the clear import of the language in *Riley* and *Carpenter* which includes, within the expectation of privacy, remote "Cloud" based storage of cellphone content on the servers of an electronic service provider (ESP) platform:

> To further complicate the scope of the privacy interests at stake, the data a user views on many modern cell phones may not in fact be stored on the device itself.
>
> * * * * * * * * * *
>
> That is what cell phones, with increasing frequency, are designed to do by taking advantage of "cloud computing." Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference. (emphasis added.)

Riley, supra, 573 U.S. at 397, 134 S.Ct. at 2491.

The narrow application of *Riley* to the cellphone device itself contradicts the Court of Appeals' prior holding in *State v. Bowers*, 405 Wis.2d 716, 985 N.W.2d 123, 2023 WI App. 4, extending a user expectation of privacy to the ESP accounts.

The Court of Appeals erroneously states that Gasper "offered no evidence" to support a subjective expectation of privacy in his cellphone or Snapchat account. In fact, Detective Schroeder's sworn affidavit requesting issuance of the search warrant of Gasper's residence [R-6, p. 18; R-App. 59] confirmed that all of Gasper's

internet Wi-Fi signals at the Gasper residence were secure and protected with a password. Detective Schroeder's search warrant affidavit states under oath:

> 38. On 03/23/2023, at approximately 0508 hours, Your Affiant traversed the roadway in front of W362S2521 Lisa Lane and used my department issued iPhone to scan for open Wi-Fi connections. After refreshing twice, I observed all available Wi-Fi signals displayed a "lock" icon, indicating they were secure and protected with a password.

Furthermore, the Affidavit of Michael Gasper [R-54, p. 1; R-App. 107; R-60, pp. 140-146; R-App. 164-170] "offered" a declaration to the court in the form of an offer of proof over the State's objection, of his subjective expectations of privacy in his cellphone data: (a) that he utilized only his cellphone for his Snapchat account and no other device; (b) his Snapchat account was a private account and never used in a public forum; and (c) his cellphone was password protected with a numerical password and thumbprint. His affidavit also recites that no other person was given access to his cellphone until the Waukesha County Sheriff's Department demanded it on March 21, 2023 after his arrest at gunpoint. [R-60, pp. 142-146; R-App. 166-170.] These facts more than meet the subjective factors identified in *State v. Bowers,* 405 Wis.2d 716, 985 N.W.2d 123, 2023 WI App. 4.

In addition, the societal recognition of expectation of privacy in cellphone content has been endorsed by several Wisconsin Supreme Court Justices; *See*: *State v. Burch*, 2021 WI ¶68, 398 Wis. 1, 961 N.W.2d 314 (Rebecca Grassl Bradley, J., concurring; Dallet, J., joined by Karofsky and Ann Walsh Bradley, JJ., concurring in part, dissenting in part). Justice Rebecca Grassl Bradley, in *State v. Burch*, in discussing whether the search of a cellphone was constitutional under the consent exception, stated that, "[b]ecause smartphones contain the 'privacies of life,' law enforcement generally needs a warrant to search the data they hold." *Burch,* 2021 WI ¶68, ¶¶37-38, ¶¶47-51 (Rebecca Grassl Bradley, J., concurring). She specifically found that in *Riley*, the Court: "held that law enforcement generally must obtain a warrant before conducting a search of smartphone data."

Moreover, Justice Dallet, joined by Justices Karofsky and Ann Walsh Bradley, recognized that, "[i]n the Fourth Amendment context, the United States Supreme Court has clearly expressed that cellphone data is in an evidence class of its own because it 'implicate[s] privacy concerns far beyond those implicated by the search of other physical belongings." *Burch*, 2021 WI ¶68, ¶72 (Dallet, J., concurring in part, dissenting in part).

It is constitutional error under the "Supremacy Clause" to refuse recognition of the U.S. Supreme Court threshold public policy decision that there is a constitutionally protected "expectation of privacy" in the data content of one's cellphone. To be sure, that expectation of privacy can be lost by public sharing, private sharing, informed consent, and potentially, abandonment. However, the U.S. Supreme Court has obviated prior threshold requirements under the Fourth Amendment that persons asserting Fourth Amendment rights in their cellphone content bear the burden of proving up an expectation of privacy in each item on their cellphones, including when it is stored remotely on an ESP server.

B. Potential Criminal Content In A Person's Cellphone And ESP Account Does Not Void The Fourth Amendment's Warrant Requirement.

The Court of Appeals' decision in a nutshell, also tells us that because Snapchat informed Gasper that Snapchat prohibits what it identifies as "suspected" child pornography on its site, and that it reserves the right to notify law enforcement authorities of such "suspected" child pornography, Gasper simply has no Fourth Amendment "expectation of privacy" in that particular unlawful contraband.

This represents a categorical change in Fourth Amendment warrant requirements. The Court of Appeals' decision dispenses with any bothersome analysis of the "third-party doctrine," or whether the government expanded the scope of a "private search" by Snapchat, or the "good faith" exception to the exclusionary rule. Instead, if the ESP reports to the NCMEC "suspected" child pornography in a user's account, the government can simply open and examine a

previously unviewed and unopened caché of data in a user's account without a warrant. This process substitutes the ESP computerized data search program for a constitutionally required "probable cause" decision by a "neutral and detached" magistrate to issue a search warrant.

The Court of Appeals' opinion recites the proposition that Gasper has no "reasonable expectation of privacy" in a single specific alleged contraband video image uploaded from his cellphone contained in the CyberTip on the theory that it was illegal "suspected child pornography." Therefore, no search warrant was required for Wisconsin Department of Justice bureaucrat, Lochowitz, or Detective Schroeder to open and view the Snapchat CyberTip of "suspected" child pornography from Michael Gasper's cellphone because the type of pornography uploaded from his cellphone was flagged by Snapchat's computer based digital filter as suspected "child pornography," versus "adult pornography." In other words, simply because the content of the digital upload was "suspected" illegal contraband, the Court of Appeals posits that Michael Gasper lost any "reasonable expectation of privacy" in his Snapchat account.

In *Payton v. New York*, 445 U.S. 573, 100 S.Ct. 1371 (1980), the Supreme Court reaffirmed the long established fundamental principle that "… a search prosecuted in violation of the Constitution is not made lawful by what it brings to light," citing *Byars v. U.S.*, 273 U.S. 28, 29, 47 S.Ct. 248-49 (1927). The fundamental flaw in the Court of Appeals holding is that a "search" is not a "search" if the "search" reveals criminal conduct or contraband.

In the seminal Fourth Amendment case of *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507 (1967), the government's warrantless eavesdropping on the defendant's participation in illegal betting operations, conducted by him in plain view in a glass public telephone booth, where the telephone company prohibited illegal use of its system and allowed operators to listen in, did not exempt governmental eavesdropping from being a constitutionally prohibited "search". Moreover, it was the *Katz* decision which instructed courts that the focus was not

on the criminal acts which the search revealed, but on whether the defendant's use of an enclosed public telephone booth "exhibited an actual (subjective) expectation of privacy"; and also whether an expectation of privacy in the use of a public telephone booth would be societally recognized as reasonable (objective). The focus of the Court in *Katz* was certainly not on whether the criminal content of his conversation about operating an illegal betting operation was itself "societally reasonable."

C. The "Third Party" Consent Doctrine Does Not Apply To A Person's Cellphone Data Simply By Having Been Placed On An ESP's Platform.

Two U.S. Supreme Court decisions after *Katz* did address a user's expectation of privacy in information stored on a third-party data system. In *United States v. Miller,* 425 U.S. 435, 96 S.Ct. 1619 (1976), the court found that an individual lacked a reasonable expectation of privacy in records of checks upon their being deposited with his bank. In *Smith v. Maryland*, 442 U.S. 735, 99 S.Ct. 2577 (1979), the court found no "reasonable expectation of privacy" when the government accessed records of all telephone numbers to and from an individual's telephone. Then, in *Carpenter v. United States*, 585 U.S. 296, 138 S.Ct. 2206 (2018), the Court specifically rejected application of the holdings in *U.S. v. Miller*, *supra*, and *Smith v. Maryland*, *supra*, to data and content of cellphone stored information which "… *provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious and sexual associations*." *Carpenter, supra*, 138 S.Ct. at 2217. The *Carpenter* Court determined that governmental accessing and analyzing cellphone data and information was a "search" requiring a search warrant; rejecting the government's request to extend the "third-party" consent doctrine to a distinct category of information:

> The government thus is not asking for a straightforward application of the third party doctrine, but instead a significant extension of it to a distinct category of information.
>
> *Carpenter, supra,* 138 S.Ct. 2216-17.

As stated by the Circuit Judge Gorsuch in his dissenting opinion in *Carpenter*, also rejecting the application of *Smith* and *Miller* to cellphone content:

> In the end, what do Smith and Miller add up to? A doubtful application of Katz that lets the government search almost anywhere whatever it wants whenever it wants.
>
> *Carpenter v. U.S.*, *supra*, 138 S.Ct. 2264.

In *Byrd v. United States*, 584 U.S.395, 138 S.Ct. 1518 (2018) in a six member opinion, the Supreme Court found that deliberate violation by the defendant of the contractual terms of an automobile rental contract did not defeat the defendant's expectation of privacy in the contents of the trunk of the rental car (i.e., 49 bricks of heroin). No third-party consent was implied from the rental contract.

In *United States v. Matlock*, 415 U.S. 164, 94 S.Ct. 988 (1974), the Supreme Court explained that a landlord cannot consent to a governmental search of an apartment leased to an individual suspected of conducting illegal activity in the demised premises.

In *Stoner v. California*, 376 U.S. 483, 84 S.Ct. 889 (1964), a hotel clerk cannot consent to a governmental search of a patron's rented room.

In *Minnesota v. Olson*, 495 U.S. 91, 96-97, 110 S.Ct. 1684 (1990), the U.S. Supreme Court opined "Olson's status as an overnight guest is alone enough to show that he had an expectation of privacy in the home that society is prepared to recognize as reasonable."

Precedent in the U.S. Court of Appeals for the 7th Circuit is in accord, per Circuit Judge Easterbrook's opinion in *United States v. Thomas*, 65 F. 4th 922, 925 (7th Cir. 2023) where the defendant, a known "meth" dealer with warrants out for his arrest, used a fake ID driver's license in violation of state law, to rent an apartment. This conduct on his part, while a clear breach of his lease terms, did not extinguish his reasonable expectation of privacy when law enforcement executed a warrantless search of his apartment, finding drugs and drug paraphernalia.

Accordingly, pursuant to the Supreme Court holding in *Riley*, as a matter of law, Michael Gasper's Motion to Suppress meets the objective "reasonable

expectation of privacy" threshold requirements for standing to assert Fourth Amendment violations relative to the Attorney General's Office and Detective Schroeder's warrantless opening and review of his cellphone data.

D. Snapchat's Unilateral Service Documents Do Not Operate To Waive Gasper's Fourth Amendment Rights Against Warrantless Searches By Law Enforcement Of His Cellphone And Related ESP Account.

Tacitly recognizing the constitutional infirmity of requiring a person to first prove-up a subjective and objective "expectation of privacy" when challenging a warrantless search of cellphone content on an ESP server, the Court of Appeals' decision moved to an examination of the actual relationship between Michael Gasper and Snapchat by looking to the terms of access and use of Snapchat's platform.

The Snap, Inc. unilateral documents sent to its customers are its: (a) "Terms of Service" [R-41, pp. 1-16; R-App. 61-76]; (b) "Community Guidelines" [R-42, pp. 1-6; R-App. 77-82]; and (c) "Sexual Content Community Guidelines Explainer Series" [R-44, pp. 1-4; R-App. 83-86].

The relevant provisions delineating Snapchat's relationship for purposes of this case are as follows:

Snap Inc. Terms of Service
Effective: November 15, 2021

> **3. Rights You Grant Us**
> While we're not required to do so, we may access, review, screen, and delete your content at any time and for any reason, . . . or if we think your content violates these Terms. (emphasis added.)
>
> [R-41, p. 4; R-App. 64.]

> **9. Safety**
> By using the Services, you agree that you will at all times comply with these Terms, including our Community Guidelines and any other policies Snap makes available in order to maintain the safety of the Services.

> If you fail to comply, we reserve 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. (emphasis added.)
>
> [R-41, p. 7; R-App. 67.]

In **Sections 1. 2. and 3.** of the November 15, 2021 **Terms of Service** document, Snap, Inc. and its users grant conditional use licenses to each other, specifically referencing a user's account "**content**". However, in **Section 9.** of its November 15, 2021 **Terms of Service**, Snap, Inc. notifies its users that "… we reserve the right …" to notify third parties, including law enforcement, and provide those third parties with "… information relating to your account." Conspicuously absent from the Snap, Inc. reservation of right in **Section 9.** is a specific authorization to provide a user's account "content" to law enforcement.

Community Guidelines
Updated: January 2023

> * * * * We report all instances of child sexual exploitation to authorities, including attempts to engage in such conduct. Never post, save, send, forward, distribute, or ask for nude or sexually explicit content involving anyone under the age of 18 (this includes sending or saving such images of yourself). (emphasis added.)
>
> [R-42, p. 2; R-App. 78.]

Community Guidelines Explainer Series
Updated: January 2023

> * * * * We report violations of these policies to the U.S. National Center for Missing and Exploited Children (NCMEC), as required by law. NCMEC then, in turn, coordinates with domestic or international law enforcement, as required. (emphasis added.)
>
> [R-44, p. 3; R-App. 85.]

These Snap, Inc. documents warn its customers that it can internally monitor the data passing through its portals. They do not explicitly say that Snapchat will

physically open and examine the customer's account content. In fact, this monitoring is done via an internally programmed algorithm hash technology.

Snap, Inc.'s January 2023 Community Guidelines and its Community Guidelines Explainer Series document do not have any explicitly identified effective date during January of 2023. Accordingly, the evidentiary foundation of their applicability to Gasper's January 13, 2023 cellphone upload is not sufficiently established. Furthermore, the "Community Guidelines" document and Community Guidelines Explainer Series document, reference an intent to "report" to "authorities" and "report" to "NCMEC" instances of child sexual exploitation, not law enforcement agencies. Furthermore, none of these Snap, Inc. documents grant "*governmental agencies*" any authority to open and view the customer account data. That would constitute waiver of a fundamental constitutional right. The U.S. Supreme Court has stated over and over:

> Waivers of constitutional rights not only must be voluntary but must be knowing, intelligent acts done with sufficient awareness of the relevant circumstances and likely consequences.
> *Brady v. United States*, 397 U.S. 742 at 7484, 90 S.Ct. 1463 (1970).

This seminal principle of constitutional law is iterated in *Gideon v. Wainright*, 372 U.S. 335, at 339-340, 83 S.Ct. 792 (1963); *Williams v. Kaiser*, 323 U.S. 471, at 472, 65 S.Ct. 363 (1945); *Johnson v. Zerbst*, 304 U.S. 458, at 464, 58 S.Ct. 1019 (1938); *Patton v. United States*, 281 U.S. 276, at 312, 50 S.Ct. 253 (1930).

As explained by the U.S. Court of Appeals for the 2nd Circuit in Section II. A. of its opinion in *U.S. v. Maher*, 120 F.4th 297 (2024), decided the same day as the Court of Appeals' decision here in Gasper, unilateral notification provisions in an ESP terms of service do not extinguish a person's expectation of privacy in the content of the user's files, as against the government. *Maher, supra,* 204 F.4th 306-309, quoting from Orin S. Kerr, "*Terms of Service and Fourth Amendment Rights*," 172 U.Pa.L.Rev. 287, 291 (2024). *See also*: *U.S. v. Warshak*, 631 F.3d 266, at 283-287 (6th Cir. 2010).

II. The Warrantless Viewing By Law Enforcement Agents Of The Snapchat CyberTip Does Not Satisfy The "Private Search" Exception To The Fourth Amendment.

A. Law Enforcement Opening And Physical Viewing of Gasper's 16 Second Video Uploaded To His Snapchat Account From His Cellphone Expanded The Scope Of The Computer Data Scan Contained In The CyberTip From NCMEC.

It is undisputed that no private person or entity opened the Snapchat CyberTip containing an upload of a 16 second video allegedly depicting "suspected child pornography" prior to Wisconsin Department of Justice bureaucrat, Matthew Lochowitz, and Waukesha County Sheriff Department Detective Schroeder doing so. Snap, Inc. personnel did not do so. Neither did personnel at the National Center for Missing and Exploited Children.

Here, it is also undisputed that both Wisconsin Department of Justice (DOJ) bureaucrat, Matthew Lochowitz, and Waukesha County Sheriff's Department Detective David Schroeder, following DOJ's official protocol, were the first persons to physically open and view the content of the previously unopened CyberTip video, without a warrant. [R-60, pp. 151-152; R-App. 172-173.]

Notably, Detective Schroeder testified that every charge against Gasper arose from use of Gasper's cellphone. [R-60, p. 96; R-App. 142.]

Detective Schroeder's March 20, 2023 search warrant affidavit submitted to Waukesha County Circuit Court Judge Paul Bugenhagen, Jr., in paragraphs 27 through 31, identified the specific factual bases for his seeking issuance of the search warrant as being the content of NCMEC CyberTip #152547912. [R-38, pp. 1-8; R-App. 23-30.]

In his trial court testimony, Detective Schroeder testified as follows:

> Q. Would it be fair to state that it was based upon that viewing of the imagery in the CyberTip that formed the basis for your application for a search warrant of Mr. Gasper's residence?
>
> A. Yes, sir.

[R-60, pp. 100-101; R-App. 146-147.]

None of the paragraphs in Detective Schroeder's lengthy sworn application for a warrant (misnomered "search warrant") submitted to Circuit Judge Bugenhagen, make any reference to the integrity of the Snapchat database; what was in that database; or the reliability of PhotoDNA, MD5, or any other computerized logarithm scanning program being utilized by Snapchat, NCMEC, Wisconsin Department of Justice, or Detective Schroeder, himself. This information was not provided to the circuit court until briefing the Motion To Suppress, long after execution of the search warrant.

In short, the issuing judicial officer of the warrant, had no basis upon which to issue the search warrant other than the "judgment call" of Detective Schroeder after his warrantless opening and viewing of the 16 second video imagery in the CyberTip.

Detective Schroeder's description of that imagery to the issuing court is found in paragraph 31.c. of his affidavit. [R-6, p. 21; R- App. 58.]

That description exemplifies that Detective Schroeder's exercise of personal judgment, based on what the video imagery visually depicted to him, and his estimate of the actual age of the female subject. He does not comment on the subject's physical size or apparent ethnicity; and concedes his inability to comment on breast development because of her wearing a t-shirt. The imagery reportedly does not show any pubic hair - but that is ambiguous because shaving of the pubic area would remove any visible pubic hair.

These descriptions are brought to this Court's attention not to cast aspersions on the accuracy of Detective Schroeder's opinion as to the age of the subject in the video. The point is that those observations arose only after his warrantless physical observations of cellphone cyberdata and formed the only factual basis provided to the issuing court to support "probable cause" for the court on which it relied in issuing the search warrant for Gasper's house, its contents, his person and his cellphone.

Nowhere in Detective Schroeder's affidavit is there any mention of the CyberTip being generated by computerized "hash technology" or the reliability of such technology. That is a fundamental flaw in the Department of Justice protocol.

Detective Schroeder's personal visual review clearly did expand the scope of Snapchat's algorithmic computerized review of Gasper's uploaded media data, regardless of whether Schroeder's personal conclusion about the age of the subject was accurate or inaccurate. However, it illustrates that Detective Schroeder, himself, was not confident in the reliability of Snapchat's computer scan alone to accurately assess the subject's age which is the essential element of a criminal charge for purposes of "probable cause" in a child pornography case.

B. The Warrantless Opening And Viewing Of Gasper's CyberTip By The Wisconsin Department Of Justice And The Waukesha County Sheriff's Department Expanded the Scope of Snapchat's Private Search.

In 2018 the Supreme Court issued its opinion in *Carpenter v. U.S.*, 585 U.S. 296, 138 S.Ct. 2206 (2018), expanding the constitutional reach of its earlier landmark 2014 decision in *Riley v. California*, *supra,* 573 U.S. 373 (2014). *Carpenter, supra,* and impressed Fourth Amendment warrant requirements upon governmental; accessing and reviewing private electronic data extracted from cellphones by third party private electronic service providers (ESP).

The Supreme Court in *Walter v. U.S.*, 447 U.S. 649 (1980); *U.S. v. Jacobsen*, 466 U.S. 109 (1984) and the Wisconsin Supreme Court in *State v. Payano-Roman*, 290 Wis.2d 380, 714 N.W.2d 548 (2006) confirm that "private searches" by third parties are an exception to the Fourth Amendment because the Fourth Amendment only applies to government action. Under this exception, when there is an antecedent "private party" search, the government may be justified in conducting a subsequent warrantless search only when it does not exceed the scope of the private party's antecedent search.

In *U.S. v. Wilson,* 13 F.4th 961 (9th Cir. 2021) and in *U.S. v. Holmes,* 121 F.4th 727 (2024), the U.S. Court of Appeals for the 9th Circuit addressed the unconstitutionality of law enforcement expansion of the scope of a previously unopened CyberTip derived from a computerized database search by an ESP of a user's private account. In both cases, law enforcement officers opened and viewed the previously unopened cyberdata contained in the CyberTip, without a warrant. In this respect, the facts in both *Wilson* and *Holmes* track with the facts in Gasper.

In Gasper's case, the governmental investigative process began with the Wisconsin Department of Justice receiving a CyberTip containing digital image data from Snapchat, extracted from Gasper's "cloud" account.

A CyberTip, by definition, only consists of a report of ". . . suspected incidents of child sexual exploitation that occur on the Internet; [*see:* Official Website of the United States Department of Justice, Office of Justice Programs, "CyberTipline: Your Resource for Reporting the Sexual Exploitation of Children". [R-53, pp. 1-3; R-App. 31-33.] Detective Schroeder testified on direct examination:

> Q Okay. Tell me about a CyberTip. What is a CyberTip?
>
> A. The CyberTip tip is from the National Center for Missing & Exploited Children, I'll refer to that as NCMEC, N-C-M-E-C. Anybody can file a CyberTip, if you go to Google and type in that you want to report something regarding child exploitation, NCMEC is probably going to be one of the first things that comes up as a -- anybody can file a CyberTip, …
>
> (emphasis added.)
>
> [R-60, pp. 10-14; R-App. 113-117.]

Detective Schroeder's March 20, 2023 search warrant affidavit submitted to Waukesha County Circuit Court Judge Paul Bugenhagen, Jr., in paragraphs 27 through 31, identified the specific factual bases for his seeking issuance of the search warrant as being the content of NCMEC CyberTip #152547912. [R-38, pp. 1-8; R-App. 23-30.] In his testimony, Detective Schroeder testified as follows:

> Q. The image was in the CyberTip itself, correct?
>
> A. Yeah, this e-mail is to notify us that we have a new case in IDS. Then I would go into that portal and download the file out of IDS. It's at that point that they would be able to see the image.
>
> Q. So is that the standard operating procedure in your department when you get such an image from the DOJ?
>
> A. Yes, I've been doing this for three years and this is the way that I have always done it.
>
> Q. Would it be fair to state that it was based upon that viewing of the imagery in the CyberTip that formed the basis for your application for a search warrant of Mr. Gasper's residence?
>
> A. Yes, sir.

[R-60, pp. 100-101; R-App. 146-147.] None of the paragraphs in Detective Schroeder's lengthy affidavit (misnomered "search warrant") make any reference to the content or integrity of the Snapchat database, or the reliability of PhotoDNA, MD5, or any other computerized logarithm scanning program being utilized by Snapchat, NCMEC, the Department of Justice, or Detective Schroeder, himself.

In short, circuit court Judge Bugenhagen, as the issuing judicial officer of the warrant, had no basis upon which to issue the search warrant other than the "judgment call" of Detective Schroeder after he opened and viewed the 16 second video imagery in the CyberTip without a warrant.

Detective Schroeder's description of that imagery to the issuing court is found in paragraph 31.c. of his affidavit and reads as follows:

> c. Description: This file is a 16 second color video. The video depicts a prepubescent light skinned female with dark hair, wearing what appears to be a blue t-shirt laying on her back. The prepubescent female does not have any pubic hair growth and breast development is unknown as the prepubescent female's breasts are covered by the t-shirt.

This description exemplifies that Detective Schroeder's exercise of personal judgment, based on what the video imagery visually depicted to him, to estimate the actual age of the female subject. The imagery reportedly does not show any pubic hair - but that is ambiguous because shaving of the pubic area would remove any visible pubic hair. He does not comment on the subject's physical size or apparent ethnicity; and cannot comment on breast development because of her wearing a tee shirt.

These descriptions are not brought to this Court's attention in this Brief to cast aspersions on Detective Schroeder's opinion as to the age of the subject in the video. The point is that these ambiguous observations arose from a warrantless search that formed the only factual basis provided to the issuing court to support "probable cause" for the court to issue the search warrant for Gasper's house, its contents and his cellphone.

Nowhere in Detective Schroeder's affidavit is there any mention of his relying on computerized "hash technology" or the reliability of such technology. That is the fundamental flaw in the Department of Justice protocol. It is at this early stage of investigating a child pornography case, prior to law enforcement opening and viewing "suspected" child pornography images technologically extracted by an ESP from a person's private cellphone account, that law enforcement needs to obtain a search warrant to conduct that examination.

The key word "suspected" was emphasized by the U.S. Court of Appeals in *Wilson*, and by the circuit court here, because it is elemental that ". . . mere suspicion does not suffice to establish "probable cause". *Brinegar v. U.S.*, 338 U.S. 160, 69 S.Ct. 1302 (1949). Accordingly, a computerized CyberTip of "suspected" child pornography standing alone, is not sufficient to provide "probable cause" for a search warrant to issue.

The U.S. Supreme Court's admonition in *Riley* and *Carpenter* is exquisitely clear that a warrant must be applied for before law enforcement agents open and view "suspected" contraband in cellphone data. A search warrant application in that instance informs the issuing judicial officer whether the CyberTip and its sourcing are sufficiently reliable to constitute "probable cause". Without that review, every computer-generated CyberTip would automatically substitute itself for the "detached and neutral magistrate" required by the Fourth Amendment.

The Court of Appeals decision here concedes that private internet platform companies that apply their hashtag technology to content passing through their computerized filter portals are "… neither law enforcement officers or criminal justice professionals." Yet, it is these private persons - not a neutral and detached magistrate - who control the ESP's database content, select the computer hash technology, apply it and transmit any resulting "SCSAM" via a CyberTip.

The Court of Appeals' theory is essentially the same theory that was urged by the government prosecutors in *Riley, infra,* which, upon careful consideration, was unanimously rejected by the Supreme Court in *Riley v. California, supra*, at 573 U.S. 373, 398, 134 S.Ct. 2473, 2482 and 2492.

> The **United States first proposes** that the *Gant* standard be imported from the vehicle context, **allowing a warrantless search of an arrestee's cell phone whenever it is reasonable to believe that the phone contains evidence of the crime of arrest**. (emphasis added.)

The Supreme Court's response to that position is summarized by this quote:

> Our cases have determined that "[w]here a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, … **reasonableness generally requires the obtaining of a judicial warrant**." *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 653, 115 S.Ct. 2386, 132 L.Ed.2d 564 (1995). **Such a warrant ensures that the inferences to support a search are "drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime**." (emphasis added.)
>
> *Riley v. California, supra*, 573 U.S. at 382, 134 S.Ct. at 2482.

Specifically, the Supreme Court's unanimous opinion in *Riley* closed with this admonition, which was later echoed in *Carpenter*:

> Our cases have recognized that the Fourth Amendment was the founding generation's response to the reviled "general warrants" and "writs of assistance" of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity. Opposition to such searches was in fact one of the driving forces behind the Revolution itself.
>
> * * * * * * * * * *
>
> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life," *Boyd, supra,* at 630, 6 S.Ct. 425 (1886). The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. **Our answer to the question of what police must do <u>before searching a cell phone</u> seized incident to an arrest is accordingly simple - <u>get a warrant</u>.** (emphasis added.)

Riley v. California, *supra*, 573 U.S. at 403, 1345 S.Ct. at 2495.

The Court of Appeals' decision in Gasper utterly fails to provide any explanation for the Department of Justice deliberately adopting a system which requires its own agents, and taught Detective Schroeder, to directly disobey the foregoing unmistakable command issued in 2016 by the Chief Justice of the United States Supreme Court, <u>writing for a unanimous court</u> in *Riley v. California*, *supra*; and reaffirmed by a similar directive in 2018 in *Carpenter*: "**<u>get a warrant</u>**". [*See: Carpenter v. U.S., supra,* 138 S.Ct. at 2221.]

III. <u>The "Good Faith" Exception To The Exclusionary Rule Does Not Apply To Obviate The Constitutional Violation Of The Fourth Amendment Warrant Requirement</u>.

The Wisconsin Attorney General has adopted and teaches law enforcement personnel to open and physically view without a warrant all CyberTip data received from NCMEC. Detective Schroeder explained this in his testimony, where he described his attendance at a seminar for law enforcement officers only months

before the hearing on this suppression motion, conducted by Wisconsin Assistant Attorney General Maas (who signed the Administrative Subpoena in this case), discussing *Wilson, supra*, and the attendees being instructed that they were not to request a warrant before opening and viewing CyberTip data from the NCMEC. [R-60, pp. 151-155; R-App. 172-176.]

This represents deliberate and intentional implementation by the Wisconsin Attorney General of its own public policy decision in direct conflict with the public policy decisions of the United States Supreme Court in *Carpenter*, *supra*, and *Riley*, *supra*, with respect to cellphone data searches.

These public policy decisions weighed the "cost to society" of implementing the exclusionary rule in warrantless cellphone content search cases. The resulting public policy decision with respect to cellphone privacy is unmistakably set forth in the quotes from *Riley, supra,* and *Carpenter*, *supra*, found on page 38 of this Respondent's Brief: "Get A Warrant."

The Supreme Court in *Riley* was fully aware of the impact of its decision to law enforcement investigative techniques:

> **We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime**. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. **Privacy comes at a cost**. (emphasis added.)
>
> *Riley v. California*, *supra*, 573 U.S. at 401, 134 S.Ct. at 2493.

The U.S. Court of Appeals in *U.S. v. Holmes*, 121 F.4th 727 (2024) engaged in an extensive analysis of the law supporting application of the "good faith" exception to the exclusionary rule for governmental violation of the Fourth Amendment warrant requirement for conduct identical to that existing here.

The *Holmes* court quoting from the U.S. Supreme Court Opinion in *Davis v. United States*, 564 U.S. 229, 131 S.Ct. 2419 (2011) stated:

> *When law enforcement asserts that it acted in good faith by relying on then-existing law, it must point to "binding appellate precedent" that authorizes the challenged conduct at issue.*
>
> [*Davis, supra*, at 564 U.S. at 241.]

The *Holmes* court continues to explain: "*Good faith is not established where existing precedent is unclear or makes the government's position only "plausibly permissible*." [*Holmes, supra*, 121 F.4th at 734-735.] At best, in the present case there is a split in the U.S. Courts of Appeal on the principles to be applied in the "private search" exception to the Fourth Amendment. Accordingly, the state of the law does not satisfy the "good faith" test set forth by the U.S. Supreme Court in *Davis v. U.S.*, 564 U.S. 229, 131 S.Ct. 2419 (2011), which is binding precedent.

The warrantless CyberTip data review procedure in this case represents a deliberate, systemic refusal to conform to the announced public policy constitutional determinations of the U.S. Supreme Court, which acknowledge application of the exclusionary rule as the societal "price" to pay for privacy - by prohibiting warrantless searches conducted by law enforcement officials of CyberTips containing cyberdata which emanated from cellphones.

Judicial implementation of this public policy was exemplified by the 2021 decision of the U.S. Court of Appeals for the 9th Circuit in *U.S. v. Wilson*, 13 F.4th 961 (9th Cir. 2021) and in *U.S. v. Holmes*, 121 F.4th 727 (9th Cir. 2024) with respect to warrantless police review of the CyberTip upload from a defendant's cellphone of "suspected" child pornography. In *Wilson*, *Holmes*, and in the present case, there was no antecedent authorization given by anyone to the government's warrantless examination of the CyberTip data extracted from defendant's cellphone.

There can be no "good faith" exception in this case because doing so ". . . would expand the good-faith exception to swallow, in a single gulp, the warrant requirement itself. That cannot be the law." *U.S. v. Sheehan*, 70 F.4th 36 (1st Cir. 2023).

In *Herring v. U.S.*, 555 U.S. 135, 144, 129 S.Ct. 694 (2009), the Supreme Court opined:

> 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. As laid out in our cases, the exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence. (emphasis added.)

The Wisconsin Attorney General has arrogated to itself the authority to reject and substitute its judgment for that of the United States Supreme Court on what the public policy considerations are for applying the exclusionary rule with respect to warrantless examination of cellphone data. In doing so, the Department of Justice does not meet the "clear and convincing" standard to satisfy its "good faith" under either *U.S. v. Leon*, 468 U.S. 897 (1984) or *State v. Eason*, 245 Wis.2d 206, 629 N.W.2d 625, 2001 WI 98 ¶74. The focus "tests" in *Leon, supra*, and the extra two tests in *Eason, supra*, have no application here because, at the direction of the Wisconsin Attorney General, no antecedent warrant is to be sought. If the Wisconsin Attorney General asserts that warrantless searches of cellphone data is "unsettled," the mandate from the United States Supreme Court is crystal clear in both *Riley* and *Carpenter*; when in doubt, "Get A Warrant". The Wisconsin Attorney General deliberately and with full knowledge of the Supreme Court's endorsement of the exclusionary rule, intentionally refuses to comply with that directive and trains law enforcement officers not to comply. That is systemic, deliberate, reckless, and grossly negligent conduct. It is certainly not "good faith."

CONCLUSION

Whether under the "reasonable expectation of privacy" public policy directive to "get a warrant" by the Supreme Court in both *Carpenter* and *Riley*, or deterrence of governmental expansion of the scope of previously unopened and unviewed ESP "private search" results of cyberdata computer scanning of a customer's private account data, the exclusionary rule requires suppression of evidence obtained as a result of warrantless opening and viewing of cellphone based CyberTip data from ESP customers' private internet accounts.

Accordingly, for all of the reasons set forth more particularly in this Defendant-Respondent-Petitioner's Brief, the published opinion of the Court of Appeals in this matter should be reversed and the decision and order of the circuit court granting the defendant's Motion to Suppress all evidence seized and all statements by Gasper following the subject search conducted on March 21, 2023, should be reinstated and affirmed.

Respectfully submitted this 23rd day of May, 2025.

Attorneys for Defendant-Respondent-Petitioner:

Law Offices of Joseph F. Owens, LLC
Electronically Signed By
/s/ Joseph F. Owens
Joseph F. Owens
State Bar No. 1016240

Law Offices of Debra K. Riedel
Electronically Signed By
/s/ Debra K. Riedel
Debra K. Riedel
State Bar No. 1002458

CERTIFICATION AS TO FORM AND LENGTH OF BRIEF

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 10,901 words.

Dated at New Berlin, Wisconsin on May 23, 2025.

Electronically Signed By
/s/ Joseph F. Owens
Attorney Joseph F. Owens
State Bar No: 1016240

DEFENDANT-RESPONDENT-PETITIONER'S BRIEF APPENDIX CERTIFICATION

I hereby certify that filed with this Brief, either as a separate document or as a part of 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 and Court of Appeals; (3) a copy of any unpublished opinion cited under Wis. Stat. §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 on May 23, 2025.

Electronically Signed By
/s/ Joseph F. Owens
Attorney Joseph F. Owens
State Bar No: 1016240