

**FILED**  
**11-26-2024**  
**CLERK OF WISCONSIN**  
**SUPREME COURT**

**STATE OF WISCONSIN  
SUPREME COURT**

---

**STATE OF WISCONSIN,**

Plaintiff-Appellant,

-v-

Appeal No. 2023-AP-2319 - CR

**MICHAEL JOSEPH GASPER,**

Defendant-Respondent.

---

**Petition for Review of a Decision of the Wisconsin Court of Appeals,  
District II, Dated October 30, 2024, Reversing An Order Granting  
Suppression Of Evidence Obtained By Warrantless Internet Search  
Entered In The Circuit Court For Waukesha County In  
Case No. 23-CF-000470, The Honorable Shelley J. Gaylord Presiding**

---

**PETITION FOR REVIEW**

---

ATTORNEYS FOR PETITIONER, MICHAEL JOSEPH GASPER,  
(DEFENDANT-RESPONDENT):

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

-and-

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

**TABLE OF CONTENTS**

	<b><u>Page</u></b>
OVERVIEW .....	4 - 7
TABLE OF AUTHORITIES CITED .....	8-10
REQUEST FOR REVIEW .....	11
STATEMENT OF ISSUES PRESENTED FOR REVIEW .....	11 - 12
STATEMENT OF CRITERIA FOR GRANTING REVIEW .....	13
STATEMENT OF THE CASE .....	13 - 16
A. Nature of the Case .....	13
B. Procedural History .....	13 - 15
C. Statement of Facts .....	15 - 16
ARGUMENT .....	17 - 33
I. Gasper Was Entitled To A “Reasonable Expectation of Privacy” In Data Uploaded To His Snapchat Account From His Cellphone.....	17 - 26
A. Cellphone Content Is Categorically Granted A Reasonable Expectation Of Privacy.....	17 - 20
B. Potential Criminal Content Of A Person’s Cellphone And ESP Account Do Not Void The Fourth Amendment’s Warrant Requirement .....	21 - 24
C. Snapchat’s Contract Documents Do Not Operate To Waive Gasper’s Fourth Amendment Rights Against Warrantless Searches By Law Enforcement Of His Cellphone And Related ESP Account .....	24 - 26

	<b><u>Page</u></b>
II. The March 3, 2023 Warrantless Viewing By Law Enforcement Of The Snapchat CyberTip Does Not Satisfy The “Private Search” Exception To The Fourth Amendment .....	26 - 31
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 .....	26 - 29
B. The Warrantless Opening And Viewing Of Snapchat’s CyberTip By The Wisconsin Department Of Justice And The Waukesha County Sheriff’s Department Violated The Fourth Amendment .....	29 - 31
III. The “Good Faith” Exception To The Exclusionary Rule Does Not Apply To Obviate The Constitutional Violation Of The Fourth Amendment Warrant Requirement In This Case .....	32 - 33
CONCLUSION .....	34
CERTIFICATION OF LENGTH AND FORM .....	35
APPENDIX CERTIFICATION .....	35

## OVERVIEW

The Court of Appeals’ decision in this warrantless search case announces, in a case of first impression, the fundamental legal proposition that an electronic service provider’s (ESP) Terms of Service adhesion contract operates to void a user’s objective and subjective Fourth Amendment expectation of privacy in data uploaded to the user’s ESP account.<sup>1</sup>

The Court of Appeals expressly identifies this case as presenting an issue of first impression:

¶ 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.)

[Slip Opinion, October 30, 2024, p. 12.]

The Court of Appeals in this opinion, which is recommended for publication, holds as a matter of law that ESP contract language of the sort utilized by Snapchat vitiates any “subjective” or “objective” expectation of privacy in a user’s account for Fourth Amendment purposes:

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.)

[Slip Opinion, October 30, 2024, ¶ 28, p. 13.]

The Court of Appeals’ Opinion proceeds to conclude that, under its legal analysis, Mr. Gasper contractually forfeited any expectation of privacy in the

---

<sup>1</sup> The circuit court Decision and Order and professional literature in the field of cybernetics uses the acronym “ISP” sometimes refer to providers such as Snapchat as an Internet Service Provider. The court of appeals’ Decision uses the acronym “ESP” referring to Snapchat as an Electronic Service Provider. For purposes of this appeal these two acronyms are used interchangeably.

content of his Snapchat account, which included a video uploaded from his cellphone. Therefore, the Court of Appeals posits that no Fourth Amendment “search” occurred when, without a warrant, Wisconsin law enforcement authorities in the Wisconsin Attorney General’s Office, and a Waukesha County Sheriff’s Detective, opened and viewed the content of previously unopened and unviewed CyberTip “hash” data of “suspected” child pornographic material (SCSAM) which, in the law enforcement agents’ opinions, constituted child pornography versus adult pornography. The Court of Appeals summarized its analysis with a categorical conclusory statement:

¶29 Detective Schroeder’s viewing of the video that accompanied the CyberTip did not constitute a search under the Fourth Amendment.

[Slip Opinion, October 30, 2024, p. 14.]

This case vitiates the Fourth Amendment rights of all members of the public who upload data from their cellphones to remote “cloud” storage accounts provided by an Electronic Service Provider (ESP).

Under the Wisconsin Department of Justice current investigative regimen, law enforcement agents are instructed by that Department to engage in warrantless opening and viewing of “Suspected Child Sexual Abuse Material” (SCSAM) via CyberTips received from the National Center for Missing and Exploited Children (NCMEC). That process directly violates the Fourth Amendment when applied to cellphone use and related data storage accounts per the U.S. Supreme Court precedents of *Carpenter v. United States*, 585 U.S. 296, 138 S.Ct. 2206 (2018) and *Riley v. California*, 573 U.S. 373, 134 S.Ct. 2473 (2014) and two U.S. Court of Appeals Circuits, *U.S. v. Wilson*, 13 F.4<sup>th</sup> 961 (9<sup>th</sup> Cir. 2021) and *U.S. v. Maher*, \_\_\_ F.4<sup>th</sup> \_\_\_, 2024 WL 4610759.

Under this process, when proprietary software employed by an Electronic Service Provider (ESP), such as Snapchat, Facebook, Google or Instagram, 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. Neither Snapchat or NCMEC opened or viewed the SCSAM data. However, NCMEC, using the user's Internet Protocol (IP) address, did locate the user's geographic locale.

Since the geographic locale of the user's IP address was within the State of Wisconsin, the Wisconsin Attorney General was sent the "CyberTip" by NCMEC. It is undisputed that under the Wisconsin Attorney General's official protocol, the previously unviewed CyberTip "hash" data is to be opened and physically viewed without a warrant by a Department of Justice administrative bureaucrat, (in this case one Matthew Lochowitz). Notably, the uncontroverted fact of this deliberate systemic governmental action by Wisconsin Attorney General personnel was virtually ignored by the Court of Appeals in its October 30, 2024 Opinion.

After opening and viewing the imagery contained in the CyberTip without a warrant, the Department of Justice then determined which local law enforcement agency had jurisdiction over the user's place of residence and forwarded the CyberTip to that agency. That was the Waukesha County Sheriff's Department, where Detective David Schroeder, also following the Wisconsin Attorney General's protocol, opened and viewed the CyberTip data image without a warrant.

The Court of Appeals decision announces that both of these acts of opening and viewing previously unopened stored user electronic data were not warrantless "searches" by government agents because Snapchat told its users that it prohibited storing such data on its servers, would monitor and potentially report it to law enforcement authorities.

This case therefore raises the threshold issue of whether a search warrant is required for law enforcement to open and view the content of data stored in a user's ESP account provided by the ESP to law enforcement personnel via a previously unopened "CyberTip" from NCMEC, which ostensibly matched the "hash" data of the CyberTip's imagery to an ESP proprietary database of prohibited imagery. In this case, the integrity of Snapchat's database was never established and Detective

Schroeder simply read into the record the CyberTip document in which the scanning software was identified as “MD5” - not “PhotoDNA”.

Based upon this factual record, the trial court followed 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*, 13 F.4<sup>th</sup> 961 (9<sup>th</sup> Cir. 2021) to grant the defense motion to suppress. On October 30, 2024, the same day that the Wisconsin Court of Appeals issued its Opinion in *Gasper*, the U.S. Court of Appeals for the 2<sup>nd</sup> Circuit joined that array of precedent in *U.S. v. Maher*, \_\_\_ F.4<sup>th</sup> \_\_\_, 2024 WL 4610759 [published but available only on Westlaw] [Pet. App. 199-224].

The Wisconsin Court of Appeals decision here posits that if an ESP computerized data filter program detects potential contraband in the form of “suspected” child pornographic content (SCSAM) in a customer’s account, the customer’s contract with the private ESP operates to forfeit any Fourth Amendment protection against governmental search and seizure of that content without a warrant.

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” one day can morph overnight into being applied to 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 and communications relating to obtaining abortion 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 contract provisions prohibiting illegal conduct or contraband do not waive the Fourth Amendment warrant requirement.

## TABLE OF AUTHORITIES CITED

<u>CASES</u>	<u>Page</u>
<i>Bumper v. North Carolina</i> , 391 U.S. 543, 885 S.Ct. 1788 (1968) .....	17
<i>Brinegar v. United States</i> , 338 U.S. 160, 69 S.Ct. 1302 (1949) .....	30
<i>Byars v. United States</i> , 273 U.S. 28, 47 S.Ct. 248-49 (1927) .....	22
<i>Byrd v. United States</i> , 584 U.S.395, 138 S.Ct. 1518 (2018) .....	23
<i>Carpenter v. United States</i> , 585 U.S. 296, 138 S.Ct. 2206 (2018) .....	5, 7, 11, 15, 18, 22, 23, 29, 31, 32, 33
<i>Herring v. United States</i> , 555 U.S. 135, 129 S.Ct. 694 (2009) .....	33
<i>Katz v. United States</i> , 389 U.S. 347, 88 S.Ct. 507 (1967) .....	22, 23
<i>Minnesota v. Olson</i> , 495 U.S. 91, 110 S.Ct. 1684 (1990) .....	23
<i>Payton v. New York</i> , 445 U.S. 573, 100 S.Ct. 1371 (1980) .....	22
<i>Riley v. California</i> , 573 U.S. 373, 134 S.Ct. 2473 (2014) .....	5, 7, 11, 15, 18, 19, 20, 24, 29, 30, 31, 32, 33
<i>Smith v. Maryland</i> , 442 U.S. 735, 99 S.Ct. 2577 (1979) .....	22, 23
<i>State v. Bowers</i> , 405 Wis.2d 716, 985 N.W.2d 123, 2023 WI App. 4 .....	19



**CASES****Page**

<i>State v. Burch</i> , 398 Wis. 1, 961 N.W.2d 314, 2021 WI 68 .....	19, 20
<i>State v. Eason</i> , 245 Wis.2d 206, 629 N.W.2d 625, 2001 WI 98 ¶74 .....	33
<i>State v. Tullberg</i> , 2014 WI 134, ¶27, 359 Wis. 2d 421, 857 N.W. 2d 120 .....	17
<i>Stoner v. California</i> , 3 76 U.S. 483, 84 S.Ct. 889 (1964) .....	23
<i>United States v. Ackerman</i> , 831 F.3d 1292 (10 <sup>th</sup> Cir. 2016) .....	27
<i>United States v. Leon</i> , 468 U.S. 897 (1984) .....	33
<i>United States v. Maher</i> , __ F.4 <sup>th</sup> __, 2024 WL 4610759 [Westlaw printed copy in Appendix] .....	5, 7, 26
<i>United States v. Matlock</i> , 415 U.S. 164, 94 S.Ct. 988 (1974) .....	23
<i>United States v. Miller</i> , 425 U.S. 435, 96 S.Ct. 1619 (1976) .....	22, 23
<i>United States v. Nafzger</i> , 965 F.2d 213 (7 <sup>th</sup> Cir. 1992) .....	17
<i>United States v. Sheehan</i> , 70 F.4 <sup>th</sup> 36 (1 <sup>st</sup> Cir. 2023) .....	33
<i>United States v. Thomas</i> , 65 F. 4 <sup>th</sup> 922, 925 (7 <sup>th</sup> Cir. 2023) .....	24
<i>United States v. Warshak</i> , 631 F.3d 266 (6 <sup>th</sup> Cir. 2010) .....	27

**CASES****Page**

<i>United States v. Wilson</i> , 13 F.4 <sup>th</sup> 961 (9 <sup>th</sup> Cir. 2021) .....	5, 7, 11, 30, 32
--	---------------------

**STATUTES CITED**

Wis. Stat. §808.10 .....	11
Wis. Stat. §809.62 .....	11
Wis. Stat. §809.62(1r) .....	13

**OTHER AUTHORITIES**

U.S. Dept. of Justice, Office of Justice Programs Article entitled: “CyberTipline: Your Resource for Reporting The Sexual Exploitation of Children” Published 2003 .....	29
--	----

## **REQUEST FOR REVIEW**

The Defendant-Respondent, Michael Joseph Gasper, petitions the Supreme Court of Wisconsin, pursuant to Wis. Stat. §808.10 and 809.62 to review the decision of the Wisconsin Court of Appeals, District II, in *State of Wisconsin v. Michael Joseph Gasper*, Appeal No. 2023-AP-002319-CR, filed on October 30, 2024, which the Court of Appeals has recommended for publication.

### **STATEMENT OF ISSUES PRESENTED FOR REVIEW**

**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 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.4<sup>th</sup> 961 (9<sup>th</sup> Cir. 2021), and referencing multiple law review articles in footnote 2. of its Decision and Order [Pet. App. 2].

The trial court decision, adverse to the State, was raised by the State in pages 15 - 23 of its appellate brief.

**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.)

[Pet. App. 1-2, Slip Opinion pp. 1-2.]

**II. WHETHER THE MARCH 3, 2023 WARRANTLESS VIEWING BY LAW ENFORCEMENT OF THE SNAPCHAT CYBERTIP SATISFIES THE “PRIVATE SEARCH” EXCEPTION TO THE FOURTH AMENDMENT.**

**Answered By The Trial Court:** In The Negative.

The trial court decision, adverse to the State, was raised by the State in pages 24-34 of its appellate brief.

**Not Addressed By The Court Of Appeals,** which expressed the following rationale set forth in footnote 8. on page 14 of the Slip Opinion:

<sup>8</sup> 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 VIOLATION OF THE FOURTH AMENDMENT WARRANT REQUIREMENT IN THIS CASE.**

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

The trial court ruling, adverse to the State, was raised in the State’s appellate brief on pages 41-43.

**Not Answered By The Court Of Appeals,** which expressed the following rationale set forth in footnote 8. on page 14 of the Slip Opinion:

<sup>8</sup> Because we determine that no Fourth Amendment “search” occurred, we need not reach the additional grounds the State set forth for reversal . . . .

### **STATEMENT OF CRITERIA FOR GRANTING REVIEW**

The issues in this case meet the following criteria for granting review in Wis. Stat. §809.62(1r):

(a) A real and significant question of federal and state constitutional law is presented because the Court of Appeals' decision identifies this case as presenting an issue of first impression under the Fourth Amendment relating to law enforcement warrantless access to an internet user's data uploaded from the user's cellphone to an Electronic Service Provider's system.

(b) The issues raised in the Petition for Review similarly demonstrate a need for the Supreme Court to establish a policy relating to the criteria for the judiciary to follow in granting or denying requests for warrants to open and physically view content of user accounts maintained on Electronic Service Provider servers.

(c) A decision by the Supreme Court will develop, clarify and harmonize the law, and the primary question presented is novel, the resolution of which will have statewide impact and center on issues of law of the type that are likely to recur unless resolved by the Supreme Court.

(d) The decision of the Court of Appeals as it relates to data uploaded from cellphones to "the *Cloud*" is in conflict with controlling opinions of the United States Supreme Court and two other federal court of appeals' decisions.

### **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 data uploaded to user accounts 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; Pet. App. 46-48.]

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; Pet. App. 49-63]. The application for Search Warrant was predicated upon assertions made by Detective Schroeder [R-6, pp. 20-22 ¶¶27-38; Pet. App. 60-62] in which he stated that he had opened and reviewed the video referenced in a Snapchat report of "apparent child pornography" to the National Center for Missing and Exploited Children (NCMEC) via CyberTip #152547912. In doing so, he 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; Pet. App. 61.]

On March 22, 2023, the Waukesha County District Attorney's Office filed the Criminal Complaint in this matter based on the information first obtained by the Wisconsin Department of Justice from 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; Pet. App. 23 - 42].

On May 11, 2023, Gasper filed a separate Motion to Suppress Statements and Fruits of Illegal Arrest. [R-24, pp. 1-3; Pet. App. 43-45.]

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; Pet. 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; Pet. 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.

**C. Statement of Facts.**

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. [Pet. App. 2-5.]

In short, the 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 an 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. 32; Pet. App. p. 66.]

It is uncontroverted that every charge against Gasper came exclusively from use of Gasper's cellphone. [R-60, p. 96; Pet. App. 153.]

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

The Court of Appeals' Opinion in ¶12 reversed the circuit court's finding 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. [Pet. App. 7.]

The Court of Appeals' Opinion in ¶15 recites that Snapchat internally obtained the subject video by scanning its servers. [Pet. App. 8-9.]

The Court of Appeals' Opinion in ¶¶16-19 then identified the Snapchat documents it deemed relevant to its decision consisting of three contractual 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 was the November 2022 "Snap, Inc. Terms of Service". There was no evidentiary foundation as to when the January 2023 Snapchat's "Community Guidelines" and its January 2023 "Sexual Content Community Guidelines Explainer Series" was adopted or disseminated by Snapchat to its users. [Pet. 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 Microsoft's Photo DNA program to scan user files. [Pet. App. 2.] 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, and not Microsoft's Photo DNA program, despite Detective Schroeder's verbal testimony that he believed Snapchat had used "Photo DNA". [R-38; Pet. App. 64-71; R-60, pp. 23-27; 30-35; 37-41; 150-151; Pet. App. 129-141; 172-175; 182-183.]

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. [Pet. 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, pp. 1-17; Pet. App. 98-112-B; R-60, pp. 140-146; Pet. App. 175-181.] 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 at pages 21-22 in the Court of Appeals.



## 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.**

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 resulting 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 a search warrant being 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. Nafziger*, 965 F.2d 213 (7<sup>th</sup> 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 through his cellphone. [R-60, p. 96; Pet. App. 153.] 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.

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) announce a public policy decision that in today's world cellphone users have 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 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 servers of an electronic service provider (ESP).

In *Riley, supra*, 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:

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 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; Pet. App. 62] confirmed that all of Gasper 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; Pet App. 98; R-60, pp. 140-146; Pet. App. 175-181] constituted a declaration to the court in the form of an offer of proof 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; Pet. App. 177-181.] 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 (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 cell phone 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 cell phone 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 to the Supreme Court threshold 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 have to prove up an expectation of privacy in each item on their cellphones, including when it is stored remotely on an ESP server.

Accordingly, "cloud" storage of his cellphone data on his Snapchat account meets Michael Gasper's "reasonable expectation of privacy" threshold standing requirements to assert Fourth Amendment violations relative to the Wisconsin Attorney General's Office and Detective Schroeder's warrantless opening and review of his cellphone data.

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

The Court of Appeals' decision in a nutshell, 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 the Fourth Amendment warrant requirements. The Court of Appeals' decision dispenses with the need to engage in any bothersome analysis of 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 open and examine a previously unviewed and unopened cache of data in a user's account without a warrant. This process substitutes the ESP 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." The state's substantive argument here is that 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 the closed 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. 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.”

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 and deposits 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 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 search doctrine to a distinct category of information:

The government thus is not asking for a straight forward 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 contract 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).

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 7<sup>th</sup> Circuit is in accord, per Circuit Judge Easterbrook’s opinion in *United States v. Thomas*, 65 F. 4<sup>th</sup> 922, 925 (7<sup>th</sup> 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.

C. **Snapchat’s Contract 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 moves to an examination of the actual relationship between Michael Gasper and Snapchat by looking to the terms of the contract between them.

The Snap, Inc. contractual documents are its: (a) “Terms of Service” [R-41, pp. 1-16; Pet. App. 72-87]; (b) “Community Guidelines” [R-42, pp. 1-6; Pet. App. 88-93]; and (c) “Sexual Content Community Guidelines Explainer Series” [R-44, pp. 1-4; Pet. App. 94-97].



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

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

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; Pet. App. 75.]

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; Pet. App. 78.]

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; Pet. App. 89.]

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; Pet. App. 96.]

Snap, Inc. warns its customers that it can internally monitor the data passing through its portals. This apparently is done via an internally programmed algorithm hash technology. In its November 2022 Terms of Service, Snap, Inc. notifies its customers that it “reserves the right” and “may” report to law enforcement negatively flagged customer data which Snap, Inc. In its January 2023 Community Guideline documents, which do not have an explicit effective date in January of 2023, Snapchat states that it will notify the NCMEC of suspected child pornography, not law enforcement agencies. However, none of the Snap, Inc. private contractual documents state the user grants “governmental agencies” any authority to open and view the customer data flagged by Snap, Inc.’s data filter technology. That is the key element that is missing from the Court of Appeals’ decision. As explained by the U.S. Court of Appeals for the 2<sup>nd</sup> Circuit in the Discussion Section II. A. of its opinion in *U.S. v. Maher*, \_\_ F.4<sup>th</sup> \_\_, 2024 WL 4610759, released on October 30, 2024, the same day as the Wisconsin Court of Appeals’ decision in *Gasper*, an ESP terms of service “does not extinguish a person’s expectation of privacy, as against the government, in the content in its files.”

**II. The March 3, 2023 Warrantless Viewing By Law Enforcement Of The Snapchat CyberTip Satisfies 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 did so. Snap, Inc. personnel did not do so. Neither did personnel at the National Center for Missing and Exploited Children.

The legal import of these facts is exhaustively explained by then Circuit Judge Neil Gorsuch, in *United States v. Ackerman*, 831 F.3d 1292 at pp. 1295-1304 (10<sup>th</sup> Cir. 2016). The Gorsuch opinion in *Ackerman*, *supra*, at pp. 1304-1305, also explains that the “third party doctrine” does not absolve a warrantless governmental search of an ESP reported CyberTip from the Fourth Amendment warrant requirements, citing *United States v. Warshak*, 631 F.3d 266, 283-288 (6<sup>th</sup> Cir. 2010).

Here, it is 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; Pet. App. 183-184.]

Notably, Detective Schroeder testified that every charge against Gasper arose from use of Gasper’s cellphone. [R-60, p. 96; Pet. App. 153.]

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; Pet. App. 64-71.] In his 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; Pet. App. 157-158.] 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.

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; Pet. App. 61.]

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 cannot 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 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 the CyberTip being generated by computerized “hash technology” or the reliability of such technology. That is fundamental flaw in the Department of Justice protocol at this preliminary stage of investigating a child pornography case.

Detective Schroeder’s physical 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 ability of Snapchat's computer scan alone to accurately assess the subject's age.

**B. The Warrantless Opening And Viewing Of Snapchat's CyberTip By The Wisconsin Department Of Justice And The Waukesha County Sheriff's Department Violated The Fourth Amendment.**

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*, impressed Fourth Amendment warrant requirements upon government accessing and reviewing private electronic data extracted from cellphones by third party private service providers (ISP).

In Gasper's case, the governmental investigative process began with 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; Pet. App. 193-195.] 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; Pet. App. 124-128.]

The key word “suspected” was important to the Court of Appeals in *Wilson* and to 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 CyberTip of “suspected” child pornography standing alone is not sufficient to provide “probable cause” for a search warrant to issue.

The Supreme Court is exquisitely clear in its admonition that a warrant should 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 inferences to be drawn from 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 does not dispute that private internet platform companies that apply their hashtag technology to images and files passing through their portals are “... neither law enforcement officers or criminal justice professionals.” Yet, it is these private persons - not a neutral and detached magistrate - who decide on the ESP’s database content, then select and program the computer hash technology, apply it and transmit its resulting identification of “suspected child pornography” via a CyberTip.

The Court of Appeals’ theory is essentially the same theory urged by the government 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 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.

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 before searching a cell phone seized incident to an arrest is accordingly simple - get a warrant.** (emphasis added.)

*Riley v. California, supra*, 573 U.S. at 403, 134 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 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, writing for a unanimous court in *Riley v. California, supra*; reaffirmed by a similar directive in 2018 in *Carpenter*: **“get a warrant”**. *Carpenter v. U.S., supra*, 138 S.Ct. at 2221.

**III. The “Good Faith” Exception To The Exclusionary Rule Does Not Apply To Obviate The Constitutional Violation Of The Fourth Amendment Warrant Requirement In This Case.**

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 Gasper), 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; Pet. App. 183-187.]

This represents knowing and intentional implementation by the Wisconsin Attorney General of a 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.

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 CyberTip provided cellphone data.

Judicial implementation of this public policy was exemplified by the 2021 decision of the U.S. Court of Appeals for the 9<sup>th</sup> Circuit in *U.S. v. Wilson*, 13 F.4<sup>th</sup> 961 (9<sup>th</sup> Cir. 2021) with respect to warrantless police review of the CyberTip upload from a defendant’s cellphone of “suspected” child pornography. In *Wilson* and in the present case, there was no antecedent consent given to the government’s warrantless review 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.4<sup>th</sup> 36 (1<sup>st</sup> 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 Attorney General, there no antecedent warrant is to be sought. The law with respect to warrantless searches of cellphone data is not “unsettled”. The mandate from the United States Supreme Court is crystal clear in both *Riley* and *Carpenter*: “Get A Warrant”. The Wisconsin Attorney General deliberately and with full knowledge of the exclusionary rule, intentionally refuses to comply with that directive and trains law enforcement officers not to comply. At a minimum, that is “systemic negligence,” and certainly not “good faith.”

### **CONCLUSION**

For the foregoing reasons set forth particularly above, the Petitioner, Michael J. Gasper, requests that based upon the criteria identified herein, the Supreme Court undertake review and consideration of the issues identified herein.

Respectfully submitted this 26<sup>th</sup> day of November, 2024.

Attorneys for Defendant-Appellant:

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

By: Debra K. Riedel

State Bar No. 1002458

---

**CERTIFICATION AS TO FORM AND LENGTH OF  
PETITION FOR REVIEW**

---

I hereby certify that this Petition for Review conforms to the rules contained in Wis. Stat. §§809.19(8)(b), (bm) and (c) and 809.62(4) for a petition produced with a proportional serif font. The length of this Petition is 7,913 words.

Dated at New Berlin, Wisconsin on November 26, 2024.

*Electronically Signed By*

/s/ Joseph F. Owens

Attorney Joseph F. Owens  
State Bar No: 1016240

**APPELLANT'S PETITION FOR REVIEW APPENDIX CERTIFICATION**

I hereby certify that filed with this Petition for Review, either as a separate document or as a part of this Petition for Review, is an appendix that complies with Wis. Stat. §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 November 26, 2024.

*Electronically Signed By*

/s/ Joseph F. Owens

Attorney Joseph F. Owens  
State Bar No: 1016240