FILED
04-16-2024
CLERK OF WISCONSIN
COURT OF APPEALS

STATE OF WISCONSIN
WISCONSIN COURT OF APPEALS
DISTRICT II

STATE OF WISCONSIN,

Plaintiff-Appellant,

-v-

MICHAEL JOSEPH GASPER,

Defendant-Respondent.

Appeal No. 2023-AP-2319 - CR

Circuit Court Case No. 23-CF-000470
Circuit Court of Waukesha County
Hon. Shelley J. Gaylord, Presiding

BRIEF AND SUPPLEMENTAL APPENDIX OF DEFENDANT-RESPONDENT

Attorneys for Defendant-Respondent:
Electronically signed 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
(262) 785-0320
Owenslaw2@gmail.com

Electronically signed by:
DEBRA K. RIEDEL
State Bar No. 1002458

Law Offices of Debra K. Riedel
2665 S. Moorland Road, Suite 200
New Berlin, WI 53151
(414) 277-7818
riedellaw@dkriedellaw.com

OVERVIEW

This case addresses the Fourth Amendment rights of all members of the public who use cellphones. The Wisconsin Attorney General's Office utilize what is clearly a very efficient system for investigating CyberTips emanating from Internet Service Providers (ISP) which extract data from a person's cellphone use. However, the Wisconsin Attorney General's system, while efficient, is constitutionally flawed because it is predicated on a search by the government of the content of cellphone users' accounts without a warrant.

Under the Wisconsin Department of Justice investigative system, law enforcement agents are instructed to open and view third party "Suspected Child Sexual Abuse Material" (SCSAM) received from the National Center for Missing and Exploited Children (NCMEC) without a warrant. That process violates the Fourth Amendment when applied to cellphone use and data.

Under this process, when proprietary software employed by an Internet Service Provider (ISP), such as Snapchat, Facebook, or Instagram, detects SCSAM, the ISP 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 ISP differs from one to the other. Neither the ISP 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 the "CyberTip" by NCMEC. It is undisputed that under the Wisconsin Attorney General's system, the previously unviewed CyberTip image data is opened and physically viewed, without a warrant, by a Department of Justice administrative bureaucrat, (in this case identified as Matthew Lochowitz). Notably, this key fact is scrupulously avoided

in the State's Brief. 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 system, opened and viewed the CyberTip data image without a warrant.

Both of these acts of 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.

The Attorney General's Brief at p. 40 warns this court that requiring law enforcement agents to obtain a warrant before opening CyberTips received from NCMEC will "… grind both law enforcement agencies and the courts charged with reviewing warrant applications to a halt." This "doomsday" prediction fails to recognize that only previously unopened cellphone CyberTips would be subject to the Fourth Amendment warrant requirements of *Carpenter v. U.S.*, 138 S.Ct. 2206 (2018) and *Riley v. California*, 573 U.S. 373 (2014).

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 from a previously unopened CyberTip from NCMEC, which ostensibly matched the CyberTip's imagery to an ISP unidentified database of imagery through an Artificial Intelligence (AI) computerized scanning program. In this case, the integrity of

Snapchat's database was never identified and its scanning software is identified as "MD5" - not "PhotoDNA". Based upon these factual conclusions, the circuit court applied the U.S. Supreme Court holdings in *Carpenter*, *infra*; *Riley, infra;* and *U.S. v. Wilson*, 13F.4th 961 (9th Cir. 2021) to grant the defense motion to suppress.

From a policy perspective, a streamlined warrant application procedure based upon an officially endorsed technologically reliable construct for CyberTip reliability, shown to have been followed by an ISP, would avoid this problem. An example would be the body of law granting *prima facie* evidentiary status to alcohol breath testing devices which have been certified to be reliable by a State administrative agency (such as the Wisconsin Department of Transportation). Law enforcement and judicial officers would thereby have a fully vetted process to assess "probable cause" when a search warrant is sought to open and view a private citizen's cellphone data. Such a process would be as facially reliable to establish "probable cause" for issuance of a search warrant as the routine statements by search warrant applicants to an issuing judicial officer which rely on information from historically reliable "Confidential Informants".

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 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 cellphone data. Instead, they turn to the judiciary to provide a loophole to avoid compliance with the Fourth Amendment.

The Wisconsin Attorney General's Brief advances various arguments requesting this Court to adopt the State's basic theme that cellphone customers waive their Fourth Amendment privacy rights by agreeing to an ISP's service contract. The State posits that if an ISP computerized filter program detects

potential contraband in the form of "suspected" child pornographic content in a customer's account, the customer's contract with the private ISP operates to forfeit in advance any Fourth Amendment protection against governmental searching and seizing that content without a warrant. If that is the law, we all need to know it because what is contraband one day can morph overnight into another form of contraband by legislative fiat (e.g., material sympathetic to the Communist Party during the 1950's and intoxicating liquor during the Prohibition Era of the 1920's). The State basically maintains, without a sufficient evidentiary foundation, that ISP Artificial Intelligence (AI) software programs are so reliable that human review for "probable cause" should be deemed superfluous and completely unnecessary for the issuance of a search warrant.

TABLE OF CONTENTS

TABLE OF AUTHORITIES CITED

CASES **Page**

STATUTES CITED

OTHER AUTHORITIES

STATEMENT OF ISSUES

I. WHETHER GASPER HAD A "REASONABLE EXPECTATION OF PRIVACY" IN CELLPHONE UPLOADS TO HIS SNAPCHAT ACCOUNT?

Answered by the Circuit Court: Yes.

II. WHETHER THE "PRIVATE SEARCH DOCTRINE" ALLOWS A LAW ENFORCEMENT AGENCY TO OPEN A PREVIOUSLY UNOPENED VIDEO UPLOADED FROM GASPER'S CELLPHONE TO HIS PRIVATE SNAPCHAT ACCOUNT?

Answered by the Circuit Court: No.

III. WHETHER THE "GOOD FAITH EXCEPTION" TO THE EXCLUSIONARY RULE CAN VALIDATE THE WARRANTLESS SEARCH AND VIEWING OF THE PREVIOUSLY UNOPENED VIDEO UPLOADED FROM GASPER'S CELLPHONE TO HIS PRIVATE SNAPCHAT ACCOUNT?

[**This issue was not presented or argued by the State in the Circuit Court**.]

Not answered by the Circuit Court:
"*U.S. v. Reddick, good faith exception (5th Cir. 1981) not argued in Gasper. Good faith unlikely in Gasper's case given the split in court decisions*."

STATEMENT ON ORAL ARGUMENT AND PUBLICATION

A. Oral Argument.

The Defendant-Respondent, Michael J. Gasper, agrees with the State that oral argument would aid in addressing the issues presented in this case, which involve complicated technology and are of statewide import.

B. Publication.

Resolution of the case by the Court of Appeals 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. Standard Of Review.

The State seeks appellate review of the circuit court's decision granting the defendant's Motions to Suppress in this case which involve both questions of fact and law. [R-23, pp. 1-20; Supp. App. pp. 3-22.] This case presents the grant of a suppression motion based on the Fourth Amendment to the United States Constitution and Article I, Section 11 of the Wisconsin Constitution. It raises questions of constitutional fact and law. *State v. Howes*, 373 Wis.2d 648, 893 N.W.2d 812, 2017 WI 18 ¶17. Circuit court decisions on questions of fact are entitled to deference and will not be reversed unless clearly erroneous. Wis. Stat. §805.17(2). Circuit court decisions in questions of law are reviewed on appeal *de novo*. *State v. Vanmanivong*, 261 Wis.2d 202, 661 N.W.2d 76, 2003 WI 41 ¶17.

Issue 1. The State's first issue on appeal relates to Gasper's "reasonable expectation of privacy". In deciding this issue the circuit court relied upon the U.S. Supreme Court's decisions in *Riley v. California*, 573 U.S. 373 (2014) and *Carpenter v. U.S.*, 138 S.Ct. 2206 (2018). The circuit court's decision applied evidentiary findings of fact to a legal standard, the result of which is reviewed *de novo* on appeal. The circuit court accepted as established facts of record that Gasper used only a cellphone on a private Snapchat account which was password protected, as was his access to his internet IP address. In addition, there was no evidence or allegation that Gasper shared data on his account with other users. The circuit court ruled as a matter of law that a search warrant was required to open and view the CyberTip data extracted by Snapchat.

Issue 2. The State's second issue on appeal asserts that the circuit court erred in failing to find that the "private search" exception to the Fourth Amendment warrant requirement was satisfied. The evidentiary facts were undisputed that no person opened or viewed the 16 second video CyberTip prior to Wisconsin Attorney

General Agent Lochowitz and Waukesha County Sheriff's Office Detective Schroeder doing so without a warrant. This issue therefore presents the circuit court applying evidentiary facts to a legal standard, which is reviewed *de novo* on appeal.

Issue 3. The State's third issue, the "good faith" exception to the exclusionary rule, was never raised by the State in the circuit court other than a vague statement made in passing by Assistant District Attorney Gordon that the State agents did not act "unreasonably". [R-60, p. 170; Supp. App. p. 163.] In terms of the applicable "standard of review", the State asks this appellate court to essentially act as a trial court and apply evidentiary facts by "clear and convincing evidence" to find an exception to the "exclusionary rule", which otherwise applies to violations of the Fourth Amendment warrant requirements. This novel appellate procedure requested by the State places the defendant in the position of having to defend, and this Court to rule on, an issue as to which the defendant has had no prior notice, opportunity to cross-examine, or adduce evidence beyond that which is in the record. That issue is the "good faith" exception to the exclusionary rule which otherwise applies to violations of the warrant requirement of the Fourth Amendment. In a criminal case, this implicates Sixth Amendment rights of the defendant and is objected to on that basis. [*See: Giordenello v. U.S.*, 357 U.S. 480, 488, 78 S.Ct. 1245, 1251 (1958) and *U.S. v. Hahn*, 922 F.2d 243 (5th Cir. 1991)]. Accordingly, this issue is not properly before the Court on appeal. However, to avoid any issue of waiver or forfeiture by the Respondent, the arguments of the State on this issue will be addressed in Respondent's Brief strictly as an issue of law using the facts of record as they exist.

B. Supplemental Statement Of Facts.

The State's Appellate Brief recites 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 review the hash data contained in the CyberTip. [R-60 pp. 23-27; Supp. App. pp. 100-104; R-60, pp. 30-35; Supp. App. pp. 105-110; R-60 pp. 137-140; Supp. App. pp. 143-146; R-60 pp. 150-151; Supp. App. pp. 153-154; R-38 p. 3; Supp. App. p. 32.]

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, Supp. App. pp. 111-112.]

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; Supp. App. p. 123.]

The only representation of accuracy of PhotoDNA was Detective Schroeder's unsupported reference to advertising in response to inquiry from the court as follows:

> The Court: I'm just saying, he described PhotoDNA. He's described his experience. Is there something else?
>
> The Witness: I think PhotoDNA advertises one in 10 billion for a false positive, so that would be my impression, that unless I have one in 10 billion, I'm going to open child sexual abuse material when I click on that video.

> Mr. Owens: That's no foundation. That's what some advertiser says.

[R-60, p. 67; Supp. App. p. 122.]

These facts become important because the circuit court actually researched the State's assertions of "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; Supp. App. p. 23.] The circuit court found those assertions by the State not credible. On page 5 of the circuit court's decision [A-App. p. 7-8] 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 marked as Trial Exhibit 3 [R-38, pp. 1-8; Supp. App. pp. 30-37] 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 Trial Exhibit 3 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 = False indicates that the reported media was detected by PDNA hash matching technology 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; Supp. App. pp. 30-37] shows that program "MD5" was used, but the key word "False" does not appear anywhere in that document - which would indicate that PhotoDNA was used to detect the requested media. In the absence of the word "False" in the document, the reported media was not detected by PhotoDNA.

The State's Brief accurately recites 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, a date of birth of 04-06-1971, and an "IP address" of "184.100.214.42."[1] [R-60, pp. 156-159; Supp. App. pp. 159-162.]

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 Brief avoids informing this Court that the CyberTip was then opened and viewed without a warrant by Wisconsin Department of Justice "designee", Matthew Lochowitz. This was the first warrantless search. According to the State Attorney General's investigating *schema,* 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; Supp. App. pp. 113-116; R-60, pp. 96-99; Supp. App. pp. 124-127; R-60, pp. 100-101; Supp. App. pp. 128-129.] This "Administrative Subpoena" was ostensibly issued pursuant to Wis. Stat. §165.505(2) without "probable cause" by a non-judicial officer. [R-39, pp. 1-3; Supp. App. pp. 38-40.] 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 media CyberTip file was then sent by the DOJ to the Waukesha County Sheriff's Department.

---

[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.

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" 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 solely upon Detective Schroeder's warrantless March 2, 2023 opening and viewing of the subject Snapchat media file. [R-60, pp. 106 - 111; Supp. App. pp. 130-135.] The precatory recitations of the search warrant requested 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, and a plethora of items which are described more particularly in the precatory paragraphs of the subject search warrant. However, the operative portion of the search warrant "particularly" described its scope as being 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; Supp. App. p. 53.]

The resulting search warrant was exhibited and executed on March 21, 2023 at 5:33a.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; Supp. App. pp. 136-

140.] Detective Schroeder confirmed that official reports filed by Detective Knipfer and Deputy Thompson 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; Supp. App. pp. 138-129.] The defendant, Michael Gasper, without an arrest warrant, was immediately handcuffed and placed into a sheriff's vehicle, his cell phone 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; Supp. App. pp. 141-142.]

ARGUMENT

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

A. Cellphone Data Is Categorically Granted A Reasonable Expectation Of Privacy As A Matter of Law.

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 provides in identical language:

> **Searches and seizures**. SECTION 11. 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 warrant 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.

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 on two levels by government agencies in the investigative process resulting in the criminal charges here preferred against Michael Gasper. These agencies were: (a) the Wisconsin Attorney General's Office; and (b) the Waukesha County Sheriff's Office. This unconstitutional warrantless search led to the issuance of a search warrant being executed on March 21, 2023 with 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).]

The State's Brief accurately summarizes the chronological steps taken by it to access and review a single CyberTip of alleged contraband video imagery uploaded from the defendant, Michael Gasper's, cellphone. Notably, it is uncontroverted that the alleged contraband imagery in this case relied upon by the

State as constituting the basis for the criminal charges filed against the defendant, was solely through his cellphone. [R-60, p. 96; Supp. App. p. 124.] No other electronic device is involved. This fact has major significance here because the fundamental privacy rights of persons to their cellphone content controls the Fourth Amendment obligations imposed on law enforcement conduct in this case.

The Argument portion of the State's Appellate Brief begins with the statement that the defendant bears the burden of demonstrating that he or she had a reasonable expectation of privacy in the subject of the alleged unconstitutional search. This is an accurate statement but skips over the correlative burden of the State, that in the case of a warrantless search, the government bears the burden of establishing by "clear and convincing evidence" an exception to the Fourth Amendment warrant requirement. *Coolidge v. New Hampshire*, 403 U.S. 443, 91 S.Ct. 2022 (1971); *U.S. v. Kennedy*, 427 F.3d 1136, 1140 (8th Cir. 2005).

The State's Brief on p. 20 erroneously states that Gasper offered no evidence to support his subjective expectation of privacy in his cellphone or Snapchat account. In fact, Detective Schroeder's sworn affidavit in support of issuance of the search warrant of the residence [R-45, p. 18; Supp. App. p. 68] confirmed that the 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.

In addition, the Affidavit of Michael Gasper [R-54, p. 1; Supp. App. p. 73; R-60, p. 141; Supp. App. p. 147] represented to the court in the form of an offer of proof 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; Supp. App. pp. 148-152.] 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.

Moreover, cellphones and their content are granted special protected privacy status under the Fourth Amendment. In *Riley v. California,* 573 U.S. 373, 134 S.Ct. 2473, 189 L.Ed.2d 432 (2014), the defendant was convicted of complicity in a drive-by shooting based on a warrantless search of data on his cellphone incident to his arrest. The Supreme Court in a unanimous opinion, categorically announced that all persons have a "reasonable expectation of privacy" in the content of their cellphones, including that stored on remote services. "***Modern cellphones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse***." *Riley*, *supra*, 573 U.S. at 393, 134 S.Ct. at 2488-89.

The breadth of this holding has been recognized 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," and went on to state that "[p]ermitting law enforcement to rummage through the data residing in smartphones without a warrant would 'allow free rein to search for potential evidence of criminal wrongdoing,' which the Fourth Amendment prohibits". *Burch, supra*, ¶47, ¶52.

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). She found that, "[p]eople have a unique and heightened expectation of privacy in their cell phone data that demands commensurate Fourth Amendment protection." *Id.* It is therefore, "a grave analytical error to 'mechanically apply ["to cell phone data Fourth Amendment rationales that were developed without such invasive technologies in mind."] *Id*., ¶86.

The *Riley, supra,* U.S. Supreme Court opinion explains in detail why it was granting "categorical" recognition of a "reasonable expectation of privacy" as a matter of law 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.

> 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.

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. The State's citations from *State v. Bruski*, 2007 WI 25, 299 Wis.2d 177, 727 N.W.2d 503; and *Illinois v. Caballes*, 543 U.S. 405, 125 S.Ct. 834 (2005) predate and are superseded by *Riley v. California, supra,* and are therefore inapplicable here.

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

The State tacitly narrows its position to the proposition that Gasper has no "reasonable expectation of privacy" in the 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 State posits that Michael Gasper lost any "reasonable expectation of privacy" in that uploaded data.

Framing the issue in this manner runs afoul of the basic Fourth Amendment principle that illegal content of private communications does not void the Fourth Amendment's warrant requirements. The fact that the subject and content of conversations intercepted by an unauthorized wiretap in *Katz v. U.S.*, 389 U.S. 347, 88 S.Ct. 507 (1967) were incriminating did not affect the Supreme Court's upholding of Katz's Fourth Amendment privacy rights in those conversations. In *Payton v. New York*, 445 U.S. 573, 100 S.Ct. 1371 (1980), the Supreme Court reiterated this principle in upholding the defendant's privacy rights in his home even though the home was being used to harbor a fugitive. In doing so, 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 State's Brief contains absolutely no authoritative precedent for its theory that the existence of putative illegal content in a private upload of data from a customer's cellphone on an internet service provider's (ISP) platform voids that person's Fourth Amendment privacy rights in that data vis-à-vis the government.

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 Electronic Media.

The Snap, Inc. contractual documents are its: (a) "Terms of Service" [R-41, pp. 1-16; A. App. pp. 17-32]; (b) "Community Guidelines" [R-42, pp. 1-6; A. App. pp. 33-38]; and (c) "Sexual Content Community Guidelines Explainer Series" [R-

44, pp. 1-4; A. App. pp. 39-42]. These documents tell customers not to use Snapchat's platform to disseminate child pornography. Snap, Inc. warns its customers that it can monitor the data passing through its portals, which it apparently does via an internally programmed algorithm hash technology. Snap, Inc. also notifies its customers that it can report to law enforcement negatively flagged customer data which Snap, Inc. believes may violate its "Terms of Service" and/or "Community Guidelines". However, none of the Snap, Inc. contractual documents inform users that the user grants governmental agencies authority in advance to open and view the customer data flagged by Snap, Inc.'s filter without government first complying with applicable Fourth Amendment legal constraints.

1. Snap, Inc.'s Contract Identifies That User Rights Are Governed By Prevailing Law In The State of California.

On this point, Snap, Inc.'s "Terms of Service" contract identifies that all legal issues arising with respect to Snap, Inc.'s conduct under its "Terms of Service" are governed by California federal and state law. Paragraph 20. of Snapchat's Terms of Service reads:

> **20. Choice of Law**
> *Except to the extent they are preempted by U.S. federal law, the laws of California, other than its conflict-of-laws principles, govern these Terms and any claims and disputes (whether contract, tort, or otherwise) arising out of or relating to these Terms or their subject matter.*

Under the Supremacy Clause of the U.S. Constitution, the decision of the U.S. Court of Appeals for the Ninth Circuit in *U.S. v. Wilson*, 13 F.4th 961 (9th Cir. 2021) is therefore the controlling authority for all legal issues relating to contractual provisions governing the forwarding of customer account data to law enforcement agencies by Snap, Inc.

2. The Governing Law In California On The Issue Of Fourth Amendment Privacy Rights Of Cellphone Users Is *U.S. v. Wilson*, 13 F.4th 961 (9th Cir. 2021).

The State refuses to accept as controlling precedent on this constitutional issue the decision of the U.S. Court of Appeals for the Ninth Circuit in *U.S. v. Wilson*, 13 F. 4th 961 (9th Cir. 2021). Snap, Inc. is based in Anaheim, California, and *U.S. v. Wilson* originated in the U.S. District Court for the Southern District of California. The U.S. Court of Appeals for the 9th Circuit is located in Santa Monica, California. Accordingly, Snap, Inc. customers are entitled to rely upon the U.S. Court of Appeals for the 9th Circuit Fourth Amendment decisions governing law enforcement rights and duties relating to accessing Snap, Inc. customer data pursuant to controlling federal constitutional decisional law prevailing in the State of California according to Snap, Inc.'s contractual documents with its customers.

Notably, in *Wilson*, a law enforcement agent followed the exact same procedure as was followed in the present case. A CyberTip was generated by Snapchat's algorithm based scanning system. It was not viewed by any human being until opened by law enforcement officials without a warrant. The U.S. Court of Appeals for the 9th Circuit reversed Wilson's conviction in the California state court system, and rejected all of the arguments that the State now makes here in this case relative to the third party "private search" doctrine. The Court of Appeals in *Wilson, supra,* rejected the government's theory that visual inspection by law enforcement of previously unopened CyberTip content does not constitute an expansion of the Artificial Intelligence (AI) review of a customer's previously unopened data by an ISP such as Snapchat.

II. The March 3, 2023 Warrantless Viewing By Detective Schroeder 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 Artificial Intelligence (AI) Data Scan Contained In The CyberTip From NCMEC.

The State completely avoids addressing Department of Justice bureaucrat Lochowitz's warrantless viewing of the Snapchat CyberTip. The State's Brief argues only that Detective Schroeder's visual review of the video imaging contained in the Snapchat CyberTip did not require a warrant based upon the "Third Party Private Search" exception to the Fourth Amendment. The State's position is that the algorithm AI computer scan by Snapchat, Inc.'s scanning technology was not expanded by Detective Schroeder's in-person opening and review of it. This position is expressly rejected by the U.S. Court of Appeals for the 9th Circuit in *U.S. v. Wilson*, 13 F.4th 961 (9th Cir. 2021).

The decision of the 9th Circuit in *Wilson* followed the Supreme Court's decisions in *Riley* and *Carpenter* in deciding that a law enforcement warrantless human review of a previously unopened CyberTip file of AI computer scanned "suspected child pornography" is a significant expansion of a computer generated data search conducted by a private third party.

Because the subject CyberTip originated from Snap, Inc.'s database in California, the applicable law on whether the CyberTip constituted a "search," and whether law enforcement visual review of Snap, Inc.'s computerized hash matching technology is a significant expansion of a computer based private third party search, and is therefore governed by *U.S. v. Wilson*.

As pointed out by the 9th Circuit opinion in *Wilson*:

> All Google communicated to NCMEC in its CyberTip was that the four images Wilson uploaded to his email account matched images previously identified by some Google employee at some time in the past as child pornography and classified as depicting a sex act involving a prepubescent minor (the "AI" classification).
>
> * * * * * * * * * * *
>
> Based only on the barebones CyberTip, Agent Thompson testified, he opened and reviewed each of Wilson's images to determine "whether or not it is a case that . . . can be investigated" for violations of federal law.
>
> A detailed description of the images was then included in the applications for search warrants. The gulf between what Agent Thompson knew about Wilson's images from the CyberTip and what he subsequently learned is apparent from those descriptions.
>
> *U.S. v. Wilson*, *supra*, 13 F.4th at 972.

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. Accordingly, the State's citation to *U.S. v. Bebris*, 4 F.4th 551 (7th Cir. 2021) and *U.S. v. Ringland*, 966 F.3d 731 (8th Cir. 2020) have no application here.

The State recites the holdings by the Supreme Court in *Walter v. U.S.*, 447 U.S. 649 (1980); *U.S. v. Jacobsen*, 466 U.S. 109 (1984) and *State v. Payano-Roman*, 290 Wis.2d 380, 714 N.W.2d 548 (2006). These cases 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 a prior third party private search, the government may be justified in conducting a warrantless search, but only when it does not exceed the private party's antecedent search.

The legal analysis of this precept is exhaustively explained by then Circuit Judge Neil Gorsuch, in *United States v. Ackerman,* 831 F.3d 1292 at pp. 1295-1304 (10th 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 ISP reported CyberTip from the Fourth Amendment warrant requirements, citing *United States v. Warshak,* 631 F.3d 266, 283-288 (6th Cir. 2010). *Ackerman*, also explains that the "private search doctrine" does not apply to NCMEC activity which goes beyond the initial bare reporting function of the Internet Service Provider (ISP), here "Snapchat." *(Ackerman, supra,* at pp. 1305-1308).

In this case, 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 16 second video. [R-60, pp. 151-152; Supp. App. pp. 154-155.]

It was based upon his observations from his warrantless search of a CyberTip that Detective Schroeder, on March 20, 2023, sought and obtained a search warrant of Gasper's home [R-60, p. 101; Supp. App. p. 129], seized his cellphone, and arrested Gasper. During the subsequent in-custody interrogation of Gasper, he downloaded data from Gasper's Snapchat account which was then used to draft all of the charges against Gasper in this case. Notably, Detective Schroeder testified

that every charge against Gasper was from use of Gasper's cellphone. [R-60, p. 96; Supp. App. p. 124.]

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; Supp. App. pp. 30-37.] 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; Supp. App. pp. 128-129.] None of the paragraphs in Detective Schroeder's lengthy affidavit (misnomered "search warrant") 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, 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 describing the image subject derived by Detective Schroeder from his physical 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 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. 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 not brought to this Court's attention in this Brief 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 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 the preliminary stage of investigating a child pornography case when law enforcement seeks to open and view "suspected" child pornography images which have been technologically extracted by an ISP from a person's private cellphone account, and which have not been previously opened, that law enforcement needs to obtain a search warrant.

The parties do not dispute that Snap, Inc. is not a government agent and do not assign governmental status to NCMEC, neither of whom viewed Gasper's uploaded video media data. The key question presented, therefore, is whether Detective Schroeder's opening, viewing, and judgmental assessment of the content of the CyberTip without first obtaining a warrant expanded the scope of Snapchat's computerized algorithmic scan. Detective Schroeder's physical visual review clearly did expand the scope of Snapchat's Artificial Intelligence (AI) 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. 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 Gasper's CyberTip By The Wisconsin Department Of Justice And The Waukesha County Sheriff's Department Detective Violated The Fourth Amendment.

In 2018 the Supreme Court issued its opinion in *Carpenter v. U.S.*, 585 U.S. ___, 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 *Carpenter*, the government did not obtain a warrant supported by probable cause, but acquired the defendant's cellphone records via a court order issued under the federal "Stored Communication Act." [18 U.S.C. §2703]. That statute facially allows a court order to compel a communication company to produce customer cellphone data to the government upon merely a showing of "reasonable grounds" to believe that the stored data is "relevant and material to an ongoing investigation." That standard is virtually the same as the "administrative subpoena" standard and the warrant for records (WFR) used by the State in this case per Wis. Stat. §165.05. [R-39, pp. 1-3; Supp. App. pp. 38-40.]

The Supreme Court in *Carpenter* explained that such procedure is unconstitutional as follows:

> Under the standard in the Stored Communications Act, however, law enforcement need only show that the cell-site evidence might be pertinent to an ongoing investigation—a "gigantic" departure from the probable cause rule, as the Government explained below. App. 34. **Consequently, an order issued under Section 2703(d) of the Act is not a permissible mechanism for accessing historical cell-site records. Before compelling a wireless carrier to turn over a subscriber's CSLI, the Government's obligation is a familiar one—get a warrant**. (emphasis added.)
>
> *Carpenter v. U.S.*, *supra,* 585 U.S. ___, 138 S.Ct. at 2221.

> Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection. The Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment.
>
> *Carpenter v. U.S.*, *supra,* 585 U.S. ___, 138 S.Ct. at 2220.

The State here also cites *U.S. v. Reddick,* 900 F.3d 636 (5th Cir. 2018) in support of its position, and a U.S. District Court case out of New Mexico. U.S.

District Court decisions, however, do not constitute binding precedent even in the same district. [*Camreta v. Greene*, 563 U.S. 692, 131 S.Ct. 220 at Footnote 7 (2011) citing 18 J. Moore et al., Moore's Federal Practice § 134.02[1] [d], p. 134–26 (3d ed.2011).]

The 5th Circuit's 2018 opinion in *Reddick* was not a cellphone case and did not have the benefit of the virtually contemporaneous 2018 U.S. Supreme Court decision in *Carpenter*. However, the *Reddick* court, unlike the circuit court here, was presented with unopposed unchallenged assertions that the evidentiary value of the technical scan of the defendants' computer files using Microsoft's proprietary PhotoDNA program could not be improved upon by, and was therefore not "expanded" by, human viewing of "suspected child pornography". Any precedent value in *Reddick* to this case, however, is voided due to the lack of an evidentiary foundation in this present case that PhotoDNA was used. In addition, its utility as precedent is also superseded by the Supreme Court's warrant requirement in *Riley* in cellphone cases. While the 2018 decision in *Reddick* appears facially to conflict with the later 9th Circuit 2021 decision in *Wilson*, the *Wilson* court had the benefit of the Supreme Court's controlling decision in *Carpenter*, and the *Reddick* court did not.

The State also cites *U.S. v. Miller*, 982 F.3d 412 (6th Cir. 2020) which has no application here because the *Miller* court did not adopt the State's third party search theory presented here. Instead, the Court of Appeals in *Miller* ignored the District Court's reliance upon computer hash search alleged infallibility, and hinged denial of the defendant's motion to suppress on waiver by the defendant in failing to join issue with the limitations of the ISP's hash-value computer technology. Here, the circuit court's decision does exactly that in calling out the lack of reliability set forth within the published literature provided to the court by the State about the MD5 hashing program and the lack of foundation as to the content of the database which

the CyberTip image was being compared. [R-60, pp. 62-66; Supp. App. pp. 117-121.]

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).

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; Supp. App. pp. 707-72.] 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; Supp. App. pp. 95-99.]

Accordingly, a CyberTip of "suspected" child pornography is not sufficient to provide "probable cause" for a search warrant to issue. It is the need to obtain "probable cause" that requires law enforcement to obtain a warrant to physically view reported cellphone data which has triggered an ISP third party private algorithm CyberTip notification to NCMEC. Here, warrantless analysis of the subject CyberTip content by Department of Justice bureaucrat Lochowitz and

Deputy Schroeder resulted in governmental expansion of Snap, Inc.'s internal algorithm based customer cellphone uploaded data review. These governmental acts thereby void any application of the "private search" exception to the warrant requirement of the Fourth Amendment.

The Supreme Court is exquisitely clear in its admonition that a warrant should be applied for before law enforcement agents open and view computer generated "suspected" child 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 avoid and substitute itself for the "detached and neutral magistrate" required by the Fourth Amendment. This is the most basic fatal flaw in the State's position.

After-the-fact protestations of infallibility of artificial intelligence (AI) systems and Snap, Inc.'s hashing technology is pressed on this Court in the State's Brief, but it is too little too late. All of that information should have been presented in support of issuing a search warrant before Department of Justice bureaucrat Lochowitz and Detective Schroeder unilaterally opened and viewed the CyberTip content. That is the kind of information that also should have been provided to the judicial officer when Detective Schroeder was planning to apply for a search warrant of the defendant's home and electronic devices.

Notably, the State's Brief concedes 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 ISP's database content, select and program the computer hash technology, apply it and transmit its resulting identification of "suspected child pornography" via

CyberTips to governmental agencies. The State urges this Court to sanction that process without any foundation about how such databases were compiled and what their content consists of. Focusing on the technical capacity of a search engine is meaningless if the database it is searching is infected or not purposely vetted to retain only reliable source material.

The State's theory espoused here was the same theory urged by the government in *Riley*, *infra*, and, 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, 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.

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.

Fundamental policy decisions in *Riley* and *Carpenter* requiring a warrant to search cellphone data were intentionally announced by the U.S. Supreme Court to restrict governmental authority with respect to examining cellphone content without a warrant.

These crystal clear decisions evidence the Court's deep concern that "administrative subpoenas", based on "reasonable belief" of law enforcement officers; and the allowance of warrantless searches by law enforcement officers of cellphone data obtained solely from remote servers scanned by private party computer AI programs are constitutionally unacceptable under the Fourth Amendment. The Supreme Court explicitly harkened back to the invasive power asserted by the British Crown at the time of the American Revolution. 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, 1345 S.Ct. at 2495.

The State utterly fails to provide any explanation for the Department of Justice deliberately adopting a system which requires its agent, Matthew Lochowitz, and 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*; and which was 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 In This Case To A Systemically Flawed Investigative System.

The Wisconsin Attorney General has adopted and teaches law enforcement personnel to open and physically view all CyberTip data received from NCMEC without a warrant. 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 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; Supp. App. pp. 154-158.]

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. That public policy decision weighs the "cost to society" of implementing the exclusionary rule in warrantless cellphone

search cases. That policy decision with respect to cellphone privacy is unmistakably set forth in the quotes from *Riley, supra,* and *Carpenter, supra,* found on pages 34 and 40 of this Respondent's Brief: "Get A Warrant."

The warrantless CyberTip data review procedure followed by Detective Schroeder and Mr. Lochowitz 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 reviews 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 9th Circuit in *U.S. v. Wilson*, 13 F.4th 961 (9th 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.

The State's citation of *State v. Burch*, 398 Wis. 1, 961 N.W.2d 314, 2021 WI 68 is fragile at best. In *Burch,* the fact of antecedent consent and the lack of any precedent to a case of "second search," were essential to the Wisconsin Supreme Court garnering a majority decision to deny application of the exclusionary rule in *State v. Burch*, 398 Wis. 1, 961 N.W.2d 314, 2021 WI 68. The unmistakable U.S. Supreme Court policy decisions announced in *Carpenter* and *Riley* to the warrantless search of a cellphone case, render *Burch* completely inapplicable to apply a "good faith" exception in this case.

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).

This is a cellphone case, not a vehicle search. There was no mistaken or defective warrant issued here. There was no error by officers in executing an overly broad warrant or arrest pursuant to a statute subsequently found to be constitutionally void. This case originates from a warrantless cellphone search by law enforcement personnel following a state-wide constitutionally defective system deliberately and knowingly created by the Wisconsin Attorney General. 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 arrogates 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 AI review 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,* identified in the State's Brief on page 41 have no application here because, at the direction of the Attorney General, there are no warrants. Furthermore, if the law with respect to warrantless searches of cellphone data is "unsettled" as maintained by the State's Brief at p. 42, the mandate from the United States Supreme Court is nevertheless 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 not "good faith."

CONCLUSION

Whether under the historical "trespass to chattels" theory espoused by then Circuit Judge Gorsuch in *Ackerman, supra*; or the present day "reasonable expectation of privacy" public policy directive to "get a warrant" by the Supreme Court in both *Carpenter* and *Riley*; or the "expansion of scope" of privately AI filtered metadata by warrantless governmental review; the exclusionary rule requires suppression of evidence obtained as a result of warrantless opening and viewing of cellphone based CyberTip data.

Accordingly, for all of the reasons set forth more particularly in this Respondent's Brief, the decision and order of the circuit court granting the defendant's Motion to Suppress all evidence seized and all statements by Gasper flowing from the search conducted of Gasper's property on March 21, 2023 should be affirmed.

Respectfully submitted this 16th day of April, 2024.

Attorneys for Defendant-Respondent:

Law Offices of Joseph F. Owens, LLC
Electronically Signed By

Joseph F. Owens
Joseph F. Owens
State Bar No. 1016240

Electronically Signed By

Debra K. Riedel
Debra K. Riedel
State Bar No. 1002458

CERTIFICATION AS TO FORM AND LENGTH OF APPELLATE BRIEFS

I hereby certify that this Brief conforms to the rules contained in Wis. Stat. Section 809.19(8)(b) (bm), and (c) for a Brief. The length of this brief is 10,466 words.

Dated at New Berlin, Wisconsin on April 16, 2024.

Electronically Signed By

Joseph F. Owens
Attorney Joseph F. Owens
State Bar No: 1016240

APPELLANT'S BRIEF APPENDIX CERTIFICATION

I hereby certify that filed with this Brief 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;

(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 April 16, 2024.

Electronically Signed By

Joseph F. Owens
Attorney Joseph F. Owens
State Bar No: 1016240