

No. 25-

---

---

IN THE  
**Supreme Court of the United States**

---

MICHAEL JOSEPH GASPER,

*Petitioner,*

*v.*

STATE OF WISCONSIN,

*Respondent.*

---

ON PETITION FOR A WRIT OF CERTIORARI  
TO THE SUPREME COURT OF WISCONSIN

---

---

**PETITION FOR A WRIT OF CERTIORARI**

---

---

DEBRA K. RIEDEL  
LAW OFFICES OF  
DEBRA K. RIEDEL  
2665 South Moorland Road,  
Suite 200  
New Berlin, WI 53151  
(414) 277-7818  
riedellaw@dkriedellaw.com

JOSEPH F. OWENS  
*Counsel of Record*  
LAW OFFICES OF  
JOSEPH F. OWENS, LLC  
2665 South Moorland Road,  
Suite 200  
New Berlin, WI 53151  
(262) 785-0320  
owenslaw2@gmail.com

*Counsel for Petitioner*

---

---

120998



COUNSEL PRESS  
(800) 274-3321 • (800) 359-6859

## **QUESTIONS PRESENTED**

This is a Fourth Amendment warrantless search case arising in the context of private cellphone cyberdata.

Question 1. Whether a person is entitled to a constitutionally protected “reasonable expectation of privacy” in data uploaded from their privacy protected cellphone to their remote private Electronic Service Provider (ESP) account (i.e., “the Cloud”).

Question 2. Whether warrantless viewing by law enforcement of a previously unviewed virtual computer scan “CyberTip” provided to the National Center for Missing and Exploited Children (NCMEC) by a commercial ESP violates the Fourth Amendment and does not fall within the “Private Search” exception to the Fourth Amendment.

Question 3. Whether the “Good Faith Exception” to the exclusionary rule applies to obviate an otherwise unconstitutional violation of the Fourth Amendment warrant requirement by law enforcement’s warrantless viewing of a person’s privacy protected cyberdata uploaded from their cellphone to their remote ESP account.

**PARTIES TO THE PROCEEDING**

Petitioner, Michael Joseph Gasper, was the Defendant-Respondent below and is a natural born American citizen and resident of the Village of Dousman, Waukesha County, State of Wisconsin.

Respondent, State of Wisconsin, was the Plaintiff-Appellant below.

## RELATED CASES

- *State of Wisconsin v. Michael Joseph Gasper*, Case No. 2023-CF-000470, Waukesha County Circuit Court, State of Wisconsin. [Unpublished Decision and Order entered: October 30, 2023].
- *State of Wisconsin v. Michael Joseph Gasper*, [reported at 2024 WI App. 72, 414 Wis.2d 532, 16 N.W.3d 279, vacated and affirmed on other grounds] Wisconsin Court of Appeals. [Reversed and cause remanded: October 30, 2024].
- *State of Wisconsin v. Michael Joseph Gasper*, Wisconsin Supreme Court Vacated Court of Appeals reasoning and affirmed on other grounds. [Filed January 14, 2026, reported at 2026 WI 3, 419 Wis.2d 12, 30 N.W.3d 367].

**TABLE OF CONTENTS**

	<i>Page</i>
QUESTIONS PRESENTED .....	i
PARTIES TO THE PROCEEDING .....	ii
RELATED CASES .....	iii
TABLE OF CONTENTS.....	iv
TABLE OF APPENDICES .....	vii
TABLE OF CITED AUTHORITIES .....	viii
OPINIONS BELOW.....	1
JURISDICTIONAL STATEMENT .....	1
CONSTITUTIONAL AND STATUTORY PROVISIONS.....	1
STATEMENT OF THE CASE .....	4
REASONS FOR GRANTING THE PETITION.....	8
I. Gasper Was Entitled To A “Reasonable Expectation of Privacy” In Data Uploaded To His Snapchat Account From His Cellphone .....	10
A. Cellphone Content Is Categorically Granted A Reasonable Expectation Of Privacy .....	10

*Table of Contents*

	<i>Page</i>
B. Potential Criminal Content Of A Person’s Cellphone And ESP Account Do Not Void The Fourth Amendment’s Warrant Requirement .....	13
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.....	18
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.....	21
A. Law Enforcement Opening And The 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 .....	21
B. The Warrantless Opening And Viewing Of Gasper’s CyberTip By The Wisconsin Department Of Justice And The Waukesha County Sheriff’s Department Violated The Fourth Amendment .....	24

*Table of Contents*

	<i>Page</i>
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.....	28
CONCLUSION .....	32

**TABLE OF APPENDICES**

	<i>Page</i>
APPENDIX A — WISCONSIN SUPREME COURT DECISION, JANUARY 14, 2026 . . . . .	1a
APPENDIX B — OPINION OF THE COURT OF APPEALS FOR THE STATE OF WISCONSIN, DISTRICT II, FILED OCTOBER 30, 2024. . . . .	90a
APPENDIX C — OPINION OF THE CIRCUIT COURT FOR THE STATE OF WISCONSIN, WAUKESHA COUNTY, FILED OCTOBER 30, 2023. . . . .	106a
APPENDIX D — ORDER OF THE CIRCUIT COURT FOR THE STATE OF WISCONSIN, WAUKESHA COUNTY, FILED FEBRUARY 16, 2024 . . . . .	118a
APPENDIX E — DEFENDANT’S MOTION TO SUPPRESS EVIDENCE AND DERIVATIVE FRUITS OF SEARCH OF PREMISES AND ELECTRONIC DEVICES DATED MAY 10, 2023. . . . .	119a

## TABLE OF CITED AUTHORITIES

	<i>Page</i>
<b>CASES:</b>	
<i>Brady v. United States</i> , 397 U.S. 742, 90 S. Ct. 1463 (1970) . . . . .	20
<i>Brinegar v. United States</i> , 338 U.S. 160, 69 S. Ct. 1302 (1949) . . . . .	25
<i>Bumper v. North Carolina</i> , 391 U.S. 543, 885 S. Ct. 1788 (1968) . . . . .	10
<i>Byars v. United States</i> , 273 U.S. 28, 47 S. Ct. 248 (1927) . . . . .	14
<i>Byrd v. United States</i> , 584 U.S. 395, 138 S. Ct. 1518 (2018) . . . . .	16
<i>Carpenter v. United States</i> , 585 U.S. 296, 138 S. Ct. 2206 (2018) . . . . .	9-11, 15, 16, 24, 27-29, 31
<i>Davis v. United States</i> , 564 U.S. 229, 131 S. Ct. 2419 (2011) . . . . .	29, 30
<i>Gideon v. Wainright</i> , 372 U.S. 335, 83 S. Ct. 792 (1963) . . . . .	20
<i>Herring v. United States</i> , 555 U.S. 135, 129 S. Ct. 694 (2009) . . . . .	30
<i>Johnson v. Zerbst</i> , 304 U.S. 458, 58 S. Ct. 1019 (1938) . . . . .	20

*Cited Authorities*

	<i>Page</i>
<i>Katz v. United States</i> , 389 U.S. 347, 88 S. Ct. 507 (1967).....	14-16
<i>Minnesota v. Olson</i> , 495 U.S. 91, 110 S. Ct. 1684 (1990) .....	17
<i>Patton v. United States</i> , 281 U.S. 276, 50 S. Ct. 253 (1930).....	20
<i>Payton v. New York</i> , 445 U.S. 573, 100 S. Ct. 1371 (1980).....	13
<i>Riley v. California</i> , 573 U.S. 373, 134 S. Ct. 2473 (2014) .....	9-11, 17, 24, 26-29, 31
<i>Schneckloth v. Bustamonte</i> , 412 U.S. 218 (1973).....	13
<i>Smith v. Maryland</i> , 442 U.S. 735, 99 S. Ct. 2577 (1979).....	15, 16
<i>State v. Denk</i> , 315 Wis.2d 5, 758 N.W.2d 775, 2008 WI 130 .....	13
<i>State v. Eason</i> , 245 Wis.2d 206, 629 N.W.2d 625, 2001 WI 98. ....	31
<i>State v. Payano-Roman</i> , 290 Wis.2d 380, 714 N.W.2d 548 (2006).....	14

*Cited Authorities*

	<i>Page</i>
<i>Stoner v. California</i> , 376 U.S. 483, 84 S. Ct. 889 (1964) . . . . .	17
<i>United States v. Ackerman</i> , 831 F.3d 1292 (10th Cir. 2016) . . . . .	21
<i>United States v. Peter Braun</i> , Case No. 24-CR-164, E.D.Wis. (App. No. 25-2740, 7th Cir.) . . . . .	9
<i>United States v. Holmes</i> , 121 F.4th 727 (9th Cir. 2024) . . . . .	9, 29, 30
<i>United States v. Jacobsen</i> , 466 U.S. 109, 104 S. Ct. 1652 (1984) . . . . .	14, 15
<i>United States v. Leon</i> , 468 U.S. 897 (1984) . . . . .	31
<i>United States v. Maher</i> , 120 F.4th 297 (2nd Cir. 2024) . . . . .	9, 20
<i>United States v. Matlock</i> , 415 U.S. 164, 94 S. Ct. 988 (1974) . . . . .	16
<i>United States v. Miller</i> , 425 U.S. 435, 96 S. Ct. 1619 (1976) . . . . .	15, 16
<i>United States v. Miller</i> , 982 F.3d 412 (6th Cir. 2020) . . . . .	9

*Cited Authorities*

	<i>Page</i>
<i>United States v. Nafziger</i> , 965 F.2d 213 (7th Cir. 1992).....	10
<i>United States v. Reddick</i> , 900 F.3d 636 (5th Cir. 2018) .....	9
<i>United States v. Sheehan</i> , 70 F.4th 36 (1st Cir. 2023) .....	30
<i>United States v. Thomas</i> , 65 F. 4th 922 (7th Cir. 2023) .....	17
<i>United States v. Warshak</i> , 631 F.3d 266 (6th Cir. 2010).....	21
<i>United States v. Wilson</i> , 13 F.4th 961 (9th Cir. 2021) .....	9, 25, 28, 30
<i>Walter v. United States</i> , 447 U.S. 649, 100 S. Ct. 1652 (1980) .....	14, 15
<i>Williams v. Kaiser</i> , 323 U.S. 471, 65 S. Ct. 363 (1945).....	20
<b>CONSTITUTIONAL PROVISIONS:</b>	
U.S. Const. amend. IV .....	1, 7-9, 11-14, 17, 18, 21, 24, 26-29
U.S. Const. amend. XIV .....	1, 2, 7

*Cited Authorities*

*Page*

**STATUTES:**

18 U.S.C. §2258A.....	9
28 U.S.C. §1257(a) .....	1
28 U.S.C. §2104 .....	1
28 U.S.C. §2106 .....	1
Wis. Stat. §165.505 .....	2
Wis. Stat. §165.505(2) .....	5

**OTHER AUTHORITIES:**

Official Website of the United States Department of Justice, Office of Justice Programs, “CyberTipline: Your Resource for Reporting the Sexual Exploitation of Children”.....	25
--	----

## OPINIONS BELOW

The opinion of the Wisconsin Supreme Court (Pet. App. pp. 1a-89a) issued on January 14, 2026, is reported at 2026 WI 3, 419 Wis.2d 12, 30 N.W.3d 367. The Wisconsin Court of Appeals opinion (Pet. App. pp. 90a-105a) issued on October 30, 2024, is reported at 2024 WI App 72, 414 Wis.2d 532, 16 N.W.3d 279 [vacated and affirmed on other grounds in Wis. S. Ct. *State v. Gasper* opinion *supra* at footnote 6]. The Circuit Court of Waukesha County, Wisconsin Case No. 23CF470 (Pet. App. pp. 106a-117a) Decision and Order Granting the Defendant's Motion to Suppress is unpublished.

## JURISDICTIONAL STATEMENT

This Court's jurisdiction is invoked pursuant to 28 U.S.C. §1257(a); 28 U.S.C. §2104 and 28 U.S.C. §2106. This case arises from a final Decision and Order rendered by the Supreme Court of the State of Wisconsin on January 14, 2026, which Decision infringed fundamental rights provided by the Fourth and Fourteenth Amendments to the Constitution of the United States relating to the defendant, Michael J. Gasper.

## CONSTITUTIONAL AND STATUTORY PROVISIONS

The Constitution of the United States provides in pertinent part 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.

**Section 1, Amendment XIV**

No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

The Statutes of the State of Wisconsin provide in pertinent part as follows:

**§165.505 Internet crimes against children and human trafficking; administrative subpoena.**

(1) . . . . .

(2)(am) The attorney general or his or her designee may issue and cause to be served a subpoena, in substantially the form authorized under s. 885.02, upon a provider of an electronic communication service or a remote computing service to compel the production of any of the items listed in par. (c) if all of the following apply:

1. The information likely to be obtained is relevant to an ongoing investigation of a human trafficking crime or an Internet crime against a child.

2. The attorney general or his or her designee has reasonable cause to believe that an Internet or electronic service account provided by an electronic communication service or a remote computing service has been used in the crime.

**(bm)** The attorney general or his or her designee issuing a subpoena under par. *(am)* shall ensure that the subpoena describes each record or other information pertaining to a customer or subscriber of the service to be produced and prescribes a reasonable return date by which the person served with the subpoena must assemble each record or other information and make them available.

**(c)** A person who is duly served a subpoena issued under par. *(am)* shall, if requested, provide the following information about the customer or subscriber:

1. Name.
2. Address.
3. Duration, including the start date and end date, of the assignment of any Internet protocol address to the customer or subscriber.

(d) A person served with a subpoena under par. (am) may, before the return date indicated under par. (bm), petition a circuit court in the county where the subpoena was issued for an order to modify or quash the subpoena or to prohibit disclosure of information by the court.

### STATEMENT OF THE CASE

On January 13, 2023, the defendant, Michael Joseph Gasper, uploaded video cyberdata from his cellphone to his private account at Snapchat. A CyberTip was generated exclusively by computer scan of the video imagery without any human viewing by Snapchat, and forwarded to the National Center for Missing and Exploited Children (NCMEC) as Suspected Child Sexual Abuse Material (SCSAM). CyberTip #152547912 described the upload of a 16-second video on January 13, 2023 by a Snapchat username “mike\_g6656,” with an IP address of 184.100.214.42, linked to the defendant, Michael Gasper’s name and address.

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 was opened and physically viewed without a warrant by a Wisconsin Department of Justice administrative bureaucrat (in this case one Matthew Lochowitz). In conformity with the Wisconsin Attorney General’s implementation of the national protocol, Mr. Lochowitz then sent an “Administrative Subpoena” to Century Link to obtain the individual subscriber name and geographic address associated with the IP Address.

This constitutionally suspect “Administrative Subpoena” was issued pursuant to Wis. Stat. §165.505(2) without “probable cause” and is issued by a non-judicial officer on “reasonable cause to believe.”

After opening and viewing the imagery contained in the CyberTip without a warrant, the Wisconsin 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.

On March 20, 2023, Waukesha County Circuit Court Judge Paul Bugenhagen issued a Search Warrant of the defendant, Michael J. Gasper, and his residence to seize all electronic devices, including cellphones. The Search Warrant was predicated 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”) based upon assertions by Detective Schroeder stating he had opened and viewed a video contained in a Snapchat CyberTip report of “apparent child pornography” from the National Center for Missing and Exploited Children (NCMEC) via CyberTip #152547912. In doing so, Detective Schroeder physically viewed the CyberTip video flagged by Snapchat’s “hash” coded program on his computer without a warrant, which he described contained imagery depicting sexual intercourse between an anonymous adult male and an anonymous female he perceived to be a prepubescent light skinned female of an undetermined age or ethnicity.

It is uncontroverted that all of the criminal charges against Gasper arose exclusively from Gasper's privacy protected cellphone, as was his Snapchat account.

On March 22, 2023, the Waukesha County District Attorney's Office filed the Criminal Complaint in this matter based on the information initially obtained by the Wisconsin Department of Justice's warrantless opening and viewing of the previously unviewed content of the CyberTip from the National Center for Missing and Exploited Children (NCMEC); 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, and then the entire content of Gasper's cell phone.

On May 10, 2023, Gasper filed a Motion to Suppress Evidence and Derivative Fruits of Search of Premises and Electronic Devices pursuant to the Fourth and Fourteenth Amendments to the United States Constitution prohibiting unreasonable searches and seizures.

On May 11, 2023, Gasper filed a separate Motion to Suppress Statements and Fruits of Illegal Arrest pursuant to the Fourth and Fourteenth Amendments to the United States Constitution prohibiting illegal arrests and unreasonable searches and seizures incident thereto.

On October 2, 2023, the circuit court conducted a full-blown evidentiary hearing on both Motions to Suppress.

On October 30, 2023, the circuit court issued a written Decision and Order granting Gasper's Motions to Suppress all of the State's evidence pursuant to the

Fourth and Fourteenth Amendments to the United States Constitution. (Pet. App. pp. 106a-118a)

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.

On February 16, 2024, the circuit court entered a formal Order granting Gasper's Motions to Suppress, and denominated it a final order for purposes of appeal.

On October 30, 2024, the Wisconsin Court of Appeals, District II, issued its Decision in this case reversing the circuit court orders which had granted Gasper's Motions to Suppress. (Pet. App. pp. 90a-105a)

On November 26, 2024, the defendant, Michael J. Gasper, filed a Petition for Review in the Wisconsin Supreme Court alleging violation of his Fourth and Fourteenth Amendment constitutional rights against unreasonable search and seizures.

On March 13, 2025, the Wisconsin Supreme Court granted Gasper's Petition for Review.

On January 14, 2026, the Wisconsin Supreme Court issued a 58-page Opinion vacating the Court of Appeals' rationale and expressly voiding any precedential value to the Court of Appeals' Opinion, but affirmed reversal of the trial court's Decision and Order granting the Motion to Suppress on other grounds, relying principally on the "private search" exception to the Fourth Amendment prohibition against unreasonable searches and seizures. (Pet. App. pp. 1a-89a)

At every stage of this criminal case the fundamental constitutional issue of what constitutes a warrantless unreasonable search and seizure of a person's cyberdata originating from their cellphone was raised, preserved, and passed on by the respective courts below. All of the lower court opinion passages reflective thereof are contained in the Appendix and are too voluminous to iterate specifically in this part of the Petition for Certiorari.

### **REASONS FOR GRANTING THE PETITION**

The rules determining what privately stored information is "contraband" one day can morph overnight into other forms of "contraband" simply by legislative fiat (i.e., material sympathetic to the Communist Party during the 1950s; information relating to intoxicating liquor during the Prohibition Era of the 1920s; and in today's volatile political environment, legislatively outlawed information and communications relating to obtaining women's health and pregnancy services).

The Decision of the Wisconsin Supreme Court here petitioned from vitiates the Fourth Amendment rights of all members of the public who upload data from their cellphones to remote "cloud" storage accounts maintained by an Electronic Service Provider (ESP).

Operating under a national internet investigative protocol, Wisconsin Department of Justice 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).

Under this process, when proprietary software employed by an Electronic Service Provider (ESP), such as Snapchat, Facebook, Google, or Instagram, detects contraband in the form of Suspected Child Sexually Abusive material (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. This process, which is implemented in numerous states, has generated an explosion of Fourth Amendment constitutional litigation.

This process facially violates the Fourth Amendment when applied to cellphone use and related ESP internet data storage accounts per language in 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). This analysis is followed by two U.S. Court of Appeals Circuits in *U.S. v. Wilson*, 13 F.4th 961 (9th Cir. 2021); *U.S. v. Maher*, 120 F.4th 297 (2nd Cir. 2024); and *U.S. v. Holmes*, 121 F.4th 727 (9th Cir. 2024). It is not followed in two U.S. Court of Appeals Circuits, *Reddick*, 900 F.3d 636 (5th Cir. 2018) and *Miller*, 982 F.3d 412 (6th Cir. 2020). In addition, in *Peter J. Braun* (Case No. 24-CR-164, E.D. Wis.), United States District Judge Lynn Adelman issued a 19-page decision on September 3, 2025, which follows the holdings in the Second and Ninth Circuits suppressing warrantless seizure of cyberdata evidence of child pornography, which U.S. District Court decision is in direct conflict with the subsequently issued Opinion of the Wisconsin Supreme Court as to which this Petition for Certiorari is directed. *Braun* is now pending on appeal by the U.S. Attorney General’s Office in the U.S. Court of Appeals for the Seventh Circuit as Case No. 25-2740.

**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.**

Gasper’s case presents this Court with a classic unconstitutional warrantless search by two levels of government agencies engaging in an investigative process resulting in 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 at gunpoint. [*Bumper v. North Carolina*, 391 U.S. 543, 548, 885 S. Ct. 1788 (1968); *U.S. v. Nafzger*, 965 F.2d 213 (7<sup>th</sup> Cir. 1992).]

Notably, it is uncontroverted that all of the alleged contraband imagery in this case identified as constituting the basis for the criminal charges filed against Michael Gasper, originated solely through his cellphone. No other electronic device was involved. This fact has major significance here because the fundamental privacy rights of all persons to their cellphone content impacts the Fourth Amendment obligations imposed on law enforcement to everyone in our society.

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 a constitutionally protected expectation of privacy in the data content of their cellphones. The Supreme Court policy decisions in *Riley* and *Carpenter* do not limit their reach to the internal memory of the cellphone device itself. The language in *Riley* and *Carpenter* 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 explained 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.

Detective Schroeder's sworn affidavit requesting issuance of the search warrant of Gasper's residence confirmed that all of the Wi-Fi signals at the Gasper residence were secure and protected with a password.

The Affidavit of Michael Gasper 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 at the time of his arrest at gunpoint.

To be sure, the expectation of privacy can be lost by public sharing, private sharing, informed consent, and potentially, abandonment. However, U.S. Supreme Court precedent 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 held by their cellphones, including when it is stored remotely on an ESP server. Accordingly, "cloud" storage of his cellphone data on his Snapchat account met 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.**

When an ESP reports to the NCMEC "suspected" child pornography in a user's account, the government asserts that it 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 scan search program for a constitutionally required "probable cause" decision by a "neutral and detached" magistrate in issuing a search warrant.

In other words, simply because the content of a digital ESP upload was "suspected" illegal contraband by Snapchat's proprietary virtual data search engine, the Wisconsin Supreme Court posits that Michael Gasper lost any "reasonable expectation of privacy" in his Snapchat account. Both acts by Wisconsin law enforcement in opening and viewing the previously unopened CyberTip image data were warrantless "searches" by government agents at the state and local levels. *Schneekloth 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 in Wisconsin and many states 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.

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).

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.”

The U.S. Supreme Court in *Walter v. U.S.*, 447 U.S. 649, 100 S. Ct. 1652 (1980); *U.S. v. Jacobsen*, 466 U.S. 109, 104 S. Ct. 1652 (1984) and the Wisconsin Supreme Court in *State v. Payano-Roman*, 290 Wis.2d 380, 714 N.W.2d 548 (2006) confirm that “private searches” by third parties are an exception to the Fourth Amendment because the Fourth Amendment only applies to government action. Under this exception, when there is an antecedent “private party” search, the government may be justified in conducting

a subsequent warrantless search only when it does not exceed the scope of the private party's antecedent search. The focus of the U.S. Supreme Court in *Walter* and in *Jacobsen*, was the degree of intrusion by the government when compared to that of the private party. In *Walter*, the Court found that the government's use of an electronic movie projector to view suspected pornographic movies was an expansion of the degree of intrusion presented by naked eye view of the film strips by the private party to whom the films had been mis-delivered. In *Jacobsen*, the Court found that binary testing of a white powder that had already been spilled from a box in the hands of FedEx employees, did not increase the degree of intrusion in comparison to that of the FedEx employees.

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

Accordingly, pursuant to the Supreme Court holding in *Riley*, as a matter of law, Michael Gasper's Motion to Suppress meets the objective "reasonable expectation of privacy" threshold requirements for standing to assert Fourth Amendment violations relative to the Wisconsin Attorney General's Office and Detective Schroeder's warrantless opening and review of his cellphone data, albeit shelved in the "cloud."

**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.**

When defending a warrantless search of cellphone content on an ESP server, the Wisconsin Supreme Court 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”; (b) “Community Guidelines”; and (c) “Sexual Content Community Guidelines Explainer Series.”

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).

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).

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).

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).

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 unidentified

“. . . information relating to your account.” Both of its January 2023 “Community Guideline” documents do not have an explicit effective date in January of 2023, and given the January 13, 2023 date of Gasper’s upload of flagged data, there is an evidentiary lack of nexus between Snapchat’s undated January 2023 “Community Guidelines” and Gasper’s upload to constitute a breach of contract on his part. Importantly, none of the Snap Inc. private contractual documents state the user grants to “***governmental agencies***” any authority to open and view the customer data flagged by Snap Inc.’s data filter technology. None of these Snap Inc. documents contain provisions that constitute waiver of a fundamental constitutional right. The U.S. Supreme Court has stated over and over:

Waivers of constitutional rights not only must be voluntary but must be knowing, intelligent acts done with sufficient awareness of the relevant circumstances and likely consequences.

*Brady v. United States*, 397 U.S. 742, at 748, 90 S. Ct. 1463 (1970).

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

As explained by the U.S. Court of Appeals for the Second Circuit in Discussion Section II. A. of its opinion in *U.S. v. Maher*, 120 F.4th 297, p. 308 (2024), Google’s

contractual terms of service “did not extinguish Maher’s reasonable expectation of privacy in that content as against the government.” (emphasis added).

**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.**

**A. Law Enforcement Opening And The 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 animate person opened the Snapchat CyberTip containing Gasper’s upload of a 16-second video from his cellphone, allegedly depicting “suspected child pornography” prior to Wisconsin Department of Justice bureaucrat, Matthew Lochowitz, and Waukesha County Sheriff Department Detective Schroeder doing so. Snap Inc. personnel did not do so. Neither did personnel at the National Center for Missing and Exploited Children.

The legal import of these facts are exhaustively explained by then U.S. 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, 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 (6th 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 actual imagery related to the CyberTip alleged hash value data match originated by Snap Inc.

Notably, Detective Schroeder testified that every charge against Gasper arose from the content of Gasper's cellphone.

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. 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.

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 algorithmic

scanning program being utilized by Snapchat, NCMEC, by the Wisconsin Department of Justice, or by Detective Schroeder, himself.

In short, the issuing judicial officer of the search warrant which was issued, had no basis upon which to issue the search warrant other than the “judgment call” of Detective Schroeder following his warrantless opening and viewing of the 16-second video imagery in the CyberTip originating from the upload from Gasper’s cellphone.

That description exemplifies 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 he specifically disclaims the ability to comment on breast development because of her wearing a t-shirt. The imagery reportedly does not show any pubic hair—but that is ambiguous because shaving of the pubic area would remove any visible pubic hair.

These descriptions are brought to this Court’s attention not to cast aspersions on the accuracy of Detective Schroeder’s opinion as to the age of the subject in the video. The point is that those human observations, which arose from a warrantless search of a “suspected” child pornography “hash” data scan by a non-governmental ESP’s proprietary coded programming, formed the only factual basis provided to the issuing judicial officer 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 match technology" or the reliability of such technology. There is no consideration of the possibility of Artificial Intelligence (AI) fantasy imaging or authenticity testing. These are forensic fundamental flaws in the Department of Justice protocol at this stage of investigating a child pornography case.

Detective Schroeder's physical visual review necessarily expanded the scope of a Snapchat algorithmic "hash" scan of Gasper's uploaded media metadata, regardless of whether Schroeder's personal conclusion about the age of the subject is accurate or inaccurate. However, it illustrates that Detective Schroeder, himself, was not confident in the ability of Snapchat's coded "hash" scan alone to sufficiently assess the subject's age for him to discern the video as depicting adult pornography versus child pornography without his physically viewing the reported cyberdata imagery.

**B. The Warrantless Opening And Viewing Of Gasper'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 (ESP).

In Gasper’s case, the governmental investigative process began with Wisconsin Department of Justice receiving a CyberTip containing digital image “hash” data, extracted by Snapchat from Gasper’s “cloud” account, uploaded from his cellphone.

A CyberTip, by definition, only consists of a report of “. . . suspected incidents of child sexual exploitation that occur on the Internet.” (emphasis added). [*see*: Official Website of the United States Department of Justice, Office of Justice Programs, “CyberTipline: Your Resource for Reporting the Sexual Exploitation of Children.”]. 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).

The key word “suspected” was important to the U.S. Court of Appeals in *Wilson* and to the Waukesha County Circuit Court here because it is elemental that “. . . mere suspicion does not suffice to establish “probable cause” (emphasis added). *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 U.S. 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 CyberTip arising from algorithmic “hash” data would automatically substitute itself for the “detached and neutral magistrate” required by the Fourth Amendment.

The Wisconsin Supreme Court decision does not dispute that private internet platform companies that apply their proprietary hash scan 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 trained law enforcement officers, and certainly not a neutral and detached magistrate—who make determinations as to the ESP’s archival pornographic comparison databank content; program the hash scan technology; apply it; and transmit their search engine’s resulting identification of “suspected child pornography” via a CyberTip.

The Wisconsin Supreme Court’s theory is essentially the same theory urged by the government in *Riley, infra* (i.e. a computer data scan is the evidentiary equivalent of a magistrate). This theory 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 upon 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.

\* \* \* \* \*

**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 Wisconsin Supreme Court 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 a national template that teaches law enforcement personnel to open and physically view on their computer screens, 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 David Maas (who signed the Administrative Subpoena here 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.

This conduct represents knowing and deliberate implementation by the Wisconsin Attorney General of a departmental enforcement 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 U.S. Court of Appeals in *U.S. v. Holmes*, 121 F.4th 727 (9th Cir. 2024) engaged in an extensive analysis of the law supporting application of the “good faith” exception to the exclusionary rule for governmental violation of the Fourth Amendment warrant requirement for conduct identical to that existing here.

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

When law enforcement asserts that it acted in good faith by relying on then-existing law, it must point to “binding appellate precedent” that authorizes the challenged conduct at issue.

[*Davis, supra*, at 564 U.S. at 241.]

The *Holmes* court continues to explain: “*Good faith is not established where existing precedent is unclear or makes the government’s position only “plausibly permissible.”* [*Holmes, supra*, 121 F.4th at 734-735.] At best, in the present case during 2023 there was a split in the U.S. Courts of Appeals on the principles to be applied in the “private search” exception to the Fourth Amendment. Accordingly, the state of the law in 2023 does not satisfy the “good faith” test set forth by the U.S.

Supreme Court in *Davis v. U.S.*, 564 U.S. 229, 131 S. Ct. 2419 (2011), which is binding precedent.

The warrantless CyberTip data review procedure exposed 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 cellphone data provided by CyberTip.

Judicial implementation of this public policy was also exemplified by the 2021 decision of the U.S. Court of Appeals for the Ninth Circuit in *U.S. v. Wilson*, 13 F.4th 961 (9th Cir. 2021) and *U.S. v. Holmes*, 121 F.4th 727, 734-737 (9th Cir. 2024), with respect to warrantless police review of CyberTip uploads from a defendant’s cellphone of “suspected” child pornography. In *Wilson*, *Holmes*, and in the present case, there was no antecedent consent given to the government’s warrantless review of the CyberTip data extracted from defendant’s cellphone.

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

In *Herring v. U.S.*, 555 U.S. 135, 144, 129 S. Ct. 694 (2009), the U.S. 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 Wisconsin Department of Justice protocol 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, no antecedent warrant is to be sought. The mandate from the United States Supreme Court is crystal clear in both *Riley* and *Carpenter*: when in doubt, “Get A Warrant.” The Wisconsin Attorney General, deliberately and with full knowledge of the 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

There are two doctrinal principles that can come from a decision by this Court on the constitutional issues presented here:

1. A customer ostensibly granting an ESP permission to virtually “hash” scan a person’s private data for material objectionable to the ESP does not grant to the government unfettered access to download and view that cyberdata imagery without a warrant.

2. The investigative methodology employed by the government’s nationwide data scan protocol is fundamentally flawed. That protocol is to instruct law enforcement to physically view, without a warrant, “hash” coded matching imagery, derived by an ESP’s scan of a subject’s privately protected cellphone account content in the “cloud,” which imagery allegedly matches “known” child pornography imagery previously selected and inserted by an ESP into its own platform private archival database—a far cry from forensic reliability of the FBI’s national fingerprint database, a system which is strictly administered from collection to archiving by highly trained forensic professionals.

The government’s process here puts the constitutional cart before the horse. Instead, the government’s process does not begin first by physically vetting for authenticity and evidentiary foundation the “known” child pornography matching imagery within an ESP’s own proprietary archived database. The ESP’s search engine’s reliability is not vetted in a peer-reviewed process. Most notably, the “known” imagery previously archived by the ESP’s

algorithmic “hash” database is not viewed first before involving the suspect’s private domain.

3. A constitutional process would require the government to present the “known” child pornographic imagery extracted from the ESP’s archived data bank to a neutral and detached magistrate, coupled with an evidentiary showing that the proprietary “hash match” technology employed by the ESP in generating the “CyberTip” match is sufficiently reliable to provide “probable cause” to support issuing a search warrant to open and view the suspected contraband content within the subject person’s cellphone or ESP private account. Such a process would require only technical reprogramming of the present process.

The defendant, Michael Joseph Gasper, therefore, respectfully requests this Court to issue a Writ of Certiorari to review and reverse the action of the Supreme Court of the State of Wisconsin in this matter and affirm the Circuit Court of Waukesha County, Wisconsin’s Decision and Suppression Order.

Respectfully submitted,

DEBRA K. RIEDEL  
LAW OFFICES OF  
DEBRA K. RIEDEL  
2665 South Moorland Road,  
Suite 200  
New Berlin, WI 53151  
(414) 277-7818  
riedellaw@dkriedellaw.com

JOSEPH F. OWENS  
*Counsel of Record*  
LAW OFFICES OF  
JOSEPH F. OWENS, LLC  
2665 South Moorland Road,  
Suite 200  
New Berlin, WI 53151  
(262) 785-0320  
owenslaw2@gmail.com

*Counsel for Petitioner*

## **APPENDIX**

**TABLE OF APPENDICES**

	<i>Page</i>
APPENDIX A — WISCONSIN SUPREME COURT DECISION, JANUARY 14, 2026 . . . . .	1a
APPENDIX B — OPINION OF THE COURT OF APPEALS FOR THE STATE OF WISCONSIN, DISTRICT II, FILED OCTOBER 30, 2024. . . . .	90a
APPENDIX C — OPINION OF THE CIRCUIT COURT FOR THE STATE OF WISCONSIN, WAUKESHA COUNTY, FILED OCTOBER 30, 2023. . . . .	106a
APPENDIX D — ORDER OF THE CIRCUIT COURT FOR THE STATE OF WISCONSIN, WAUKESHA COUNTY, FILED FEBRUARY 16, 2024 . . . . .	118a
APPENDIX E — DEFENDANT’S MOTION TO SUPPRESS EVIDENCE AND DERIVATIVE FRUITS OF SEARCH OF PREMISES AND ELECTRONIC DEVICES DATED MAY 10, 2023. . . . .	119a

1a

**APPENDIX A — WISCONSIN SUPREME  
COURT DECISION, JANUARY 14, 2026**

SUPREME COURT OF WISCONSIN

No. 2023AP2319-CR

STATE OF WISCONSIN,

*Plaintiff-Appellant,*

v.

MICHAEL JOSEPH GASPER,

*Defendant-Respondent-Petitioner.*

REVIEW of a decision of the Court of Appeals.  
Waukesha County Circuit Court  
(Shelley J. Gaylord, Reserve J.),  
No. 2023CF470

Decided January 14, 2026

ANNETTE KINGSLAND ZIEGLER, J., delivered the majority opinion of the Court, in which JILL J. KAROFKY, C.J., and REBECCA GRASSL BRADLEY, BRIAN K. HAGEDORN, and JANET C. PROTASIEWICZ, JJ., joined. ANNETTE KINGSLAND ZIEGLER, J., filed a concurring opinion. REBECCA FRANK DALLET, J., filed a concurring opinion, in which SUSAN M. CRAWFORD, J., joined with respect to ¶¶67–85. BRIAN K. HAGEDORN, J., filed a concurring opinion, in which JILL J. KAROFKY, C.J., and JANET C. PROTASIEWICZ, J., joined. SUSAN M. CRAWFORD, J., filed an opinion concurring in part and dissenting in

*Appendix A*

part, in which REBECCA FRANK DALLET, J., joined with respect to ¶¶113–124.

¶1 ANNETTE KINGSLAND ZIEGLER, J. This is a review of a published court of appeals decision, *State v. Gasper*, 2024 WI App 72, 414 Wis. 2d 532, 16 N.W.3d 279, reversing the Waukesha County circuit court’s order granting defendant Michael Joseph Gasper’s motion to suppress evidence.

¶2 Gasper was charged with ten counts of possessing child pornography<sup>1</sup> and nine counts of child exploitation based upon the content on his cell phone.<sup>2</sup> Law enforcement obtained a warrant for his cell phone after the National Center for Missing and Exploited Children (“NCMEC”) forwarded a CyberTipline report<sup>3</sup> (which included a single, flagged, 16-second video) from Snapchat to the Wisconsin Department of Justice (“DOJ”). No person at Snapchat or NCMEC viewed the contents. Instead, Snapchat scanned its platform and identified the video file it flagged as known CSAM using a hash-based scanning program. The flagged video was first viewed by a person when an employee of the

---

1. Child pornography is commonly referred to as child sexual abuse material (“CSAM”); hereinafter we use CSAM.

2. Gasper accessed his Snapchat account exclusively from his cell phone.

3. The CyberTipline is a website operated by NCMEC to receive and process reports of online child sexual exploitation from the public and electronic service providers (“ESPs”). The information from these reports is then shared with the appropriate law enforcement agencies for investigation and action. We refer to the report hereinafter as a “CyberTip.”

*Appendix A*

DOJ did so without a warrant. Then the CyberTip with the flagged video was forwarded to local law enforcement who also viewed the video without obtaining a warrant. Gasper seeks to suppress this evidence on the basis that it was obtained in violation of his Fourth Amendment rights.

¶3 The circuit court granted Gasper’s motion to suppress all evidence of CSAM on the basis that there was a warrantless search of his cell phone which violated the Fourth Amendment to the United States Constitution under *Riley v. California*, 573 U.S. 373, 134 S. Ct. 2473, 189 L. Ed. 2d 430 (2014), and *Carpenter v. United States*, 585 U.S. 296, 138 S. Ct. 2206, 201 L. Ed. 2d 507 (2018). The circuit court also determined that suppression was appropriate because Message-Digest 5 (“MD5”),<sup>4</sup> a traditional hash-value scanning program, is “not secure,” stating “[c]ollision 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.”

¶4 The court of appeals reversed in a published opinion determining that there was no Fourth Amendment violation because Gasper did not have a reasonable expectation of privacy. *Gasper*, 414 Wis. 2d 532, ¶¶15–16. The court of appeals concluded that even if Gasper had a subjective expectation of privacy, his “obviously unlawful” conduct violated Snapchat’s terms of service and any subjective expectation that he had was “objectively unreasonable given Snapchat’s policies regarding sexual

---

4. MD5 is a cryptographic hash 128-bit algorithm. *What is MD5? Understanding Message-Digest Algorithms*, <https://www.okta.com/identity-101/md5/>.

*Appendix A*

content in general and sexually explicit content involving children in particular.” *Id.*, ¶22. The court of appeals concluded that no Fourth Amendment search occurred. *Id.*, ¶¶1, 29.

¶5 The Fourth Amendment serves as a limit on government power. *See Camara v. Mun. Ct. of City & Cnty. of San Francisco*, 387 U.S. 523, 528, 87 S. Ct. 1727, 18 L. Ed. 2d 930 (1967). (“The basic purpose of this Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by government officials.”); *Carpenter*, 585 U.S. at 305 (explaining that the Fourth Amendment places hurdles “in the way of a too permeating police surveillance”). A private search is not a government search. *United States v. Ginglen*, 467 F.3d 1071, 1074 (7th Cir. 2006). The Fourth Amendment is inapplicable to a search which has been completed by a private party as that search frustrates an individual’s expectation of privacy. *United States v. Jacobsen*, 466 U.S. 109, 117, 104 S. Ct. 1652, 80 L. Ed. 2d 85 (1984). The Fourth Amendment is implicated, however, if the government exceeds the private search. *Id.* at 115–22. Gasper does not argue that the government viewed more than the one video provided, nor does he argue that anything else of significance was in the video. Gasper relies entirely on the argument that the government exceeded Snapchat’s private search because a person in the government was the first to open and view the video, and did so without a warrant.

*Appendix A*

¶6 We conclude that the private search doctrine applies. It is undisputed that Snapchat performed a private search<sup>5</sup> when it scanned and flagged the single, 16-second video as CSAM. The government did not exceed the scope of Snapchat’s search when it viewed the video because any expectation of privacy Gasper may have had in the video was frustrated by the private search, and there was virtual certainty that law enforcement would not find anything of significance beyond what the private search revealed. As a result, the Fourth Amendment is not implicated. Accordingly, we affirm the court of appeals and remand to the circuit court for further proceedings consistent with this opinion.<sup>6</sup>

**I. FACTUAL AND PROCEDURAL BACKGROUND**

¶7 On January 13, 2023, Snapchat reported that it found CSAM and submitted a single, flagged, 16-second video to NCMEC. Snapchat’s hash-based scanning program, Microsoft’s PhotoDNA,<sup>7</sup> had detected and

---

5. Gasper does not argue that Snapchat’s search was anything other than private. For example, he does not argue that Snapchat was a government actor.

6. Although we affirm the court of appeals’ ultimate judgment reversing the circuit court’s grant of Gasper’s motion to suppress, we do so on other grounds. Thus, we clarify that the court of appeals’ reasoning is vacated and its published opinion in this case has no precedential value.

7. According to Snapchat’s 2023 Transparency Report, Snapchat uses PhotoDNA and Google’s Child Sexual Abuse Imagery Match to “identify known illegal images and videos of child sexual abuse.” Snap Inc., *Transparency Report: Combating*

*Appendix A*

flagged a CSAM video that had been uploaded to Snapchat’s servers from Gasper’s account. PhotoDNA “scans files to determine if they are copies of known and reported [CSAM] based on their ‘hash values.’”<sup>8</sup> *Gasper*, 414 Wis. 2d 532, ¶2. No person at Snapchat viewed the video.

¶8 NCMEC also did not view the video, but did confirm that the video was CSAM through a hash match of the uploaded file to visually similar files that were previously viewed and categorized by NCMEC.<sup>9</sup> NCMEC sent a CyberTip and the flagged video to the DOJ. A DOJ analyst opened the video file, without a warrant, to confirm that it contained CSAM. After confirming the video file

---

*Child Sexual Exploitation & Abuse*, WWW.VALUES.SNAP.COM, <https://values.snap.com/privacy/transparency-h1-2023> (last updated Dec. 13, 2023).

8. A hash value is “a string of characters obtained by processing the contents of a given computer file and assigning a sequence of numbers and letters that correspond to the file’s contents.” See *United States v. Reddick*, 900 F.3d 636, 637 (5th Cir. 2018). Traditional hash-value scanning programs like MD5 derive a hash value based on each individual, unique piece of data in a file. Thus, if even a single pixel in an image is altered, the resulting hash value would be substantially different. A predator could therefore make an insubstantial change to a CSAM image and avoid detection. To combat this, Microsoft developed PhotoDNA, which returns the same value even if there are slight changes made to a file. See *United States v. Miller*, 982 F.3d 412, 418 (6th Cir. 2020).

9. A hash match occurs when hash values are compared and are found to be identical. A hash value has been called a file’s fingerprint, VIN number or DNA. See *Miller*, 982 F.3d at 418.

*Appendix A*

contained CSAM, DOJ issued an administrative subpoena to the internet service provider to obtain the name and mailing address associated with the account.

¶9 The internet service provider responded with the account information which implicated Gasper. DOJ forwarded the CyberTip and attached video to the Waukesha County Sheriff's Office. There, a detective trained in this area opened the video, without a warrant, and also "confirmed that it depicted [CSAM]." *Id.*, ¶4. Based upon the CyberTip and video content, the detective then applied for, received, and executed a search warrant for Gasper's home and electronic devices. Police discovered ten files on Gasper's cell phone containing CSAM. Gasper was taken into custody, waived his *Miranda*<sup>10</sup> rights, and admitted that he had accessed and stored CSAM on his cell phone.

¶10 Gasper was charged with ten counts of Possession of Child Pornography, in violation of WIS. STAT. § 948.12(1m) and (3)(a) (2023–24),<sup>11</sup> and nine counts of Sexual Exploitation of a Child, in violation of WIS. STAT. § 948.05(1m) and (2p) (a). Gasper moved to suppress the evidence on the basis that it was an unconstitutional search in violation of the Fourth Amendment to the United States Constitution. He argued that because the government was the first to view the video and did so without a warrant, the search

---

10. *Miranda v. Arizona*, 384 U.S. 436, 86 S. Ct. 1602, 16 L. Ed. 2d 694 (1966).

11. All subsequent references to the Wisconsin Statutes are to the 2023-24 version unless otherwise indicated.

*Appendix A*

was unconstitutional. He also argued that the evidence recovered from the subsequent search warrant is likewise unconstitutional, being fruit of the initial warrantless, unconstitutional search of the Snapchat video.

¶11 The circuit court held a hearing on Gasper's motion to suppress. The Waukesha County Sheriff's Office detective was the only witness. He described how CyberTips and PhotoDNA operate. He said Snapchat uses PhotoDNA. PhotoDNA is "its own thing, its own program. It's its own software." The detective testified that PhotoDNA is, in his experience, "a reliable source of identifying suspected [CSAM.]" The detective testified that if he receives a CyberTip that has a PhotoDNA match or hash match, "[he has] never had it not be pornographic." In this case, knowing PhotoDNA was used, he said "it's likely going to be child sexual abuse material." PhotoDNA was the "sole thing that was used" to detect this CSAM.

¶12 The detective said PhotoDNA's analysis does not use an MD5 hash value for the overall file. He testified that PhotoDNA works by analyzing pieces of a file and comparing the similarity of those pieces to previously identified CSAM. Even if PhotoDNA would have used an MD5-based algorithm, there was no indication that a risk of collision (an incorrect identification or false positive match) would be present. The detective was questioned about the theoretical risk of collision, but he stated that he observed no evidence of it in this case, and that collision had only been observed in laboratory settings with extremely small sized files. NCMEC, however, does provide an MD5 hash value on the CyberTip to assist in the

*Appendix A*

future investigation. The detective referenced the MD5 hash value in his affidavit to the search warrant, but he stated that MD5 was not used in this case.

¶13 The State submitted into evidence Snapchat’s user agreement and policies and conditions which specifically “banned [CSAM]” and informed its users that Snapchat was actively scanning for CSAM on its platform. Its user agreement and policies and conditions also informed users that Snapchat’s discovery of CSAM will be reported to NCMEC and law enforcement.

¶14 Gasper did not testify, but he attempted to submit an affidavit which detailed the steps he took to keep his Snapchat account, cell phone, and Wi-Fi private and password protected. The circuit court denied his request to submit the affidavit, but accepted his statements regarding his expectation of privacy as an offer of proof.

¶15 The circuit court granted Gasper’s motion to suppress stating that “[t]here is a legitimate privacy interest in cell phones.” The court concluded that the private search doctrine is inapplicable for two reasons: (1) no human at Snapchat “eyeballed” the image, and (2) PhotoDNA assigned an MD5 hash value to the video and MD5 is categorically unreliable because of the risk of collision. The circuit court seemed to rely on information found on a website rather than the detective’s testimony to conclude that MD5 is subject to “collision” and that the technology used was “not secure.”<sup>12</sup> The circuit court stated,

---

12. In a footnote in its brief filed in the circuit court responding to Gasper’s motion to suppress, the State engaged in a general foundational discussion of hash algorithms and their

*Appendix A*

This case shows why proving probable cause on a case by case basis remains important. Relying on algorithms and computer programs as a basis for avoiding warrants is like relying on the ever changing waters of a river because technology and its limits change so fast. Ultimately, such reliance that expands the existing private/third party doctrine is for higher courts to decide.

¶16 The court of appeals reversed the circuit court’s decision and concluded that Gasper did not have a reasonable expectation of privacy:

A search occurs for the purpose of the Fourth Amendment “when an expectation of privacy that society is prepared to consider reasonable is infringed.” *State v. Purtell*, 2014 WI 101, ¶21, 358 Wis. 2d 212, 851 N.W.2d 417 (quoting [*Jacobsen*, 466 U.S. at 113]) . . . . The privacy interest is both subjective and objective: a defendant must show he or she subjectively expected privacy in the area or object, and that the expectation is one that society recognizes as reasonable.

*Gasper*, 414 Wis. 2d 532, ¶10 (internal citation omitted).

---

reliability, citing *What is MD5? Understanding Message-Digest Algorithms*, <https://www.okta.com/identity-101/md5/>, and Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 38–39 (2005). The State did not provide these articles to indicate that MD5 technology was used in the case at issue. Interestingly, the circuit court selected the okta.com article to cite in its decision.

*Appendix A*

¶17 The court of appeals stated the circuit court erred by simply relying on *Riley*, 573 U.S. 373, and *Carpenter*, 585 U.S. 296, because the appropriate “area” of the search was Gasper’s Snapchat account, not his cell phone, citing its decision in *State v. Bowers*, 2023 WI App 4, 405 Wis. 2d 716, 985 N.W.2d 123 (2022). *Gasper*, 414 Wis. 2d 532, ¶14. The court of appeals explained that in *Bowers*, it “rejected the State’s argument that because Bowers created the account with his county government email address and his employer could access the Dropbox account through the email address, Bowers lacked a reasonable expectation of privacy.” *Id.* (citing *Bowers*, 405 Wis. 2d 716, ¶¶22, 42). The court of appeals reasoned that the same analysis applied here because, “Snapchat did not access the video in Gasper’s account through his cell phone. Rather, the video was obtained directly from Gasper’s Snapchat account.” *Id.*, ¶15. The court of appeals went further to address whether Gasper had a reasonable expectation of privacy in the video in his Snapchat account and concluded that he did not. The court of appeals relied primarily on Snapchat’s Terms of Service, Community Guidelines, and Sexual Content Explainer. The court of appeals decided that “Gasper has failed to satisfy his burden to prove either his subjective or an objective expectation of privacy.” *Id.*, ¶20.

¶18 Gasper petitioned our court for review, which we granted.

**I. STANDARD OF REVIEW**

¶19 “Our review of an order granting or denying a motion to suppress evidence presents a question of

*Appendix A*

constitutional fact.” *State v. Tullberg*, 2014 WI 134, ¶27, 359 Wis. 2d 421, 857 N.W.2d 120 (quoting *State v. Robinson*, 2010 WI 80, ¶22, 327 Wis. 2d 302, 786 N.W.2d 463). We accept the circuit court’s factual findings unless they are clearly erroneous, and “independently apply constitutional principles to those facts.” *Id.*

**II. ANALYSIS****A. FOURTH AMENDMENT PRINCIPLES: PRIVATE SEARCH DOCTRINE**

¶20 The Fourth Amendment to the United States Constitution provides:

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.

U.S. CONST. amend. IV.

¶21 “The touchstone of the Fourth Amendment is reasonableness. The Fourth Amendment does not proscribe all state-initiated searches and seizures; it merely proscribes those which are unreasonable.” *Tullberg*, 359 Wis. 2d 421, ¶29 (internal citations omitted) (quoting *Florida v. Jimeno*, 500 U.S. 248, 250, 111 S. Ct.

*Appendix A*

1801, 114 L. Ed. 2d 297 (1991)).<sup>13</sup> Warrantless searches are presumptively unreasonable. *Id.*, ¶30. Fourth Amendment protections are an important check on government action. “[T]he touchstone of [Fourth] Amendment analysis [is] the question [of] whether a person has a ‘constitutionally protected reasonable expectation of privacy.’” *Oliver v. United States*, 466 U.S. 170, 177, 104 S. Ct. 1735, 80 L. Ed. 2d 214 (1984) (quoting *Katz v. United States*, 389 U.S. 347, 360, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967) (Harlan, J., concurring)).

---

13. In our case, the circuit court essentially determined that Gasper had a reasonable expectation of privacy because he used a cell phone to access Snapchat, citing *Riley v. California*, 573 U.S. 373, 134 S. Ct. 2473, 189 L. Ed. 2d 430 (2014), and *Carpenter v. United States*, 585 U.S. 296, 138 S. Ct. 2206, 201 L. Ed. 2d 507 (2018). The circuit court also distinguished cases where an individual is found not to have a reasonable expectation of privacy in documents that were conveyed to and viewed by third parties. *E.g.*, *Smith v. Maryland*, 442 U.S. 735, 742, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979) (recording of numbers dialed on a “pen register” installed by telephone company at request of law enforcement did not violate the Fourth Amendment).

It should be noted that the “third party” doctrine—which holds that an individual lacks a reasonable expectation of privacy in documents willingly conveyed to third parties—is separate and distinct from the “private search” doctrine, which applies when a third party actually performs a search of an individual’s secure property. Compare *United States v. Miller*, 425 U.S. 435, 442, 96 S. Ct. 1619, 48 L. Ed. 2d 71 (1976) (third-party doctrine applied to bank receipts conveyed to financial institution), with *United States v. Jacobsen*, 466 U.S. 109, 104 S. Ct. 1652, 80 L. Ed. 2d 85 (1984) (private party search when Federal Express employees opened suspicious package). See also *Smith v. Maryland*, 442 U.S. at 743–44 (“[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”).

*Appendix A*

¶22 The Fourth Amendment provides “rights against the government” not private parties. *Hibel v. Sixth Jud. Dist. Ct. Nev., Humboldt Cnty.*, 542 U.S. 177, 187, 124 S. Ct. 2451, 159 L. Ed. 2d 292 (2004). Stated differently, the Fourth Amendment applies to only “governmental action[.] [I]t is wholly inapplicable ‘to a search or seizure, even an unreasonable one, effected by a private individual . . . .’” *Jacobsen*, 466 U.S. at 113–14 (quoting *Walter v. United States*, 447 U.S. 649, 662, 100 S. Ct. 2395, 65 L. Ed. 2d 410 (1980) (Blackmun, J., dissenting)). A government agent may “view[] what a private party ha[s] freely made available for his inspection” without offending the Fourth Amendment. *Id.* at 119–20 (citing *Coolidge v. New Hampshire*, 403 U.S. 443, 487–90, 91 S. Ct. 2022, 29 L. Ed. 2d 564 (1971); *Burdeau v. McDowell*, 256 U.S. 465, 475–76, 41 S. Ct. 574, 65 L. Ed. 1048 (1921)). This is because a private actor’s earlier search frustrates the owner’s legitimate expectation of privacy. *Id.* at 119. In other words, under the private search doctrine, any expectation of privacy is lost because the private actor’s search abrogates the original expectation.<sup>14</sup>

It is well settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if

---

14. Gasper does not argue that Snapchat is acting at the direction of the government. The Fourth Amendment “protects against [private] intrusions if the private party acted as an instrument or agent of the Government.” *Skinner v. Ry. Lab. Execs. Ass’n*, 489 U.S. 602, 614, 109 S. Ct. 1402, 103 L. Ed. 2d 639 (1989).

*Appendix A*

that occurs the Fourth Amendment does not prohibit governmental use of that information. Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information[.]

*Id.* at 117. “[T]he critical inquiry under the Fourth Amendment is whether the authorities obtained information with respect to which the defendant’s expectation of privacy has not already been frustrated.” *United States v. Runyan*, 275 F.3d 449, 461 (5th Cir. 2001).

¶23 A private search, when repeated by the government, does not then become a government search, unless that search exceeds the scope of the private search. *Jacobsen*, 466 U.S. at 115. Herein lies the crux of Gasper’s argument—that the government exceeded Snapchat’s private search when it viewed the video without a warrant. Gasper does not argue that the video itself contained anything other than what was represented—CSAM. He also does not argue that the government searched more than the single, 16-second video Snapchat scanned, flagged, and reported. His argument relies entirely on the fact that no person at Snapchat actually looked at the video, and that because a person in the government was the first to view the video, that viewing exceeded Snapchat’s private search. But, since the State has asserted that the search was a private search, it is the defendant who bears the burden of proving that a government search occurred, to a preponderance of the evidence. *State v. Payano-Roman*, 2006 WI 47, ¶23, 290 Wis. 2d 380, 714 N.W.2d 548.

*Appendix A***B. PRIVATE PARTY SEARCH: UNCONSTITUTIONAL EXPANSION ARGUMENT**

¶24 Gasper agrees that Snapchat is a private party. Gasper argues that law enforcement unconstitutionally exceeded Snapchat’s private search because a person in government, not a person at Snapchat, was first to view the video with human eyes. More specifically, Gasper argues that it was unconstitutional for law enforcement to view the video because it “expanded the scope of the computer data scan contained in the CyberTip from NCMEC” and “expanded the scope of Snapchat’s private search.”

¶25 Stated differently, Gasper asserts that all of the CSAM evidence should be suppressed because the search violated the Fourth Amendment.<sup>15</sup> He makes much of the fact that no person at Snapchat viewed the video before forwarding it to law enforcement. But, Gasper fails to meet his burden of proving that this was a government search that exceeded the private search. The Fourth Amendment serves as a limit on government power, not a deterrent to private actors, in this case ESPs who use technology to protect the integrity of their platforms, and in so doing, find CSAM.<sup>16</sup> Snapchat’s PhotoDNA detected and flagged

---

15. Gasper also sought suppression of additional CSAM evidence recovered from the execution of a search warrant, on the basis that the subsequent search was the fruit of a warrantless, unconstitutional search of the Snapchat video.

16. We note, while federal law does not require an ESP to scan for CSAM, if CSAM is found, federal law does require the ESP to notify the authorities of an “apparent violation” which contains “[CSAM].” 18 U.S.C. § 2258A(a).

*Appendix A*

Gaspar's video as CSAM, and Snapchat reported that video to NCMEC, who then forwarded the CyberTip and video to the DOJ, who then forwarded the same to the Waukesha County Sheriff's Office.

¶26 We begin our analysis of the private search doctrine with *Walter v. United States*, 447 U.S. 649, 100 S. Ct. 2395, 65 L. Ed. 2d 410 (1980), wherein the United States Supreme Court suppressed evidence found when the FBI viewed, without a warrant, film strips that were misdelivered to a company. The company received 12 packages that contained 871 boxes of film. *Walter*, 447 U.S. at 651. The company's employees opened one or two of the packages and discovered boxes which depicted "suggestive drawings" and had "explicit descriptions." *Id.* at 652. One employee attempted to view film by holding it to the light, but was unsuccessful. *Id.* The company turned the boxes over to the FBI who reviewed them over the next two months, using a projector, without a warrant. *Id.* *Walter*, a plurality opinion, concluded that the FBI search of the film strips was unreasonable because it "constituted an unreasonable invasion of [the film strip] owner's constitutionally protected interest in privacy." *Id.* at 654. The court concluded that the projection of the films by the FBI was "a significant expansion of the search that had been conducted previously by a private party and therefore must be characterized as a separate search." *Id.* at 657. The court noted that "[p]rior to the Government screening, one could only draw inferences about what was on the films." *Id.*

*Appendix A*

¶27 *Walter* is distinguishable from the case before us today. Unlike the employee’s failed attempt to view a sampling of the film strips, Snapchat’s PhotoDNA scanned, opened, and flagged the single, 16-second video as CSAM. The government did not have access to any other materials that may have been scanned. Unlike the “private search” in *Walter*, where one could only infer what might be on the film, there was a virtual certainty that law enforcement would view nothing else of significance beyond what Snapchat’s technology scanned and reported, and that law enforcement viewing the video “would not tell [the government] anything more than [it] already had been told.” *Jacobsen*, 466 U.S. at 119. And, unlike turning over all 12 misdelivered and mostly unopened packages which contained 871 boxes of film to the FBI, Snapchat provided only the single, flagged, 16-second video. Unlike the FBI personnel who, without a warrant, took months to review all of the film strips with a projector, the government here viewed the single, 16-second video that Snapchat scanned, flagged as CSAM, and turned over to law enforcement.

¶28 The private search doctrine and whether the government exceeds the scope of the private search was next examined in *Jacobsen*, 466 U.S. 109. *Jacobsen* concluded that the Drug Enforcement Administration (“DEA”) “agent’s viewing of what a private party had freely made available for his inspection did not violate the Fourth Amendment” because “there was a virtual certainty that nothing else of significance” was in the package, and the inspection would not have provided “anything more than [what it] already had been told.” *Id.* at 119.

*Appendix A*

¶29 In *Jacobsen*, Federal Express employees accidentally damaged a package with a forklift and then opened it, pursuant to company policy, to prepare an insurance claim. *Id.* at 111. The employees discovered several plastic baggies of white powder. *Id.* Federal Express called the DEA and agents from the DEA arrived. *Id.* However, before they arrived, the box had been repackaged. *Id.* A DEA agent opened the repackaged box to test the white powder, which tested positive for cocaine. *Id.* at 111–12.

¶30 When referring to the employees’ private search, the Supreme Court stated, “Whether those invasions were accidental or deliberate, and whether they were reasonable or unreasonable, they did not violate the Fourth Amendment because of their private character.” *Id.* at 115. The Court then reasoned that although this is a private search, “additional invasions of . . . privacy by the Government agent must be tested by the degree to which they exceeded the scope of the private search.” *Id.* It determined that “the Fourth Amendment does not prohibit governmental use of the now nonprivate information.” *Id.* at 117. However, the Fourth Amendment is implicated “if the authorities use information with respect to which the expectation of privacy has not already been frustrated.” *Id.* The Supreme Court concluded that the DEA “agent’s viewing of what a private party had freely made available for his inspection did not violate the Fourth Amendment” because “there was a virtual certainty that nothing else of significance was in the package.” *Id.* at 119–20. The Court further noted that the government’s interest was “substantial,” particularly since it was “virtually certain

*Appendix A*

that the substance tested was in fact contraband.” *Id.* at 125.<sup>17</sup>

¶31 Since *Jacobsen*, the private search doctrine has been found to be applicable when there is a “virtual certainty” that the government’s search will not reveal anything more than that which the private party represented. See *United States v. Lichtenberger*, 786 F.3d 478, 488 (6th Cir. 2015); *Runyan*, 275 F.3d at 463–64; *United States v. Ackerman*, 831 F.3d 1292, 1305–06 (10th Cir. 2016). Although “virtual certainty” has not been specifically defined, it “implies something less than absolute confidence.” *United States v. Rivera-Morales*, 961 F.3d 1, 11 (1st Cir. 2020). It is “a common-sense determination into whether there is anything more than a remote or highly unlikely possibility that the officer’s actions will uncover something of significance apart from what the private searcher has found and reported.” *Id.*

¶32 Hash value comparison has been regarded as a scanning mechanism that detects CSAM with “almost absolute certainty.” *United States v. Reddick*, 900 F.3d 636, 639 (5th Cir. 2018) (quoting *United States v. Larman*, 547 F. App’x 475, 477 (5th Cir. 2013) (unpublished)). *Jacobsen*’s virtual certainty standard is met when the inspection “would not tell [the government] anything more

---

17. *Jacobsen* was a majority opinion. In *Jacobsen*, the Court also determined that the agents’ destroying cocaine to test it was a seizure that had “a de minimis impact on any protected property interest.” *Jacobsen*, 466 U.S. at 125.

*Appendix A*

than [it] had been told.” *Jacobsen*, 466 U.S. at 119.<sup>18</sup> The detective in this case testified that he had never seen a file identified by PhotoDNA as CSAM to be anything other than CSAM. And here, Gasper has not demonstrated that the government’s viewing of the 16-second video would reveal anything of significance beyond that which Snapchat scanned using PhotoDNA. The single, flagged video was removed from Gasper’s account and included as part of Snapchat’s CyberTip. Stated differently, “the government does not conduct a Fourth Amendment search when there is a ‘virtual certainty’ that its search will disclose *nothing more* than what a private party’s earlier search has revealed.” *United States v. Miller*, 982 F.3d 412, 417–18 (6th Cir. 2020) (quoting *Jacobsen*, 466 U.S. at 119). That is the case here.

¶33 We note that the Sixth Circuit in *Miller*, 982 F.3d 412, and the Fifth Circuit in *Reddick*, 900 F.3d 636, under similar facts, concluded that there is no Fourth Amendment violation because the private search doctrine applied. Gasper, however, urges us to instead adopt the reasoning of the Ninth and Second Circuits in *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021), and *United States v. Maher*, 120 F.4th 297 (2d Cir. 2024), which conclude otherwise. We, like several other states, decline Gasper’s invitation.<sup>19</sup>

---

18. Some courts have noted that a particular scanning system’s reliability might be challenged so to affect the virtual certainty standard, but that has not been demonstrated in the case at issue. *See infra* note 21.

19. Other state courts have adopted the reasoning in *Miller* and *Reddick*. *See Walker v. State*, 2023 Ark. App. 295, 669 S.W.3d

*Appendix A*

¶34 In *Miller*, a detective viewed two images identified as CSAM by a Google company scan, and the court concluded this was not a Fourth Amendment search under the private search doctrine. The court noted that a hash value is “a sort of digital fingerprint.” *Miller*, 982 F.3d at 417 (quoting *Ackerman*, 831 F.3d at 1294). Email files were scanned for certain hash values and matched to a copy of an illegal file. *Id.* at 420. Google’s scan revealed a Gmail account that had uploaded two files with hash values that matched CSAM. *Id.* Google sent the report with the files and the IP address to NCMEC. *Id.* NCMEC alerted local law enforcement. *Id.* Miller argued that the search was unconstitutional—that the police detective conducted an unreasonable search when he opened and viewed the files. *Id.* at 426. The court, however, relied on the private search doctrine and concluded that the Fourth Amendment restricts government, not private, action. *Id.* at 417. The court stated that “the government does not conduct a Fourth Amendment search when there is a ‘virtual certainty’ that its search will disclose *nothing more* than what a private party’s earlier search has revealed.” *Id.* at 417–18 (quoting *Jacobsen*, 466 U.S. at 119). The Sixth Circuit concluded that it was Google’s technology that “opened” and “inspected” the files, revealing that they had the same content as the known CSAM. *Id.* at 431. The court determined that “[t]his . . . information satisfies *Jacobsen*’s virtual-certainty test and triggers its private-search doctrine.” *Id.* at 430. Relying upon the unchallenged reliability of the hashing

---

243, 252–55 & n.8 (Ark. Ct. App. 2023); *People v. Wilson*, 56 Cal. App. 5th 128, 270 Cal. Rptr. 3d 200, 220–25 (Cal. Ct. App. 2020); *Morales v. State*, 274 So. 3d 1213, 1217–18 (Fla. Dist. Ct. App. 2019).

*Appendix A*

technology, the court concluded that the private search doctrine applied because it was virtually certain that the officer’s viewing of the files would disclose nothing more than the same images that the private actor’s employees had already viewed. *Id.* at 418.

¶35 The Sixth Circuit held that the government viewing the file did not infringe on a reasonable expectation of privacy or qualify as an unconstitutional search because the conduct did not exceed the scope of the earlier private search. *Id.* at 430. The court reasoned that it must ask “whether Google’s hash-value search of the files using its digital eyes made it virtually certain that [the detective] would discover no more than what Google had learned when he viewed the images with his human eyes.” *Id.* at 428 (citing *Jacobsen*, 466 U.S. at 119). The court concluded that because the detective “viewed only files with hash-value matches[,] . . . the private search doctrine applies.” *Id.* at 429. The court noted that rather than comparing the detective’s viewing of the files to the *Jacobsen* agent’s field test, “we must compare Google’s search of the files to the [Federal Express] employees’ search of the box.” *Id.* The Sixth Circuit concluded that the hash-value match from Google created “virtual certainty” that the investigator would view CSAM upon opening the segregated file. *Id.* at 417–18, 430. Like *Miller*, Snapchat’s PhotoDNA scanned, flagged, and verified that the files were CSAM.<sup>20</sup> “Under

---

20. Gasper’s argument hinges on the fact that no person at Snapchat viewed the video. He does not argue that Snapchat’s PhotoDNA scanned, opened, and inspected every communication in Gasper’s account. Nor do we conclude that law enforcement would be granted access to the entirety of Gasper’s Snapchat

*Appendix A*

the private-search doctrine, the government does not conduct a Fourth Amendment search when there is a ‘virtual certainty’ that its search will disclose *nothing more* than what a private party’s search has revealed.” *Id.* at 417–18. The detective here was given no more than what Snapchat’s scanning technology flagged as CSAM—a single, 16-second video.

¶36 The *Miller* court went further to explain that a hash-value scanning software may be more reliable than human observation, noting that hash-value scanning software does not contain the same human subjectivity and need for recall. The court referenced the “risk of a flaw in the [person’s] recollection,” and noted that if a person has a “quick view” of suspected CSAM, law enforcement would be permitted to conduct a more thorough investigative examination. *Id.* at 430–31 (quoting *Jacobsen*, 466 U.S. at 119) (alteration in original). But if the “view” is conducted by more reliable hash-value scanning, law enforcement would be precluded from having the same ability. *Id.* at 430. The court understood that unlike the human eye, “[c]ommon hash algorithms, by contrast, catalogue every pixel.” *Id.* The court questioned, “What sense would it make to treat a more accurate search of a file differently?” *Id.* at 431. Like in *Miller*, the record in the case before us demonstrates that Snapchat used PhotoDNA which is reliable in detecting CSAM and does so, unlike a human eye, by performing a pixel-by-pixel analysis. But the private search doctrine does not necessarily depend on the

---

account because of Snapchat’s PhotoDNA scan. The fact of this case is that Snapchat, a private actor, scanned a 16-second video, flagged it as CSAM, and turned it over to law enforcement.

*Appendix A*

reliability of the information provided. Here, PhotoDNA's hashing function flagged the reported video as it matched its previously scanned, known, CSAM. Even if PhotoDNA was deemed unreliable, which we need not decide, it is less than clear how that would impact the analysis of the private search doctrine since the analysis focuses on what the private actor searched.<sup>21</sup> The *Miller* court stated, and

---

21. We note that when considering Gasper's suppression motion, the circuit court conflated reliability of MD5 scanning programs with the private search doctrine. Gasper presented no witnesses to challenge the reliability of the PhotoDNA hash-matching technology, and yet the circuit court concluded that PhotoDNA used MD5 and that MD5 is categorically unreliable. The circuit court based its decision on the risk of "collision" and the unreliability of MD5 algorithms. The circuit court appears to have concluded that the MD5 algorithm played a role in the PhotoDNA scan. It stated, "PhotoDNA assigned Gasper's video a hash value that starts with 'MD5.' . . . If the 'MD5' is unreliable, it will create a 'collision.'" The record instead reflects that PhotoDNA is reliable and there is no evidence that MD5 was used. The detective did testify that an MD5 hash value was provided by NCMEC to assist law enforcement in future investigations. The detective stated he did not use MD5. The record does not support the circuit court's conclusion that PhotoDNA assigned the MD5 hash value, that MD5 was even used, or that there was MD5 collision. There is nothing in the record which indicates that PhotoDNA uses MD5, that Snapchat used MD5, or that anyone used MD5. Here, the CyberTip itself stated that PhotoDNA identified the reported file as known CSAM. The record reflects that the identifier operates like a "serial number" for the file. PhotoDNA is used to ensure there is no alteration that will avoid detection and instead PhotoDNA divides and identifies the scanned file compared to known CSAM files into tiny pieces, deriving a hash value for each piece and then comparing the pieces. Consequently, on this record, PhotoDNA

*Appendix A*

we agree, that “[j]ust because a private party turns out to be wrong about the legality of an item that the party discloses to police does not mean that the police violate the Fourth Amendment when they reexamine the item.” *Id.*

¶37 In *Reddick*, 900 F.3d 636, the Fifth Circuit Court of Appeals concluded that the detective did not violate Reddick’s Fourth Amendment rights by reviewing image files that had been flagged by a cloud hosting service as matching known CSAM files. The court stated:

The private search doctrine decides this case. A private company determined that hash values of files uploaded . . . corresponded to the hash values of known [CSAM] images. The company then passed this information on to law enforcement. This qualifies as a “private search” for Fourth Amendment purposes. And the government’s subsequent law enforcement actions in reviewing the images did not effect an intrusion . . . that [Reddick] did not already experience as a result of the private search.

900 F.3d at 637. Reddick argued that the detective’s warrantless opening of the files was an unlawful search. *Id.* at 638. But, “[u]nder the private search doctrine, ‘the critical inquiry under the Fourth Amendment is whether the authorities obtained information with respect to which [Reddick’s] expectation of privacy has not already been frustrated.’” *Id.* (quoting *Runyan*, 275 F.3d at 461).

---

reliably flagged the video in comparison to known CSAM files. The circuit court’s factual findings regarding MD5 were clearly erroneous.

*Appendix A*

*Reddick* stated the “hash value comparison ‘allows law enforcement to identify [CSAM] with almost absolute certainty,’ since hash values are ‘specific to the makeup of a particular image’s data.’” *Id.* at 639 (quoting *Larman*, 547 F. App’x at 477). The court concluded that when Reddick uploaded the files, PhotoDNA reviewed the hash values of those files and compared them against known hash values of CSAM. The court stated:

In other words, his “package” (that is, his set of computer files) was inspected and deemed suspicious by a private actor. Accordingly, whatever expectation of privacy Reddick might have had in the hash values of his files was frustrated by Microsoft’s private search.

...

[O]pening the file merely confirmed that the flagged file was indeed [CSAM], as suspected.

*Id.*

¶38 Gasper urges this court to instead adopt the rationale of the Ninth and Second Circuits in *Wilson*, 13 F.4th 961, and *Maher*, 120 F.4th 297, which concluded that law enforcement exceeded the scope of the private search. But, a closer look at those cases reveals that their reasoning is at odds with *Jacobsen*, 466 U.S. 109. Unlike *Jacobsen*, those courts concluded that expansion of the private search occurs when law enforcement is able to view more precise details about the content of the videos,

*Appendix A*

rather than whether law enforcement was virtually certain to view anything else of significance beyond what the private search revealed. It is incongruous to conclude that a defendant holds no privacy interest in a video flagged as CSAM by a private actor, but simultaneously recognize a privacy interest of CSAM details in the same video.

¶39 Moreover, *Wilson* and *Maher* do not seem to even consider how the scanning operates. Before any law enforcement is alerted, an ESP's scan essentially inspects the files and compares them to known CSAM in order to detect the contents. PhotoDNA alerts Snapchat when a file is found to contain CSAM. Snapchat scanned, flagged, and turned over a single, 16-second video, not all files that Snapchat may have scanned. In the case at issue, the detective viewing the reported video could not have expanded Snapchat's private search because in order to detect the CSAM in the first instance, it had already been scanned by Snapchat's PhotoDNA.

¶40 Gasper does not argue that the government search exceeded Snapchat's because it viewed more videos than the one provided or discovered more information from that video. He does not argue that the single, flagged, 16-second video contained anything other than CSAM. Gasper's argument, like in *Maher* and *Wilson*, rests solely on the fact that no person at Snapchat viewed the video and because a person in government was the first to view it, its viewing necessarily exceeded the Snapchat search. Gasper's argument assumes that a private search cannot occur unless human eyes view the evidence. He also assumes that when a person views potential CSAM, their

*Appendix A*

assessment, regardless of how long, must be more reliable than the PhotoDNA scanning system. *See supra*, ¶136. This is not to say that a computer program is infallible, but the record here bears no indication that the PhotoDNA used was somehow flawed. While the private search doctrine most often involves a person who has seen the evidence and then turns it over to law enforcement, the doctrine itself does not require that a person actually view the evidence. Whether a Snapchat employee viewed the video or not is of no moment to the private search doctrine, because the private search doctrine allows the government to review what a private actor has already searched, so long as there is a virtual certainty that its search will disclose nothing more of significance than what the private party search revealed.

¶141 Here, Snapchat scanned, flagged, and reported an “apparent” CSAM video. Of course, law enforcement may examine the exact same video more thoroughly or with a different base of knowledge than a private party so long as there is a virtual certainty that they will not find anything of significance beyond that which the private search revealed. *Miller*, 982 F.3d at 431; *Runyan*, 275 F.3d at 464; *United States v. Simpson*, 904 F.2d 607, 610 (11th Cir. 1990); *United States v. Tosti*, 733 F.3d 816, 822 (9th Cir. 2013). An officer may “learn” more than a lay person who views the same evidence and may see the details of the CSAM, but that alone does not automatically equate to the government exceeding the private search. The *Maher* and *Wilson* courts concluded that by viewing the video, suspected CSAM, law enforcement exceeded the private actor’s search because law enforcement

*Appendix A*

saw the details of the CSAM. Those courts reasoned that viewing the video revealed the “particulars” of the CSAM to law enforcement, and in so doing, the private search was exceeded. The private search doctrine is not solely evaluated from the perspective of what details law enforcement might see when viewing the video. Instead, it is evaluated from the perspective of what the private party’s search revealed and whether there is a virtual certainty that law enforcement will not find anything else of significance beyond that which the private search revealed.

¶42 *Jacobsen* did not analyze the Fourth Amendment based upon what law enforcement might see or learn when viewing the same evidence. *Jacobsen* and its progeny do not depend on the experience and knowledge of the viewer. Whether law enforcement may glean something more from viewing the same file does not amount to an expansion of the initial search. The private search is not exceeded if the identical information, here a single, 16-second video, is scanned and flagged as CSAM by a private actor, then provided to law enforcement for review and they look at the video. The test remains whether the government’s search exceeds what the private party’s search revealed. Both *Wilson* and *Maher* misapply *Jacobsen* because they turn on the fact that the investigating officers learned the CSAM details. In *Jacobsen*, the employees suspected the substance was cocaine, yet law enforcement could reopen the packages and test the powder without offending the private search doctrine. Reopening the package to view its contents was not unconstitutional. Learning whether the powder was cocaine was also not prohibited. We do

*Appendix A*

not agree with *Maher's* and *Wilson's* conclusion that law enforcement exceeds the private actor search when it views the “particulars” in the already-scanned CSAM video. We disagree that seeing the details of the CSAM is an expansion of the private search, *see Wilson*, 13 F.4th at 973, as the video was virtually certain to contain nothing else of significance. Adopting the *Maher/Wilson* reasoning would create an unworkable, subjective, after-the-fact standard to afford a defendant a privacy interest in the details of CSAM even though they have no privacy interest in that file. This approach is at odds with *Jacobsen* and the private search doctrine.

¶43 As in *Jacobsen*, the test remains whether there is a virtual certainty that the government will not find anything of significance beyond what the private search revealed. Law enforcement may more thoroughly review the video, but if law enforcement confirms that the video Snapchat scanned, flagged, and reported is CSAM and nothing more, the fact that a person in law enforcement is the first to view the video does not equate to a private search being exceeded. And, Gasper does not argue that law enforcement viewed more videos or his entire account, or that law enforcement learned anything more from viewing the video. His sole argument is that the government exceeded Snapchat's search because a person in the government was the first to actually view the video.

¶44 Yet, Gasper urges that we require law enforcement to obtain a warrant before it can view what it is given by a private party. But, allowing law enforcement to view a tip, which here includes a video scanned and flagged as

*Appendix A*

CSAM by a private party, before conducting a full-blown search, also makes practical and constitutional sense.<sup>22</sup> The detective's review of the CSAM video allows law enforcement the opportunity to determine whether what the private party saw even warrants a more thorough investigation.

¶45 In short, law enforcement may receive a tip from any number of sources. The Fourth Amendment does not protect Gasper from a private actor who discovers that CSAM has been uploaded to its platform, discovered through the private actor's scan, and the private actor forwards that CSAM to the authorities. The government did not conduct a warrantless search of Gasper's cell phone or his Snapchat account; it merely reviewed the full CyberTip which included the video flagged as "apparent" CSAM. The private search doctrine applies when, such as here, a private actor invites a government agent to recreate the private actor's search and there is "virtual certainty that nothing else of significance" is in the file, and that inspection "would not tell [the State] anything more than [it] already had been told." *Jacobsen*, 466 U.S. at 119. Nothing about this review of a tip gave law enforcement unfettered access to Gasper's Snapchat

---

22. This CyberTip is somewhat like a tip from an identified citizen informant. The fact that federal law requires that ESPs like Snapchat report "apparent [CSAM]" as the ESPs "becom[e] aware," has caused some courts to conclude that this requirement actually heightens the reliability of the tip. *State v. Silverstein*, 2017 WI App 64, ¶19, 378 Wis. 2d 42, 902 N.W.2d 550. *Silverstein* aptly compares a CyberTip to that of an identified citizen informant.

*Appendix A*

account or his cell phone. Viewing the file was not a search that expanded that of Snapchat's.<sup>23</sup>

¶46 “Under the private-search doctrine, the government does not conduct a Fourth Amendment search where there is a ‘virtual certainty’ that its search will disclose *nothing more* than what a private party’s search has revealed.” *Miller*, 982 F.3d at 417–18 (quoting *Jacobsen*, 466 U.S. at 119). The hash-based search of the files using Snapchat’s digital eyes made it virtually certain that the detective would discover no more than what Snapchat had learned when a person in government viewed the images with human eyes. *Jacobsen*, 466 U.S. at 119. Here, because the government “viewed only files with hash-value matches[,] . . . the private-search doctrine applies.” *Miller*, 982 F.3d at 429. In other words, Gasper’s individual file was inspected and deemed suspicious by a private actor, and the private actor flagged the single, 16-second video and provided it to NCMEC. Accordingly, whatever expectation of privacy Gasper might have had in the hash values of his file was frustrated by Snapchat’s private search. Opening the file “merely confirmed that the flagged file was indeed [CSAM], as suspected.” *Reddick*, 900 F.3d at 639.

### C. GASPER’S REASONABLE EXPECTATION OF PRIVACY

¶47 Gasper argues that he has a categorical expectation of privacy in the reported video under *Riley*, 573 U.S. 373. Under the facts of *Riley*, the Supreme Court held that warrantless searches of cell phones are

---

23. Nor does our private party search analysis need to turn on whether Gasper violated Snapchat’s terms of service.

*Appendix A*

presumptively unreasonable. 573 U.S. at 403. Gasper argues that he had a “reasonable expectation of privacy” in the cyberdata uploaded from his cellphone to his Snapchat account” and in the “content extracted” from that account. Gasper posits that because he accessed Snapchat exclusively from his cell phone, this case should be analyzed as if it was a cell phone search, and that he has a reasonable expectation of privacy of his cell phone and the Snapchat account.<sup>24</sup>

¶48 Because we conclude that Snapchat performed a private search when it scanned and identified the flagged video as CSAM and the government did not exceed the scope of Snapchat’s private search when it viewed the video, we need not analyze whether Gasper possessed a reasonable expectation of privacy entitling him to Fourth Amendment protection. We also need not determine to what extent, if any, Snapchat’s terms of service agreement influences a reasonable expectation of privacy in a Fourth Amendment analysis.

**D. GOOD-FAITH EXCEPTION**

¶49 Finally, Gasper argues that the good-faith exception to the exclusionary rule does not apply because that would swallow the warrant requirement. Because we determine that a warrant is not required in the case at issue, we need not analyze the good-faith exception.

---

24. No law enforcement officer accessed Gasper’s Snapchat account or cell phone without a warrant. DOJ issued an administrative warrant and law enforcement later obtained a search warrant after it also confirmed the video contained CSAM.

*Appendix A*

We caution, however, that “[t]o 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.” *Herring v. United States*, 555 U.S. 135, 144, 129 S. Ct. 695, 172 L. Ed. 2d 496 (2009). The conduct must be deliberate, reckless, or grossly negligent or the result of recurring or systemic negligence. *Id.*

¶50 We need not consider the parties’ arguments about the good-faith exception further, because we conclude that the search was not unconstitutional.

**III. CONCLUSION**

¶51 The Fourth Amendment serves as a limit on government power. *See Camara*, 387 U.S. at 528 (“The basic purpose of this Amendment, as recognized in countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by government officials.”); *Carpenter*, 585 U.S. at 305 (explaining that the Fourth Amendment places hurdles “in the way of a too permeating police surveillance”). A private search is not a government search. *Ginglen*, 467 F.3d at 1074. The Fourth Amendment is inapplicable to a search which has been completed by a private party as that search frustrates an individual’s expectation of privacy. *Jacobsen*, 466 U.S. at 117. The Fourth Amendment is implicated, however, if the government exceeds the private search. *Id.* at 115–22. Gasper does not argue that the government viewed more than the one video provided, nor does he argue that anything else of significance was in

*Appendix A*

the video. Gasper relies entirely on the argument that the government exceeded Snapchat's private search because a person in the government was the first to open and view the video, and did so without a warrant.

¶52 We conclude that the private search doctrine applies. It is undisputed that Snapchat performed a private search when it scanned and flagged the single, 16-second video as CSAM. The government did not exceed the scope of Snapchat's search when it viewed the video because any expectation of privacy Gasper may have had in the video was frustrated by the private search, and there was virtual certainty that law enforcement would not find anything of significance beyond what the private search revealed. As a result, the Fourth Amendment is not implicated. Accordingly, we affirm the court of appeals and remand to the circuit court for further proceedings consistent with this opinion.

*By the Court.*—The decision of the court of appeals is affirmed, and this cause is remanded to the circuit court for further proceedings consistent with this opinion.

*Appendix A*

ANNETTE KINGSLAND ZIEGLER, J., concurring.

¶53 I join the opinion that I wrote for the majority and write separately to expound upon this area of the law.

**I. BACKGROUND: FEDERAL LAW REQUIREMENTS**

¶54 Although we address the Fourth Amendment’s application to Wisconsin’s state law in the majority opinion, we did not detail the federal law implications when it comes to reporting CSAM. *See United States v. Miller*, 982 F.3d 412, 424 (6th Cir. 2020). Though Snapchat is not required to use any particular technology to identify CSAM, if it finds CSAM, then federal law requires it to report that CSAM to NCMEC. 18 U.S.C. § 2258A(a), (f). If such a CyberTip is forwarded to NCMEC, then NCMEC must forward the CyberTip to law enforcement for investigation. 18 U.S.C. § 2258A(c). The stated purpose of these laws is “to reduce . . . and . . . prevent the online sexual exploitation of children.” 18 U.S.C. §§ 2258A(a)(1)(A)(i), (a)(2)(A), 2510(15), 2258E.

¶55 Federal law requires Snapchat to report when it becomes aware of “apparent violations of [CSAM].” 18 U.S.C. § 2258A(a). That is exactly what Snapchat did. Snapchat reported the video and stated that it contained “apparent [CSAM].” Snapchat arrived at this conclusion utilizing its hash-value algorithm—such a system has been deemed reliable, akin to a digital fingerprint, a DNA match, or a VIN number. *United States v. Ackerman*, 831 F.3d 1292, 1294 (10th Cir. 2016); *United States v. Miller*, 982 F.3d 412, 418 (6th Cir. 2020); *see also United*

*Appendix A*

*States v. Dunning*, 2015 U.S. Dist. LEXIS 140993, 2015 WL 13736169, at \*2 (E.D. Ky. Oct. 1, 2015) (finding that the chance of two of these files coincidentally sharing the hash value to be one in 9.2 quintillion—that is, highly unlikely). Snapchat’s algorithm viewed each, individual pixel of the image, compared it to a database filled with known CSAM images, and determined that it contained contraband. Then, that single, 16-second video was removed from Gasper’s account, and Snapchat followed the procedure outlined in federal law. In this case, Snapchat alone decided that this video contained CSAM. Snapchat, as a private actor, followed the letter of the federal law. Thus, federal law supports the process used in this case. Once Snapchat reported the CSAM, the government did not expand the scope of the search. It was Snapchat who frustrated Gasper’s expectation of privacy—not the government.

¶156 Snapchat, through its algorithm, used its own resources to search for and identify contraband. Like the Supreme Court in *United States v. Jacobsen*, 466 U.S. 109, 104 S. Ct. 1652, 80 L. Ed. 2d 85 (1984), other federal appellate courts have also applied the private search doctrine and concluded that there is no expansion of the private search when there is a “virtual” or “substantial” certainty that the government agent’s search will not reveal anything more than what the private party represented. See *United States v. Phillips*, 32 F.4th 865, 870 (9th Cir. 2022); *United States v. Rivera-Morales*, 961 F.3d 1, 11, 15 (1st Cir. 2020); *United States v. Lichtenberger*, 786 F.3d 478, 488 (6th Cir. 2015); *Rann v. Atchison*, 689 F.3d 832, 836–37 (7th Cir. 2012). However, in *Jacobsen*, unlike the case at issue, law enforcement’s

*Appendix A*

search exceeded the search conducted by the Federal Express employees. Law enforcement opened the box, observed the baggies of powder, and tested the substance for cocaine. Although the testing was clearly beyond the employee's private search, the court concluded that the intrusion was nonetheless de minimis. As such, *Jacobsen* teaches that virtual certainty does not necessarily mean identical. Once the private search has frustrated an individual's reasonable expectation of privacy, the Fourth Amendment does not always require that the private search be perfectly replicated by the government.

¶57 Quite obviously, law enforcement is not required to avert its eyes from criminal activity. Viewing the provided video allowed law enforcement to confirm or dispel that it contained CSAM, as reported. Here, the government viewed what Snapchat's private search revealed: one, 16-second CSAM video from Gasper's account. It viewed what Snapchat provided and nothing more. Foregoing a warrant to view what this private actor provided through its own private search, is not only practical, it is constitutional.

¶58 Snapchat followed federal law by reporting the flagged video to NCMEC, and then NCMEC carried out its duties by forwarding the CyberTip to the government. In other words, this "apparent violation" followed congressional safeguards, which exist to reduce and prevent online sexual exploitation of children. 18 U.S.C. § 2258A(a).<sup>1</sup>

---

1. A different analysis would be needed had Snapchat provided complete access to, or all videos from, Gasper's account or other downloads which were not flagged as CSAM. But it did

*Appendix A***II. PRACTICAL IMPLICATIONS: WARRANT**

¶59 Gasper would require the detective to first obtain a warrant to view the CSAM-video Snapchat provided. But Gasper’s argument assumes Fourth Amendment protection exists here, despite this being a private search. He also assumes that law enforcement would limit its warrant request to the video alone. As the majority opinion explained, the government is not required to obtain a warrant before viewing this private search. And as a practical matter, if law enforcement had probable cause to obtain a warrant to view the video for CSAM, then it likely follows that it would have probable cause to seek a much broader warrant searching Gasper’s entire account, home, and electronic devices. Even the Second Circuit in *United States v. Maher*, a case that required a warrant before viewing CSAM, acknowledged that CyberTips can establish probable cause for a broader search warrant. *See Maher*, 120 F.4th 297, 319 (2d Cir. 2024) (stating that the CyberTip would have “demonstrate[d] probable cause to support warrants for . . . searches of . . . Google accounts and residence[s].”); *see also United States v. Cartier*, 543 F.3d 442, 446 (8th Cir. 2008). Given that the Fourth Amendment’s touchstone is reasonableness, it is more reasonable for law enforcement to conduct this limited review of a private search before engaging in a far more invasive investigation based on an expansive warrant. *State v. Tullberg*, 2014 WI 134, ¶29, 359 Wis. 2d 421, 857 N.W.2d 120.

---

not. A different analysis might occur if the algorithm deployed was proven unreliable. But it was not.

*Appendix A***III. THE GOOD-FAITH EXCEPTION**

¶60 To be clear, “[t]o trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrent is worth the price paid by the justice system.” *Herring v. United States*, 555 U.S. 135, 144, 129 S. Ct. 695, 172 L. Ed. 2d 496 (2009). The conduct must be “deliberate, reckless, or grossly negligent or the result of ‘recurring or systemic negligence.’” *Id.* When police act in good faith, or an area of the law is unsettled, there is no police misconduct to deter. *State v. Scull*, 2015 WI 22, ¶44, 361 Wis. 2d 288, 862 N.W.2d 562; *United States v. Dorosheff*, 110 F.4th 999, 1004–05 (7th Cir. 2024), *reh’g denied*, No. 22-2291, 2024 U.S. App. LEXIS 23293, 2024 WL 4178484 (7th Cir., Sept. 12, 2024). That is exactly what is missing here: a deterrent effect.

**IV. VICTIMS’ RIGHTS**

¶61 Lastly, while not dispositive in this case, it is interesting to note that Gasper’s arguments highlight the conflict between who might have competing privacy interests in the CSAM. Wisconsin has long held strong victim rights protection both in the form of legislation and in our constitution. WIS. CONST. ART. I, § 9m; WIS. STAT. ch. 950. One might opine about the child victim’s privacy interest in a CSAM file. Justice Sotomayor has recognized, “[t]here is little doubt that the possession of images of a child being sexually abused would amount to an intentional invasion of privacy tort—and an extreme one at that.” *Paroline v. United States*, 572 U.S. 434, 483, 134 S. Ct. 1710, 188 L. Ed. 2d 714 (2014) (Sotomayor, J., dissenting).

*Appendix A*

¶62 Consider also, Wisconsin’s statutory right of privacy. Wisconsin Stat. § 995.50 states that a person’s privacy is protected regardless of whether there is a criminal action. That section specifically references Wis. STAT. § 942.09 with respect to “intimate representations.” It could be that a minor would be deemed “incapable of consent” under § 942.09(1)(ae). We save these considerations for another day.

¶63 I would note, however, that Gasper’s arguments that a person at Snapchat needed to view the CSAM before law enforcement could, would subject a child victim to even more victimization. The more human eyes that witness the wrongdoing, the more the child is victimized. And, if employees of the ESPs are forced, under Gasper’s logic, to personally view and witness the CSAM video, they too may be victims of secondary trauma.<sup>2</sup> But for now, those considerations will be left for another day.

**V. CONCLUSION**

¶64 For all the foregoing reasons, I respectfully concur.

---

2. “Secondary trauma affects people who witness traumatic events . . . . It happens when people are exposed to another person’s traumatic event.” Kendall-Tackett, Kathleen, *Psychological Trauma Theory, Research, Practice & Policy, Editorial*, 15 JOURNAL OF THE AMERICAN PSYCHOLOGICAL ASSOCIATION, No. S2, S201-S202 (2023).

*Appendix A*

JUSTICE DALLET, concurring

REBECCA FRANK DALLET, J., with whom SUSAN M. CRAWFORD, J., joins with respect to ¶¶67-85, concurring.

¶65 Now more than ever we live in a digital world. Vast amounts of information are created, stored, and shared using smartphones, computers, and other digital devices. And those devices “are portals to an endless array of online services [and] communities” where we can store our private information or share it with friends and strangers alike, all with the tap of a finger. ORIN KERR, *THE DIGITAL FOURTH AMENDMENT 2* (2025). Now that we “live an online existence that can rival the physical one,” courts must grapple with the difficulties of adapting existing Fourth Amendment rules in order to preserve the delicate balance between privacy rights and the needs of law enforcement. *Id.* at 2–5.

¶66 Unfortunately both the court of appeals and majority fail at that task in this case, weakening our Fourth Amendment rights in the process. The court of appeals did so by concluding that boilerplate terms of service imposed by electronic service providers like Snapchat can limit or even eliminate users’ Fourth Amendment rights online. *See, e.g., State v. Gasper*, 2024 WI App 72, ¶¶21–22, 414 Wis. 2d 532, 16 N.W.3d 279. And although the majority wisely vacates the court of appeals’ published opinion, it does so only summarily. *See* majority op., ¶6, n.6. Making matters worse, the majority also misapplies the private-search doctrine, and concludes that no Fourth Amendment violation occurred in this case. I write separately to explain why both of these

*Appendix A*

decisions are wrong, and why the good-faith exception to the exclusionary rule nonetheless applies.

**I**

¶167 The Fourth Amendment guarantees the right of the people to be free in “their persons, houses, papers, and effects [from] unreasonable searches and seizures . . . .” U.S. CONST. amend. IV. By its terms, the Fourth Amendment therefore applies only to searches and seizures by the government, and only if they are unreasonable. A “search” in this context is a government intrusion into an area or object in which an individual has a reasonable expectation of privacy. *See Kyllo v. United States*, 533 U.S. 27, 32–33, 121 S. Ct. 2038, 150 L. Ed. 2d 94 (2001).

¶168 In this case, the State claims that Gasper lacked a reasonable expectation of privacy in the video he privately uploaded to his account because he agreed to and subsequently breached Snapchat’s terms of service.<sup>1</sup> If that were true it would be dispositive, since “no ‘search’ . . . occur[s] for Fourth Amendment purposes” if “the person objecting to a government intrusion lacks a reasonable expectation of privacy in the area examined . . . .” *United States v. Shelton*, 997 F.3d 749, 758 n.2 (7th Cir. 2021).

---

1. For ease of discussion, I use the phrase “terms of service” throughout this opinion to refer collectively to three separate Snapchat policies: its terms of service, community guidelines, and “Sexual Content Community Guidelines Explainer Series.” Each of these documents are available from Snapchat, and users must agree to their terms in order to join the platform.

*Appendix A*

¶169 The court of appeals agreed with the State’s argument, holding that the Fourth Amendment was not implicated when the DOJ analyst viewed the video for the first time without obtaining a warrant because Gasper lacked a reasonable expectation of privacy in the video. *See Gasper*, 414 Wis. 2d 532, ¶128. In doing so, the court of appeals determined that the private terms-of-service agreement between Gasper and Snapchat eliminated any Fourth Amendment protection Gasper had in the video vis-à-vis the government. *See id.* This holding, however, is a significant departure from settled Fourth Amendment doctrine in analogous real-world contexts, and would result in lesser Fourth Amendment protections in the digital world.

¶170 Before explaining why, it is helpful to describe what terms of service are. To create an account with an electronic service provider like Snapchat, users must agree to the terms of service, that is, “contractual language giving the company broad rights over” users’ accounts and the files stored there. *See Orin Kerr, Terms of Service and Fourth Amendment Rights*, 172 U. PA. L. REV. 287, 289 (2024). Two types of provisions are commonplace. The first are what Professor Orin Kerr calls “breach provisions,” which “explain what the company considers a breach that allows the company to limit or delete the user’s account.” *Id.* at 292. And the second are “rules-of-the-road provisions,” which “set expectations about how a service will be run, such as what the company will do with [users’] data in various circumstances.” *Id.*

¶171 The court of appeals relied on both types of provisions when it concluded that Gasper lacked

*Appendix A*

a reasonable expectation of privacy in the video.<sup>2</sup> Specifically, it relied on breach provisions, like Snapchat’s prohibition on uploading “nude or sexually explicit content involving anyone under the age of 18.”<sup>3</sup> *Gasper*, 414 Wis.

---

2. At times, the court of appeals described its opinion as deciding “whether Gasper had a reasonable expectation of privacy in the video *in his Snapchat account*.” *Gasper*, 414 Wis. 2d 532, ¶15 (emphasis added); *see also id.*, ¶12 (“Gasper’s Snapchat account [is] the relevant ‘area’ that was searched.” (quoting another source)). This framing is incorrect, however, since no government official ever searched Gasper’s account; the Fourth Amendment “search,” if any occurred (and, as Justice Crawford explains in her separate writing, a search did occur), happened when law enforcement viewed for the first time the video attached to the tip by Snapchat and NCMEC. The issue is thus whether Gasper had a reasonable expectation of privacy *in the video*. Despite the court of appeals’ mistaken framing, I discuss its reasoning further, since it would apply equally to the video alone. The video, after all, was subject to the same Snapchat policies as Gasper’s account, policies the court of appeals said eliminated any expectation of privacy Gasper otherwise had. *See id.*, ¶¶21–28.

3. In discussing why Gasper lacked a reasonable expectation of privacy in the video, the court of appeals noted that uploading the video to his account “was obviously unlawful.” *See Gasper*, 414 Wis. 2d 532, ¶22. In context, the court of appeals was describing why Gasper’s conduct violated Snapchat’s terms of service. It could not have meant—as the majority erroneously suggests—that Gasper lacked a reasonable expectation of privacy simply because his conduct was unlawful. *See majority op.*, ¶4. The United States Supreme Court has made clear that individuals may have reasonable expectations of privacy even while engaging in criminal activity. *See, e.g., Minnesota v. Olson*, 495 U.S. 91, 96–97, 110 S. Ct. 1684, 109 L. Ed. 2d 85 (1990); *Payton v. New York*, 445 U.S. 573, 583–603, 100 S. Ct. 1371, 63 L. Ed. 2d 639 (1980); *Katz v.*

*Appendix A*

2d 532, ¶18. The court of appeals also cited rules-of-the-road statements by Snapchat, including that it could “access, review, screen, and delete” user-uploaded content at any time for any reason, and that it would “report all instances of child sexual exploitation to authorities . . . .” *See id.*, ¶¶17–18. Together, the court of appeals held, these provisions in the terms of service meant Gasper lacked a reasonable expectation of privacy in the video (1) because uploading the video to his account breached the prohibition on uploading child-sexual-abuse material (CSAM) to the platform; and (2) because the rules-of-the-road provisions put him on notice that Snapchat could access, review, screen, or delete his content and would report any CSAM it found to law enforcement. *Id.* ¶¶21–22, 28.

¶72 The court of appeals’ decision and others like it<sup>4</sup> all rest on the false premise that in the digital world,

---

*United States*, 389 U.S. 347, 348–59, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967). As Justice Ginsburg aptly explained, “[i]f the illegality of the activity made constitutional an otherwise unconstitutional search, such Fourth Amendment protection, reserved for the innocent only, would have little force in regulating police behavior toward either the innocent or the guilty.” *Minnesota v. Carter*, 525 U.S. 83, 110, 119 S. Ct. 469, 142 L. Ed. 2d 373 (1998) (Ginsburg, J., dissenting).

4. *See, e.g., United States v. Colbert*, No. 23-cr-40019-TC-1, 2024 U.S. Dist. LEXIS 85096, 2024 WL 2091995, at \*8–9 (D. Kan. May 9, 2024) (holding that Snapchat’s terms of service eliminated a user’s expectation of privacy in his account); *United States v. Sporn*, No. 21-10016-EFM, 2022 U.S. Dist. LEXIS 39070, 2022 WL 656165, at \*9–10 (D. Kan. Mar. 4, 2022) (concluding that a violation of Twitter’s terms of service meant a user lacked a reasonable expectation of privacy in his account); *United States v. Bohannon*, 506 F. Supp. 3d 907, 915 (N.D. Cal. 2020) (stating that

*Appendix A*

the terms of private agreements and breaches of those terms can curtail or even eliminate expectations of privacy against the government. Courts have rejected that premise across a variety of analogous real-world contexts, however, and rightly held that private contracts “have little or no effect on Fourth Amendment rights.” Kerr, *Terms of Service*, *supra* at 308.

¶73 Car-rental contracts, apartment leases, and hotel-rental agreements are real-world counterparts to terms of service in the digital world. Like terms of service, each of these agreements allows a private party to use an owner’s property subject to contractual limitations. Yet breaching provisions in a car-rental contract, even ones that specify that they void the agreement, does not result in an unauthorized driver losing their reasonable expectation of privacy in the vehicle. *See United States v. Byrd*, 584 U.S. 395, 408, 138 S. Ct. 1518, 200 L. Ed. 2d 805 (2018). Likewise, breaches of apartment leases and hotel-rental agreements do not extinguish renters’ reasonable expectation of privacy in their apartment or hotel room. *See, e.g., United States v. Thomas*, 65 F.4th 922, 923–25 (7th Cir. 2023); *United States v. Cunag*, 386

---

by agreeing to the terms of service, a user consented to a search of his Microsoft OneDrive account); *but see United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) (explaining that although terms of service “might, in some cases, be sweeping enough to defeat a reasonable expectation of privacy in the contents of an email account,” the AOL terms at issue in the case did not do so); *United States v. Irving*, 347 F. Supp. 3d 615, 623 (D. Kan. 2018) (determining that Facebook’s terms of service did not eliminate a user’s expectation of privacy in his account’s contents).

*Appendix A*

F.3d 888, 895 (9th Cir. 2004). To be sure, breaches of these agreements may lead to eviction. But “the right to [evict] does not imply a right to [invite police to search the residence].” *Thomas*, 65 F.4th at 924; *but see State v. Whitrock*, 161 Wis. 2d 960, 966, 975–76, 468 N.W.2d 696 (1991) (concluding that a landlord could consent to a search after serving notice of eviction and believing the tenant had vacated the premises).

¶74 Granting a contractual right of access to an otherwise private space in the real world similarly does not eliminate reasonable expectations of privacy, thus authorizing law enforcement to access that space without a warrant. Apartment leases and hotel-rental agreements commonly include terms permitting the apartment owner or manager to access the unit for inspections or maintenance, or allowing hotel management or housekeeping to enter a guest’s room for maintenance or cleaning. Yet in both contexts, courts have made clear that granting such a right of access doesn’t eliminate the renter’s reasonable expectation of privacy and open the space up to warrantless government searches. *See United States v. Warshak*, 631 F.3d 266, 287 (6th Cir. 2010).

¶75 Nor does it matter for purposes of the reasonable-expectation-of-privacy analysis that private parties might use their contractual right to access an otherwise private space to uncover information and share it with the government. “It is true, of course, that sharing space creates risks that a co-occupant will share [otherwise private] information with the government.” *See Kerr, Terms of Service, supra* at 307. But just because the

*Appendix A*

government could discover information through someone else does not mean the government can enter a private space directly and take the information itself. *See, e.g., State v. Bowers*, 2023 WI App 4, ¶22, 405 Wis. 2d 716, 985 N.W.2d 123 (collecting cases). That is why the United States Supreme Court concluded, for example, that a warrantless search of a shared office at a union local violated the Fourth Amendment. *See Mancusi v. DeForte*, 392 U.S. 364, 369, 88 S. Ct. 2120, 20 L. Ed. 2d 1154 (1968). Even though the defendant shared the office with others, and thus did not have a reasonable expectation of privacy with respect to those individuals, he still had a reasonable expectation of privacy against a warrantless search of that office by the government. *See id.*

¶76 These same principles should apply with equal force in the digital setting of this case. *See State v. Baric*, 2018 WI App 63, ¶19, 384 Wis. 2d 359, 919 N.W.2d 221 (emphasizing that “the reasonableness of an expectation of privacy in digital files . . . on electronic platforms is determined by considering the same factors as in any other Fourth Amendment context”). Because breaches of private agreements in the real world do not eliminate renters’ or users’ reasonable expectations of privacy against government intrusion, it is irrelevant that Gasper breached Snapchat’s terms of service when he privately uploaded the video to his account. *Compare Byrd*, 584 U.S. at 408; *Thomas*, 65 F.4th at 923–25; and *Cunag*, 386 F.3d at 895; *with Gasper*, 414 Wis. 2d 532, ¶¶18, 21–25. Snapchat’s contractual right to, for example, delete his account or the video for breaching the terms of service says nothing about whether the government could search

*Appendix A*

the video without a warrant. *See Thomas*, 65 F.4th at 924. And the fact that Snapchat’s terms stated it could search Gasper’s account and would report CSAM it found to law enforcement is similarly irrelevant. *See Gasper*, 414 Wis. 2d 532, ¶¶17–18. That is because granting a private party the contractual right to access an otherwise private space doesn’t mean the government can access that same space without first obtaining a warrant. *See Warshak*, 631 F.3d at 287; *Bowers*, 405 Wis. 2d 716, ¶22. Thus, even though the terms of service put Gasper on notice that Snapchat might turn over his files to the government, “the mere *ability* of a third-party intermediary to access the contents of a [file] cannot be sufficient to extinguish a reasonable expectation of privacy.” *See Warshak*, 631 F.3d at 286 (emphasis in original).

¶77 The court of appeals’ holding to the contrary would severely undermine individuals’ privacy online. After all, if an electronic service provider’s terms of service can eliminate a user’s reasonable expectations of privacy in their digital files, then that means the government is free to access those files without obtaining a warrant and without implicating the Fourth Amendment. *See United States v. Jones*, 565 U.S. 400, 406, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012).

¶78 If that sounds alarming, that’s because it is. Social-media platforms like Snapchat are an omnipresent part of modern society. Over the last few decades, these platforms have transformed communication, supplanting older technologies. On Snapchat, users can send photos, videos, or messages instantly to friends, family, or

*Appendix A*

strangers around the world. Those messages can contain anything from intimate private details about a user’s life to funny cat videos. And that is equally true on Facebook, Instagram, and countless other social-media sites. If the voluminous, highly detailed, and broad terms of service imposed by these sites as a condition of creating an account “can narrow or eliminate Fourth Amendment rights online, then those rights may be an illusion. What the Supreme Court has given, [t]erms of [s]ervice might take away.” Kerr, *Terms of Service, supra* at 289.

¶179 Correctly understood, however, terms of service have little or no relevance to Fourth Amendment rights. They have at best limited bearing on consent to search. *See State v. Kieffer*, 217 Wis. 2d 531, 542, 577 N.W.2d 352 (1998) (describing the third-party consent doctrine). After all, the right to consent depends not “upon the law of property”—something the terms might demonstrate—but instead on actual shared use and control, which terms of service cannot establish on their own. *See United States v. Matlock*, 415 U.S. 164, 171 n.7, 94 S. Ct. 988, 39 L. Ed. 2d 242 (1974). Likewise, terms of service are only tangentially relevant to the private-search doctrine. For example, terms of service might be a minor point on the scale, helping to show whether an electronic service provider was acting as a private party or an agent of the government when it searched a user’s account. *See United States v. Rosenow*, 50 F.4th 715, 730 (9th Cir. 2022). But as with consent to search, the application of the private-search doctrine hinges on far more than just terms of service. *See generally id.* at 728–35.

*Appendix A*

¶180 What terms of service cannot do, however, is eliminate or even limit a user’s reasonable expectations of privacy online vis-à-vis a government search. To hold otherwise, as the court of appeals did in this case, is to make citizens’ Fourth Amendment rights online rise and fall on the whim of tech companies and large corporations. These important rights are, and must remain, more resilient than that.

**II**

¶181 Although the majority rightly vacates the court of appeals’ published opinion, unfortunately its decision erodes Fourth Amendment rights in different way. As Justice Crawford’s separate writing correctly explains, Gasper’s Fourth Amendment rights were violated when, without obtaining a warrant, a Wisconsin DOJ analyst viewed for the first time a video privately uploaded to Gasper’s Snapchat account. In concluding otherwise, the majority misapplies the private-search doctrine, holding that it was “virtual[ly] certain[.]” that by viewing the video for the first time, the analyst “would not find anything of significance beyond what” was already revealed by Snapchat’s prior private search. *See* majority op., ¶16; *see also United States v. Jacobsen*, 466 U.S. 109, 119, 104 S. Ct. 1652, 80 L. Ed. 2d 85 (1984). But that private search was limited in scope, scanning only the video’s hash value—“a sort of digital fingerprint”<sup>5</sup> for computer files—and identifying it as a match for the hash value of

---

5. *United States v. Ackerman*, 831 F.3d 1292, 1294 (10th Cir. 2016) (citing Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 38–40 (2005)).

*Appendix A*

an image or video previously flagged as containing CSAM. The hash match alone, however, “revealed nothing, either to [Snapchat] or those with whom it shared the match, about what in particular the [video] depicted (or even what the [file it matched to] depicted).” *United States v. Maher*, 120 F.4th 297, 306 (2d Cir. 2024). And for that reason, the analyst’s actions exceeded the scope of Snapchat’s prior private search.

¶82 In arguing otherwise, Justice Hagedorn’s concurrence illustrates the pitfalls inherent in analogizing Snapchat’s hash-value search to other contexts. To begin with, he relies on a real-world case in which individuals took private documents and turned them over to law enforcement. *See* Justice Hagedorn’s concurrence, ¶100 (citing *Burdeau v. McDowell*, 256 U.S. 465, 475, 41 S. Ct. 574, 65 L. Ed. 1048 (1921)). But in that case, law enforcement didn’t have to open a sealed envelope or other container to view the documents, their contents were plain for anyone to see.<sup>6</sup> *See* *United States v. Knoll*, 16 F.3d 1313, 1320–21 (2d Cir. 1994) (explaining that a warrant is

---

6. This was equally true in the other case Justice Hagedorn’s concurrence cites, *United States v. Simpson*, 904 F.2d 607, 610 (11th Cir. 1990). There, a private party opened a box containing magazines and videotapes, viewed the tapes, and turned them over to law enforcement. *See id.* at 608–09. Because “[t]he box’s contents had already been examined, their illicit character had been determined, and they were open for viewing by the time the Assistant United States Attorney and the F.B.I. Agent arrived on the scene,” law enforcement’s actions in that case clearly fell within the scope of the private-search doctrine. *Id.* at 610. Unlike in *Simpson*, no private party viewed the video at issue in this case before the DOJ analyst.

*Appendix A*

required for law enforcement to examine stolen files sealed in folders and boxes). That is not true in this case, however, where the only way to know the complete contents of the digital video was to open the file and view it.

¶183 Nevertheless, Justice Hagedorn’s concurrence relies on this real-world case in comparing Snapchat’s actions to a private party’s hypothetical “keyword search of . . . emails” for the name of a bank with known ties to organized crime. *See* Justice Hagedorn’s concurrence, ¶199. The hypothetical keyword search turns up five emails, which the searcher reads enough to confirm “they all contain the name of the shady bank.” *Id.* The searcher then prints them out, and hands them over to the police. *See id.* What this example proves is anyone’s guess, however, since the hypothetical bears virtually no resemblance to the facts of this case. Unlike the concurrence’s hypothetical searcher, who visually examined each email to confirm it contained the potentially incriminating information (thus invading any expectation of privacy the account holder might have had), no one at Snapchat viewed the video before it was opened by law enforcement. Moreover, unlike the unopened video file attached to the CyberTip, the hypothetical printed-out emails revealed their contents for anyone to see. In the end, all this hypothetical demonstrates is the problem with relying too heavily on real-world analogies in the digital context. As the United States Supreme Court has cautioned, such an approach results at best in “a difficult line-drawing expedition to determine which digital files are comparable to physical records,” and at worst in “a significant diminution of privacy.” *See Riley v. California*, 573 U.S. 373, 400–01, 134 S. Ct. 2473, 189 L. Ed. 2d 430 (2014).

*Appendix A*

¶84 Perhaps for that reason, Justice Hagedorn’s concurrence abandons this argument to articulate a “second way this case can be resolved,” namely “by following the analysis in the field test portion of [*United States v.*] *Jacobsen*.” Justice Hagedorn’s concurrence, ¶104. In *Jacobsen*, the United States Supreme Court held that even though DEA agents exceeded the scope of a prior private search when they performed a field test on white powder discovered in a package, that test did not violate the Fourth Amendment. *See* 466 U.S. at 123. That was so, the Court explained, because the binary nature of the test, which could reveal only whether the powder was or was not cocaine, “does not compromise any legitimate interest in privacy.” *Id.* The same result should follow here, Justice Hagedorn’s concurrence asserts, because “[a]ny additional invasion of Gasper’s reasonable expectation of privacy in this video was small to non-existent” since “its contents had already been searched and it had already been flagged for illegal CSAM.” Justice Hagedorn’s concurrence, ¶104.

¶85 This reading of *Jacobsen* is a novel one, in that it treats Snapchat’s actions—limited in scope as they were—as conclusive of whether Gasper had any remaining expectation of privacy in the video. But *Jacobsen* did not focus on what the FedEx employees did, or the scope of their search. Instead, the Court focused on the fact that the field test could reveal *only* “whether a substance is cocaine, and no other arguably ‘private’ fact.” *See Jacobsen*, 466 U.S. at 123. Accordingly, the federal courts have, with one exception, rejected arguments like the

*Appendix A*

one Justice Hagedorn’s concurrence makes.<sup>7</sup> Visually examining a file flagged as containing CSAM reveals all of the contents of that video, and thus “is a far cry from a field test’s disclosure of nothing more than a binary answer.” *Maier*, 120 F.4th at 316. Such a visual examination “reveals innumerable granular private details,” and thus “implicat[es] privacy interests beyond a binary classification.” *United States v. Wilson*, 13 F.4th 961, 979 (9th Cir. 2021). Therefore, I conclude that Gasper still had a reasonable expectation of privacy in the video even after Snapchat’s private search, and join the portion of Justice Crawford’s separate writing explaining why the events in this case violated the Fourth Amendment. *See* Justice Crawford’s concurrence in part and dissent in part, ¶¶113–24.

**III**

¶86 When evidence is obtained in violation of the Fourth Amendment, the typical remedy is to exclude evidence obtained through that unlawful search. *See State v. Blackman*, 2017 WI 77, ¶68, 377 Wis. 2d 339, 898 N.W.2d 774. Nevertheless, the exclusionary rule is not automatic, and should be applied only when doing so would yield “appreciable deterrence.”<sup>8</sup> *Davis v. United States*,

---

7. *See, e.g., Maier*, 120 F.4th at 315–16; *United States v. Wilson*, 13 F.4th 961, 978–79 (9th Cir. 2021); *United States v. Miller*, 982 F.3d 412, 429 (6th Cir. 2020); *Ackerman*, 831 F.3d at 1305–06; *but see United States v. Reddick*, 900 F.3d 636, 639 (5th Cir. 2018)

8. We could, of course, impose additional requirements on the application of the good-faith exception under the Wisconsin

*Appendix A*

564 U.S. 229, 237, 131 S. Ct. 2419, 180 L. Ed. 2d 285 (2011) (quoting another source).

¶187 To that end, the Supreme Court has applied the “good-faith exception” to the exclusionary rule, which recognizes that when law enforcement’s conduct is less culpable, applying the exclusionary rule is less likely to lead to meaningful deterrence. *Id.* at 238 (quoting *Herring v. United States*, 555 U.S. 135, 143, 129 S. Ct. 695, 172 L. Ed. 2d 496 (2009) (internal alteration omitted)). If law enforcement acts “in objectively reasonable reliance on . . . a facially valid warrant properly issued by a neutral, detached magistrate; an apparently constitutional statute; or a binding appellate precedent,” applying the exclusionary rule is not warranted. *State v. Burch*, 2021 WI 68, ¶179, 398 Wis. 2d 1, 961 N.W.2d 314 (Dallet, J., concurring in part, dissenting in part) (citing *United States v. Leon*, 468 U.S. 897, 104 S. Ct. 3405, 82 L. Ed. 2d 677 (1984); *Illinois v. Krull*, 480 U.S. 340, 107 S. Ct. 1160, 94 L. Ed. 2d 364 (1987); *Davis*, 564 U.S. at 239–41). By contrast, when law enforcement demonstrates “‘deliberate,’ ‘reckless,’ or ‘grossly negligent’ disregard for Fourth Amendment rights,” the exclusionary rule should apply to deter that misconduct. *See Davis*, 564 U.S. at 238 (quoting *Herring*, 555 U.S. at 144); *see also Burch*, 398 Wis. 2d 1, ¶180 (Dallet, J., concurring in part, dissenting in part).

---

Constitution. *See State v. Eason*, 2001 WI 98, ¶74, 245 Wis. 2d 206, 629 N.W.2d 625. Gasper did not make an argument under the Wisconsin Constitution for limiting the good-faith exception in this situation, however, and I therefore apply only the standards applicable under the United States Constitution.

*Appendix A*

¶188 Some situations, like the one in this case, fall between those two poles. And when that happens, courts must assess the situation’s unique facts, weighing the costs of suppression against the deterrence benefits of exclusion in light of “the ‘flagrancy of the police misconduct’ at issue.” *Davis*, 564 U.S. at 238 (quoting *Leon*, 468 U.S. at 909). In other words, applying the good-faith exception requires much more than the broad, legally incorrect, and conclusory statement in Justice Ziegler’s concurrence that “[w]hen police act in good faith, or an area of the law is unsettled, there is no police misconduct to deter.” Justice Ziegler’s concurrence, ¶160.

¶189 Here’s what the good-faith-exception analysis should look like. At the time the DOJ analyst viewed for the first time the video privately uploaded to Gasper’s Snapchat account, the Fifth and Sixth Circuits held that a warrant was not required before doing so under the private-search doctrine. *See, e.g., United States v. Miller*, 982 F.3d 412, 426–34 (6th Cir. 2020); *United States v. Reddick*, 900 F.3d 636, 638–40 (5th Cir. 2018). Two state courts reached the same conclusion. *See, e.g., People v. Wilson*, 56 Cal. App. 5th 128, 270 Cal. Rptr. 3d 200, 220–25 (Cal. Ct. App. 2020); *Morales v. State*, 274 So. 3d 1213, 1217–18 (Fla. Ct. App. 2019). The Ninth Circuit disagreed, however, holding that a warrant was required.<sup>9</sup> *See Wilson*,

---

9. Subsequently, the Second Circuit’s decision in *Maher* joined *Wilson*’s side of this split of authority. *See generally Maher*, 120 F.4th 297. Nonetheless, that case was not decided until after this case was on appeal, and thus is not relevant to evaluating whether to apply the exclusionary rule. *Cf. Davis*, 564 U.S. at 240–41.

*Appendix A*

13 F.4th at 964. According to testimony at the suppression hearing in this case, attorneys at DOJ analyzed this split of authority and concluded that a warrant was not required before law enforcement in Wisconsin opened for the first time a file allegedly containing CSAM that was attached to a CyberTip.

¶90 As I have written before, in the face of uncertainty, law enforcement should of course “err on the side of constitutional behavior’ and get a warrant.” *Burch*, 398 Wis. 2d 1, ¶83 (Dallet, J., concurring in part, dissenting in part) (quoting another source). Had they done so here, years of appellate proceedings could have been avoided at virtually no cost, since such a warrant would have been easy to obtain. Nevertheless, under these circumstances, I would not apply the exclusionary rule. Law enforcement’s actions here were not the kind of “deliberate,’ ‘reckless,’ or ‘grossly negligent’ disregard for Fourth Amendment rights” the exclusionary rule is needed to deter. *See Davis*, 564 U.S. at 238. Instead, law enforcement made a reasoned, though mistaken in my view, decision to follow the weight of non-binding authority on an unsettled legal question, as reflected in the decisions of two federal circuits and two state appellate courts. *See id.*; *see also United States v. Ford*, No 1:11-CR-42, 2012 U.S. Dist. LEXIS 155208, 2012 WL 5366049, at \*11 (E.D. Tenn. Oct. 30, 2012) (reaching a similar conclusion with respect to a 3-1 circuit split). Even though not all instances of law enforcement reliance on non-binding precedent will fall within the good-faith exception, this one does.

*Appendix A*

¶91 Accordingly, while I disagree with the majority's reasoning, I concur with its conclusion that Gasper's motion to suppress should have been denied. I therefore respectfully concur.

*Appendix A*

JUSTICE HAGEDORN, concurring

BRIAN K. HAGEDORN, J., with whom JILL J. KAROFSKY, C.J., and JANET C. PROTASIEWICZ, J., join, concurring.

¶192 Snapchat digitally scans its users' uploaded video content to see whether it contains known child sexual abuse material (CSAM). If it does, Snapchat flags the content and turns it over to law enforcement. In this case, Snapchat flagged a 16-second video as likely CSAM and forwarded it to law enforcement. When law enforcement received the video, they watched it—something no employee of Snapchat did. The main question in this case is whether law enforcement carried out an unreasonable search in violation of the Fourth Amendment when it watched the video. I agree with the majority that it did not. I write separately to add some additional context and analysis to this discussion.

¶193 Some basic Fourth Amendment principles guide our analysis. The Fourth Amendment generally prohibits a government search without a warrant when that search invades a reasonable expectation of privacy. *United States v. Jacobsen*, 466 U.S. 109, 113, 104 S. Ct. 1652, 80 L. Ed. 2d 85 (1984). Searches performed by private actors, however, are not government searches and therefore not subject to Fourth Amendment protections. *Id.*

¶194 What happens, though, if a private actor conducts a search and then turns over evidence to law enforcement? Must the government get a warrant to examine what a private party has already searched and provided? The

*Appendix A*

United States Supreme Court has said no; police need not “avert their eyes.” *Coolidge v. New Hampshire*, 403 U.S. 443, 489, 91 S. Ct. 2022, 29 L. Ed. 2d 564 (1971). In *Jacobsen*, the Supreme Court set out a broader principle governing police searches of evidence that has been turned over by a private party: “The additional invasions of respondents’ privacy by the Government agent must be tested by the degree to which they exceeded the scope of the private search.” *Jacobsen*, 446 U.S. at 115.

¶95 When a private actor conducts a search, the reasonable expectation of privacy has been frustrated. *Id.* at 117–18. Thus, as long as the subsequent government search does not exceed the scope of the private search, the government has not invaded any additional expectation of privacy. When a search merely replicates what the private actor did, no Fourth Amendment search occurs. *Id.* at 119–20. But *Jacobsen* also permits some searches that exceed the scope of the private party search if the additional infringement on the remaining interest in privacy is minimal. *Id.* at 124. Where the residual privacy interest is negligible, Fourth Amendment interests similarly do not justify the need for a warrant. *Id.* at 123.

¶96 *Jacobsen* applied this to two different searches by DEA (Drug Enforcement Administration) agents. For the first, DEA agents replicated what the private Federal Express employees had already done. They removed material found in the package that the employees had already opened and found a white powder. *Id.* at 111. In replicating this search, the DEA agents weren’t going to learn anything they didn’t already know, so they did not

*Appendix A*

infringe upon any further privacy interests that had not already been frustrated by the private search conducted by Federal Express employees. In the second search, DEA agents performed a field test on the white powder. *Jacobsen* initially observed that this search did exceed the scope of the prior search. *Id.* at 122. But the search was still reasonable under the Fourth Amendment because the likelihood that any legitimate interest in privacy would be compromised was “much too remote” to implicate the Fourth Amendment. *Id.* at 124. The additional invasion of privacy was small and unlikely to reveal any other “private’ fact.” *Id.* at 123. Given the virtual certainty that the test would reveal only whether the white powder was cocaine, an illegal contraband, the search was reasonable under the Fourth Amendment even though it exceeded the scope of the private search. Following this reasoning, our case can be resolved in two ways consistent with *Jacobsen*.

¶197 First, as the majority explains, the government search did not exceed the scope of the private party’s search. Snapchat, a private actor, conducted a digital search of the video—not just its label, but its contents. This means Gasper’s expectation of privacy in the contents of the video were frustrated. A human search of the video may be different in form, but not in kind. It is a search of what was in the video—just like the one conducted by Snapchat. Therefore, when the government watched the video, it did not exceed the scope of Snapchat’s private digital search. Moreover, it’s not even clear that law enforcement’s human viewing of the video should be thought of as any more invasive than the sophisticated search conducted by Snapchat—one that analyzes the

*Appendix A*

video by comparing pixels within the video to a database of known CSAM.

¶198 Justice Crawford disagrees and argues that when a human viewed the video, the government exceeded the scope of Snapchat’s search, analogizing this to a dog sniff alerting to narcotics in luggage at an airport. Justice Crawford’s concurrence/dissent, ¶123. Just as a warrant would be required to search the luggage after the dog alerts, Justice Crawford reasons, a warrant is required after a digital CSAM alert before police may watch the video. *Id.* I respectfully disagree.

¶199 Snapchat’s search was not external to the video in the way a dog sniff is external to luggage; it was a search of the video itself. The suitcase analogy falls short. A better way to view this is like a keyword search of emails. Suppose a woman suspects her husband is engaged in financial shenanigans and conducts a keyword search of his emails. She searches specifically for emails containing the name “Gambino Bank”—a local depository known for its ties to organized crime. The search locates five emails. She does not read the emails beyond her confirmation that they all contain the name of the shady bank. She then prints the emails and drops them off at the local police precinct, telling them that she believes these emails contain evidence that her husband is engaged in fraudulent financial activities.

¶100 The woman’s private search in this hypothetical is digital and depends on the content of the emails. Can law enforcement, upon receipt of the documents, read them

*Appendix A*

in full, or must they avert their eyes or obtain a warrant? Almost assuredly, courts would say law enforcement could read the emails. Indeed, in the seminal case establishing that the Fourth Amendment is not offended by a private party's search, the Supreme Court held that police can review documents turned over by private individuals and use them in a subsequent prosecution. *Burdeau v. McDowell*, 256 U.S. 465, 475–76, 41 S. Ct. 574, 65 L. Ed. 1048 (1921). The emails in my hypothetical have already been searched by the private actor, and reading the emails is no more invasive to a privacy interest than the keyword search, which likewise reviews each word and phrase. While law enforcement's examination of the incriminating emails may be different in form from the woman's keyword search, it is not different in kind.

¶101 The same logic should apply to the short video at issue here. Snapchat's digital search of the contents of the video is a real search, and law enforcement may permissibly search the contents of the video using a different method—here, watching it rather than conducting another digital scan. Under *Jacobsen* this is not an expanded search. Rather, given the frustration of any remaining privacy interests in the contents of the video, it remains within the scope of the private search.

¶102 One of the complications in this type of case is *Jacobsen*'s focus on what one might learn from a search, which is rooted in the Supreme Court's jurisprudence regarding the search of a container. *Jacobsen* focuses on whether the law enforcement's subsequent search is “virtually certain” to result in learning more than law

*Appendix A*

enforcement already knew. It is not clear to me that this focus is equally illuminating in digital searches or when the potential criminal activity is more complex. I can imagine all kinds of circumstances where law enforcement is sure to learn more than a private actor even while conducting the exact same search. A private actor suspecting financial fraud, for example, is unlikely to notice all that a trained law enforcement officer would see when replicating the private party's search. And doctrinally, the private search doctrine rests upon whether the scope of the search has been exceeded, not whether law enforcement notices more than the private actor. *See United States v. Simpson*, 904 F.2d 607, 610 (11th Cir. 1990) (reasoning the government's search does not expand upon the private party's search "simply because they took more time and were more thorough than [the private party]"). For this reason, I'm not sure the emphasis on "virtual certainty" is as helpful in light of the kind of search we are examining here.

¶103 The real question from *Jacobsen* would seem to be whether the defendant's privacy interest was frustrated. Here, the whole video was searched by Snapchat, even though Snapchat did not have a human watch the video. In my view, the expectation of privacy in the video was frustrated by Snapchat's digital viewing of the video, which means law enforcement doesn't exceed the scope of the private search by also viewing the video—albeit in a different manner.

¶104 The second way this case can be resolved is by following the analysis in the field test portion of *Jacobsen*. To the extent this search exceeds the scope of

*Appendix A*

the PhotoDNA hash search performed by Snapchat, we still must ask how much of a remaining expectation of privacy Gasper had in the video after Snapchat's search. The answer is not much. Gasper had little expectation of privacy remaining in the contents of this 16-second video after its contents had already been searched and it had already been flagged for illegal CSAM. Here, to the extent watching the video is deemed an additional government search by exceeding the scope of Snapchat's digital search, it isn't much of one. Any additional invasion of Gasper's reasonable expectation of privacy in this video was small to non-existent, and I would conclude it was insignificant—just like the field test in *Jacobsen*.

¶105 For these reasons, I respectfully concur.

*Appendix A*

JUSTICE CRAWFORD, concurring in part  
and dissenting in part.

SUSAN M. CRAWFORD, J., with whom REBECCA FRANK DALLEY, J., joins with respect to ¶¶113–124, concurring in part and dissenting in part.

¶106 Although the government’s interests in protecting children from sexual abuse and exploitation and holding perpetrators accountable are unquestionably compelling, those interests do not excuse the government from following the basic commands of the Constitution. Here, the Fourth Amendment required the government to obtain a search warrant before opening and viewing Michael Gasper’s Snapchat file.

¶107 Many electronic service providers (ESPs) digitally monitor their platforms for harmful content and voluntarily share suspected child sexual abuse materials (CSAM) with the government, as Snapchat did here. When the State opened and viewed the video file it received from Snapchat, it acquired information beyond what was detected by Snapchat’s digital scan. The State utilized that additional information—a detailed description of the contents of the video—when it applied for a search warrant for Gasper’s home and cell phone. The State should have, and readily could have, obtained a search warrant before viewing the video file it received from Snapchat. It chose not to do so. The State’s deliberate decision to open and view the file without first obtaining a search warrant cannot be excused as good faith. I would affirm the circuit court’s order suppressing the evidence the State obtained

*Appendix A*

by opening and viewing the file, specifically the content of that video. I conclude, however, that the remaining facts gained from the CyberTip and investigation were sufficient to support probable cause for the search warrant of Gasper's home and devices. I thus agree with the mandate reversing the circuit court's order suppressing evidence obtained pursuant to the search warrant.

¶108 For these reasons, I concur in part and dissent in part.

**I. BACKGROUND**

¶109 This case represents an increasingly common fact pattern as courts grapple with the Fourth Amendment rights of citizens who store photos, videos, and other data in password-protected ESP accounts in "the cloud" (remote servers in data centers maintained by ESPs). In a routine scan, Snapchat's software detected potential CSAM in a video file Gasper had uploaded and saved to his personal Snapchat account. Without opening or viewing the flagged file, Snapchat emailed a CyberTip with the attached video to the National Center for Missing and Exploited Children (NCMEC). The CyberTip included the Snapchat user name, as well as the email address and IP address attached to the account. NCMEC determined that the device associated with the IP address was located in Wisconsin and was served by CenturyLink. NCMEC then emailed the CyberTip and the additional information to the Wisconsin Department of Justice (DOJ).

*Appendix A*

¶110 A DOJ employee opened and viewed the video attached to the CyberTip without obtaining a search warrant. After viewing the video, the DOJ employee obtained the name and address associated with the IP address from CenturyLink under an administrative subpoena. The employee forwarded the video file, along with Gasper's name and home address, to the Waukesha County Sheriff's Department (Sheriff's Department). Upon receipt, a detective viewed the video, again without first obtaining a search warrant. The detective then applied for and received a warrant to search Gasper's home and devices. The warrant affidavit included a detailed description of the content of the video to support a finding of probable cause.

**II. REASONABLE EXPECTATION OF PRIVACY**

¶111 A defendant challenging a search on Fourth Amendment grounds bears the burden of proving "that he or she had an actual, subjective expectation of privacy in the area search and item seized" and "that society is willing to recognize the defendant's expectation of privacy as reasonable." *State v. Tentoni*, 2015 WI App 77, ¶7, 365 Wis. 2d 211, 871 N.W.2d 285.

¶112 The majority does not reach the question of whether Gasper had a reasonable expectation of privacy in the video file because it concludes that the State's opening of the file and viewing the video did not exceed the scope of Snapchat's "private search," and thus does not implicate the Fourth Amendment. I disagree with the majority's conclusion that the State's actions did not exceed the scope

*Appendix A*

of Snapchat’s digital scan, as discussed below. I would also hold that the court of appeals erred in concluding that Gasper did not have a reasonable expectation of privacy in the video file because his “conduct was obviously unlawful” and contrary to Snapchat’s terms of service. *State v. Gasper*, 2024 WI App 72, ¶22, 414 Wis. 2d 532, 16 N.W.3d 279. I agree with Justice Dallet that Gasper had a reasonable expectation of privacy in files he placed in his password-protected Snapchat account, and that Snapchat’s specific terms of service did not extinguish that expectation of privacy. I join her concurrence on that issue. *See* Justice Dallet’s concurrence, ¶¶67–80.

**III. THE PRIVATE SEARCH DOCTRINE**

¶113 “[T]he Fourth Amendment applies only to government action.” *State v. Payano-Roman*, 2006 WI 47, ¶17, 290 Wis. 2d 380, 714 N.W.2d 548. If the government repeats a search conducted by a private party, “[t]he Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated.” *United States v. Jacobsen*, 466 U.S. 109, 117, 104 S. Ct. 1652, 80 L. Ed. 2d 85 (1984). Whether government agents have committed additional invasions of the defendant’s privacy “must be tested by the degree to which they exceeded the scope of the private search.” *Id.* at 115. The majority holds that the State did not exceed the scope of Snapchat’s private search here. In their view, the DOJ and Sheriff’s Department merely duplicated Snapchat’s digital scan when they opened and viewed the video. But no Snapchat employee had viewed the video; nor did the government simply replicate Snapchat’s digital scan of Gasper’s file. If either had done so, this would be an easy case with no

*Appendix A*

violation of the Fourth Amendment. Unfortunately, that's not what happened here.

¶114 *Jacobsen* held that when the government's inspection reveals "nothing else of significance" beyond what was disclosed to it by a private party, no legitimate privacy interest protected under the Fourth Amendment is infringed. *Id.* at 119 (holding that a DEA agent's inspection of a package that FedEx employees had previously opened, disclosing bags of white powder, did not further infringe the defendant's privacy interests). The government here knew only that Snapchat had flagged the file as "apparent CSAM" after conducting a digital scan. It did not know what specimen of "known CSAM" Snapchat's scan had determined to digitally match Gasper's file. Nor did the government have a description of the content of the video. Until government agents opened and viewed the file, the State did not know if the file contained an intact video or if it depicted CSAM as defined by state law. See Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 40 (2005) (explaining that the hash value of a digital file "cannot be 'reversed'" to reveal the content of the file itself). Only by opening and playing the file did the government confirm it contained an intact video that was unequivocally CSAM. The detective's inclusion of a detailed description of the video in the search warrant affidavit underscores the investigative value of the evidence obtained by opening the file. It is simply not true that "nothing else of significance" was disclosed by viewing the video.<sup>1</sup>

---

1. In this case, the government's viewing of the file confirmed what it suspected: that the defendant possessed CSAM. But it is

*Appendix A*

¶115 *Jacobsen* teaches that the government’s search does not exceed the scope of a private search if it did not learn anything beyond what it could have obtained from the private searcher’s testimony. 466 U.S. at 118–20; *see also United States v. Runyan*, 275 F.3d 449, 461 (5th Cir. 2001). That obviously is not the case here. The detective’s search warrant affidavit, which includes a detailed description of the video, shows that the government obtained information useful to the prosecution by viewing the video. No Snapchat employee could have provided that information through testimony.

¶116 The majority incorrectly distinguishes the present case from *Walter*, an earlier case discussed at length in *Jacobsen*. *See Walter v. United States*, 447 U.S. 649, 651–52, 100 S. Ct. 2395, 65 L. Ed. 2d 410 (1980). Employees opened packages misdelivered to a company, discovering boxes of films labeled with suggestive drawings and explicit descriptions of the contents. *Id.* An employee attempted to view the films by holding them up to the light,

---

not hard to imagine scenarios in which the government’s viewing of a video flagged as CSAM by a digital scan would uncover additional criminal activity, such as when a video depicts the defendant engaging in sexual activity with a child or depicts a child known to the defendant. *See, e.g., United States v. Runyan*, 275 F.3d 449 (5th Cir. 2001) (officers’ searches of photos on defendant’s laptop and disks revealed evidence that he sexually exploited a child by producing CSAM); *see* WIS. STAT. §§ 948.02 (sexual assault of a child), 948.05 (sexual exploitation of a child, including producing CSAM), 948.051 (trafficking of a child), 948.07 (child enticement). Gasper himself was charged with nine counts of sexual exploitation of a child for distributing videos later found on his cell phone pursuant to the search warrant.

*Appendix A*

but was not successful. *Id.* Government agents viewed the films without a warrant. *Id.* The Court explained that “[p]rior to the Government screening one could only draw inferences about what was on the films.” *Id.* at 657. As such, “[t]he projection of the films was a significant expansion of the search that had been conducted previously by a private party and therefore must be characterized as a separate search. That separate search was not supported . . . by a warrant even though one could have easily been obtained.” *Id.* Like the company employees in *Walter*, Snapchat’s employees did not open or view the video file that its software flagged as “apparent CSAM.” Nor did NCMEC view the video. The video was not observable until government actors opened and played the file using an appropriate software program.<sup>2</sup> *Cf. Walter*, 447 U.S. at 652 n.2 (explaining that the films could not “be examined successfully with the naked eye” due to their size). The majority attempts to distinguish *Walter* by stressing that it took federal agents months to review the hundreds of boxes of film. But neither the duration of the search nor the number of files examined have constitutional relevance. As in *Walter*, the government’s viewing of the previously-unseen video expanded the private search, disclosing more information about the content of the file. Like the federal agents in *Walter*, the State could easily have obtained a

---

2. A video file, in basic terms, is a string of digital code that can be processed by a computer or other device, using a compatible program, to display a video. The contents of the file cannot be observed with the naked eye. *See generally* Catherine Guthrie & Brittan Mitchell, *The Swinton Six: The Impact of State v. Swinton on the Authentication of Digital Images*, 36 STETSON L. REV. 661, 662 (2007).

*Appendix A*

search warrant before opening the file and viewing the video. It chose not to.

¶117 The federal courts differ on what the Fourth Amendment requires in cases like Gasper’s, where the government opens and views a file flagged by an ESP’s digital scan without first obtaining a search warrant. The Ninth and, most recently, the Second Circuit have held that the government’s conduct is an unconstitutional expansion of the private search. *See United States v. Wilson*, 13 F.4th 961, 972 (9th Cir. 2021) (“[T]he government search . . . expanded the scope of the antecedent private search because the government agent viewed Wilson’s email attachments even though no Google employee—or other person—had done so, thereby exceeding any earlier privacy intrusion.”); *United States v. Maher*, 120 F.4th 297, 320 (2d Cir. 2024) (“Because no one at Google had ever opened or visually examined the contents of the Maher file . . . , such a visual examination by the police did not fall within the private search doctrine’s exception to the warrant requirement.”).

¶118 The Fifth and Sixth Circuits have held that the private search doctrine does apply when government agents conduct a warrantless viewing of the contents of an unopened file attached to a CyberTip. *See United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018); *United States v. Miller*, 982 F.3d 412 (6th Cir. 2020). They focus on the perceived reliability of the digital scan and gloss over the additional information government agents stand to gain by viewing the contents of the files. *See Reddick*, 900 F.3d at 639 (stating that viewing the file “merely dispelled any

*Appendix A*

residual doubt about the contents of the files,” similar to the agent’s field testing of the white powder in *Jacobsen*); *Miller*, 982 F.3d at 429–30 (stating that it was “virtually certain” viewing the files would reveal CSAM).

¶119 Unlike the majority, I find the federal cases holding that the government’s conduct exceeds the private search to be persuasive and in alignment with *Jacobsen*. The digital scans conducted by ESPs provide only a binary determination that a file falls within a category of contraband, and even then, the classification is a tentative one: that a file is *potential* CSAM. Only the officers’ subsequent viewing of the video confirmed that the file contained intact CSAM and, in this case, disclosed the unambiguously illegal nature of the content under Wisconsin law. *Cf. Wilson*, 13 F.4th at 973 (“Until he viewed the images, they were at most ‘suspected’ child pornography. . . . Only by viewing the images did the government confirm, and convey to the fact finder in Wilson’s criminal case, that they depicted child pornography under the applicable federal standard.”); *Maher*, 120 F.4th at 316 (“[A] human visual examination of a computer hash matched image does not disclose only whether or not the image depicts child pornography. Visual examination necessarily also reveals the particulars supporting either a ‘yes’ or ‘no’ answer.”).

¶120 Moreover, even assuming an ESP’s hash-value scanning is highly reliable and accurate in identifying CSAM, that reliability does not dispense with the Fourth Amendment’s warrant requirement. “[T]he reliability of [an ESP’s] hash matching technology is pertinent to

*Appendix A*

whether probable cause could be shown to obtain a warrant, not to whether the private search doctrine precludes the need for the warrant.” *Maher*, 120 F.4th at 319–20 (citation modified); *see also United States v. Braun*, 798 F. Supp. 3d 916, 925 (E.D. Wis. 2025) (quoting and relying on *Maher* in holding that a search warrant is required for officers to view an unopened file in a CyberTip). A law enforcement officer may, for example, have highly reliable information about the presence of drugs in a home; but the reliability of that information does not justify a warrantless entry and search. “Incontrovertible testimony of the senses that an incriminating object is on premises belonging to a criminal suspect may establish the fullest possible measure of probable cause. But even where the object is contraband, this Court has repeatedly stated and enforced the basic rule that the police may not enter and make a warrantless seizure.” *Horton v. California*, 496 U.S. 128, 137 n.7, 110 S. Ct. 2301, 110 L. Ed. 2d 112 (1990).

¶121 The majority here, along with Justice Hagedorn’s concurrence, similarly misapplies the *Jacobsen* Court’s analysis of the federal agent’s field testing of the white powder discovered by the FedEx employees. The Court conceded that the field test “exceeded the scope of the private search,” but held that the warrantless test did not compromise any legitimate expectation of privacy protected under the Fourth Amendment. 466 U.S. at 122–23. The Court emphasized that the test would “merely disclose[] whether or not a particular substance [was] cocaine.” *Id.* at 123. It implied that the contraband nature of the substance was already in plain view, stating that “[i]t is probably safe to assume that virtually all of the

*Appendix A*

tests conducted under circumstances comparable to those disclosed by this record would result in a positive finding” and that it was “virtually certain” that the substance was contraband. *Id.* at 123, 125. The Court thus focused its analysis not on the search, but the seizure: the test destroyed a trace amount of the powder, “convert[ing] what had been only a temporary deprivation of possessory interests into a permanent one.” *Id.* at 124–25. It concluded that because the test had “a *de minimis* impact on any protected property interest,” and because the law enforcement interests were substantial, the field test was a reasonable seizure under the Fourth Amendment. *Id.* at 125.

¶122 By contrast, the video contained in Gasper’s file was not in view when the government received it; nor was viewing the video equivalent to the chemical testing of an obviously contraband white powder.<sup>3</sup> “A visual examination’s revelation of particulars is a far cry from a field test’s disclosure of nothing more than a binary answer.” *Maher*, 120 F.4th at 316. *See also Wilson*, 13 F.4th at 978–79; *Miller*, 982 F.3d at 429 (concluding that the private search doctrine supported the government’s

---

3. Justice Hagedorn’s hypothetical about a woman conducting a keyword search on her spouse’s emails and handing printed copies of the emails to the police is readily distinguishable on this point. Unlike a digital file, the printed emails place the incriminating evidence in plain view. Law enforcement officers, upon being handed such emails, need not “avert their eyes.” *Coolidge v. New Hampshire*, 403 U.S. 443, 489, 91 S. Ct. 2022, 29 L. Ed. 2d 564 (1971). Justice Dallet makes a similar point in her concurrence. *See* Justice Dallet’s concurrence, ¶183.

*Appendix A*

warrantless viewing but rejecting the Fifth Circuit’s reasoning from *Reddick* “that the detective’s viewing of the images was like the DEA agent’s testing of the powder in *Jacobsen*”). The Court’s focus on the loss of property caused by testing the powder likewise has no parallel here.

¶123 The *Jacobsen* Court compared the field test to a trained canine alerting to the scent of narcotics in luggage at an airport, observing that both disclose “only the presence or absence of narcotics, a contraband item.” 466 U.S. at 123–24 (quoting *United States v. Place*, 462 U.S. 696, 707, 103 S. Ct. 2637, 77 L. Ed. 2d 110 (1983)). Notably, however, *Place* held that a dog’s detection of narcotics in luggage did not provide probable cause for a prolonged seizure of the luggage. *See* 462 U.S. at 707. The Court described the dog sniff as “*sui generis*,” and explained, “We are aware of no other investigative procedure that is so limited both in the manner in which the information is obtained and in the content of the information revealed by the procedure.” *Id.* Snapchat’s digital scans likewise reveal limited information about the files it flags. As already noted, the government did not replicate the digital scan. It opened the file and viewed the video, exposing considerably more information of significance to the government. *See supra* note 2. Opening and inspecting a digital file is more akin to a government agent opening and rummaging through a suitcase (for which a search warrant is generally required, absent exigent circumstances) than to a canine sniff or a field test that can only indicate the presence of potential contraband.

¶124 In an era of rapidly-advancing technology, including the deployment of artificial intelligence tools that

*Appendix A*

collect and analyze vast amounts of data, the majority’s application of the private search doctrine creates troubling precedent. This court, in holding that opening the file and viewing the video was no different than Snapchat’s digital scan, sanctions greater government intrusion in reliance on private companies’ technological tools. Condoning warrantless government searches that surpass a commercial entity’s previous intrusion into places in which citizens reasonably expect privacy undermines the Fourth Amendment’s protections against unreasonable searches.

**IV. APPLICATION OF THE EXCLUSIONARY RULE**

¶125 The exclusionary rule excludes “evidence discovered during an unlawful search or seizure,” as well as “evidence discovered only because of what the police learned from the unlawful activity, also referred to as ‘fruit of the poisonous tree.’” *State v. Van Linn*, 2022 WI 16, ¶ 11, 401 Wis. 2d 1, 971 N.W.2d 478 (citing *State v. Knapp*, 2005 WI 127, ¶24, 285 Wis. 2d 86, 700 N.W.2d 899). The exclusionary rule applies to state court proceedings under the Due Process Clause of the Fourteenth Amendment. *See Mapp v. Ohio*, 367 U.S. 643, 81 S. Ct. 1684, 6 L. Ed. 2d 1081, 86 Ohio Law Abs. 513 (1961). Since *Mapp*, the U.S. Supreme Court over time has curtailed the circumstances in which the exclusionary rule applies, focusing narrowly on its value in deterring police misconduct. *See* Richard M. Re, *The Due Process Exclusionary Rule*, 127 HARV. L. REV. 1885, 1887 (2014). As we have recognized, the Court has held that the rule is properly applied only “to deter deliberate, reckless, or grossly negligent conduct, or in

*Appendix A*

some circumstances recurring or systemic negligence.” See *State v. Burch*, 2021 WI 68, ¶17, 398 Wis. 2d 1, 961 N.W.2d 314 (quoting *Herring v. United States*, 555 U.S. 135, 144, 129 S. Ct. 695, 172 L. Ed. 2d 496 (2009)).

**A. THE GOOD-FAITH EXCEPTION**

¶126 The U.S. Supreme Court has held that the exclusionary rule need not be applied to evidence obtained in violation of the Fourth Amendment when law enforcement officers relied, in objective good faith, on a judicially issued warrant or other apparent legal authority. See generally *United States v. Leon*, 468 U.S. 897, 104 S. Ct. 3405, 82 L. Ed. 2d 677 (1984). We likewise have adopted a good-faith exception to the exclusionary rule under Article I, Section 11 of the Wisconsin Constitution. See *State v. Eason*, 2001 WI 98, ¶¶73–74, 245 Wis. 2d 206, 629 N.W.2d 625.

¶127 The Supreme Court has applied the good-faith exception only under circumstances showing that officers reasonably relied on then-existing legal authority in conducting a search or seizure later deemed unconstitutional. The rule was originally applied to evidence obtained in objective good-faith reliance on a judicially issued warrant. See *Leon*, 468 U.S. at 922; *Massachusetts v. Sheppard*, 468 U.S. 981, 987–88, 104 S. Ct. 3424, 82 L. Ed. 2d 737 (1984); *Arizona v. Evans*, 514 U.S. 1, 16, 115 S. Ct. 1185, 131 L. Ed. 2d 34 (1995) (applying good-faith exception to evidence collected incident to an arrest under a quashed arrest warrant that remained active due to clerical error). This court has similarly

*Appendix A*

applied the good-faith exception to unconstitutionally obtained evidence when the police reasonably relied on a facially valid search warrant. *See Eason*, 245 Wis. 2d 206, ¶73.<sup>4</sup>

¶128 The Court has also applied the exception when the government demonstrated that officers had relied, in objective good faith, on other binding legal authority, such as a statute. *See Michigan v. DeFillippo*, 443 U.S. 31, 38, 99 S. Ct. 2627, 61 L. Ed. 2d 343 (1979) (applying good-faith exception to evidence discovered in a search incident to arrest for violating an ordinance later held to be unconstitutional); *Illinois v. Krull*, 480 U.S. 340, 349–50,

---

4. Notably, this court held that, under Article I, Section 11 of the Wisconsin Constitution, additional safeguards must be present for the good-faith exception to apply in the context of a search warrant:

We hold that where police officers act in objectively reasonable reliance upon the warrant, which had been issued by a detached and neutral magistrate, a good faith exception to the exclusionary rule applies. We further hold that in order for a good faith exception to apply, the burden is upon the State to show that the process used in obtaining the search warrant included a significant investigation and a review by either a police officer trained and knowledgeable in the requirements of probable cause and reasonable suspicion, or a knowledgeable government attorney.

*State v. Eason*, 2001 WI 98, ¶74, 245 Wis. 2d 206, 629 N.W.2d 625. I note that Gasper does not make any argument here urging this court to limit the scope of the good-faith exception under Article I, Section 11 of the Wisconsin Constitution.

*Appendix A*

107 S. Ct. 1160, 94 L. Ed. 2d 364 (1987) (applying good-faith exception to evidence obtained in an administrative search of vehicles in a wrecking lot pursuant to a statute later found unconstitutional).<sup>5</sup>

¶129 Most on point here, the Court has held that “[e]vidence obtained during a search conducted in reasonable reliance on binding precedent is not subject to the exclusionary rule.” *Davis v. United States*, 564 U.S. 229, 241, 131 S. Ct. 2419, 180 L. Ed. 2d 285 (2011). Justice Sotomayor took care to note: “This case does not present the markedly different question whether the exclusionary rule applies when the law governing the constitutionality of a particular search *is unsettled*.” *Id.* at 250 (Sotomayor, J., concurring) (emphasis added).

¶130 This court has similarly applied the good-faith exception to evidence obtained when officers conduct a search in reasonable reliance on clear and settled Wisconsin precedent, even if that precedent is later deemed unconstitutional by the U.S. Supreme Court. *See State v. Dearborn*, 2010 WI 84, ¶46, 327 Wis. 2d 252, 786 N.W.2d 97. Like Justice Sotomayor, the court cautioned that “under our holding today, the exclusionary rule is inappropriate only when the officer reasonably relies on *clear and settled precedent*. Our holding does not affect

---

5. On the other hand, the Supreme Court has repeatedly declined to apply the good-faith exception to searches conducted under the authority of a statute purporting to authorize a search without probable cause or a valid warrant. *See Michigan v. DeFillippo*, 443 U.S. 31, 39, 99 S. Ct. 2627, 61 L. Ed. 2d 343 (1979) (collecting cases).

*Appendix A*

the vast majority of cases where neither this court nor the United States Supreme Court have spoken with specificity in a particular fact situation.” *Id.* (emphasis added).

¶131 Other courts have reached the same conclusion. As one district court observed, “permitting officers to rely on non-binding precedent would allow officers to pick and choose what law to follow, and would not properly serve the deterrent function of the exclusionary rule.” *United States v. Robinson*, 903 F. Supp. 2d 766, 782–83 (E.D. Mo. 2012) (collecting cases), *aff’d*, 781 F.3d 453 (8th Cir. 2015). *See also United States v. Holmes*, 121 F.4th 727, 735 (9th Cir. 2024) (exception does not apply to agent’s warrantless view of file attached to CyberTip where “the legal landscape only made plausible the contention that [the agent’s] search fell within the scope of the private-search doctrine”); *Braun*, 798 F. Supp. 3d at 930 (declining to apply good-faith exception to officer’s warrantless view of unopened file attached to CyberTip and noting that “when the law is unsettled, officers should be encouraged to err on the side of obtaining a warrant, particularly where, as here, there is no exigency”). Put differently, crediting the government’s “good faith” when it relies on favorable non-binding authority in an unsettled area of law to justify its failure to obtain a search warrant, while it ignores adverse authority, undermines the purposes of the exclusionary rule. “[W]hile an officer may reasonably rely on firm, binding precedent, the *lack of binding precedent* is not evidence of good faith.” *Young v. State*, 394 So. 3d 1174, 1179–80 (Fla. Dist. Ct. App. 2024) (emphasis added). To say otherwise “would incentivize warrantless searches under unsettled areas of law, while the Fourth Amendment

*Appendix A*

requires a warrantless search to be specifically authorized by law.” *Id.* at 1183.

¶132 In this case, the government indisputably did not rely on settled precedent when it inspected Gasper’s file without first obtaining a search warrant. Moreover, it was aware that the federal circuit courts were divided on whether a search warrant is required under similar circumstances. *Compare Wilson*, 13 F.4th 961, with *Reddick*, 900 F.3d 636, and *Miller*, 982 F.3d 412. Instead of taking the course of action that would ensure it was acting constitutionally—applying for a search warrant—the government instead chose to risk violating Gasper’s rights. The State’s policy was to open and view all of the files attached to CyberTips without a search warrant, despite knowing full well that the law was unsettled. Applying the exclusionary rule here would serve the purpose of deterring the government’s deliberate choice to evade the warrant requirement. The good-faith exception should not be applied to reward the government’s strategic avoidance of its obligations under the Fourth Amendment.

¶133 The U.S. Supreme Court has made clear what police must do—and what the DOJ and Sheriff’s Department failed to do—before searching private data: “get a warrant.” *Riley v. California*, 573 U.S. 373, 403, 134 S. Ct. 2473, 189 L. Ed. 2d 430 (2014); *Carpenter v. United States*, 585 U.S. 296, 317, 138 S. Ct. 2206, 201 L. Ed. 2d 507 (2018). And in cases of doubt, this court’s own precedent mandates that the government choose the course of action that avoids a constitutional violation. *See Dearborn*, 327 Wis. 2d 252, ¶146; *see also Burch*, 398 Wis.

*Appendix A*

2d 1, ¶183 (Dallet, J., concurring in part, dissenting in part) (“[B]ecause the police may encounter circumstances that are on the margins of the law regarding warrant exceptions . . . police officers are required to ‘err on the side of constitutional behavior’ and get a warrant.”) (citation modified). There was no exigency compelling the government to risk a constitutional violation. Over 60 days passed between the DOJ’s initial receipt of the CyberTip and the Waukesha detective’s eventual application for a warrant to search Gasper’s home and devices. There was no exigency. The DOJ could have applied for and obtained a search warrant authorizing it to open and view the file. This task is a small price to pay to safeguard the rights protected by the Fourth Amendment.

**B. THE EVIDENCE OBTAINED UNDER THE SEARCH WARRANT**

¶134 “As applied to circumstances where an application for a warrant contains both tainted and untainted evidence, the issued warrant is valid if the untainted evidence is sufficient to support a finding of probable cause to issue the warrant.” *State v. Carroll*, 2010 WI 8, ¶44, 322 Wis. 2d 299, 778 N.W.2d 1. “To establish probable cause to search, the evidence must indicate a fair probability that the particular place contains evidence of a crime.” *Id.*, ¶28 (citation modified).

¶135 Thus, although I would hold that the contents of the Snapchat video were properly excluded due to the State’s failure to obtain a warrant to open and view it, the State had sufficient untainted evidence to establish

*Appendix A*

probable cause for the warrant to search Gasper's home and devices. The evidence seized pursuant to the search warrant, which includes all ten of the videos Gasper was charged with possessing, needs not have been suppressed.

¶136 The State argued that the results of Snapchat's digital scan—the “hash-value match”—can provide probable cause for a search warrant, even when the investigator does not view the flagged file. I agree, as have other courts. *See Maher*, 120 F.4th at 319 (holding that police could have relied on Google's hash-value match with known CSAM to “demonstrate probable cause to support warrants for [the government's] searches of Maher's Google accounts *and residence*”) (emphasis added); *United States v. Cartier*, 543 F.3d 442, 446 (8th Cir. 2008) (holding that hash-value match with known CSAM supported probable cause for search warrant of defendant's computer, even though no one had observed CSAM on the computer).

¶137 The CyberTip and other lawfully collected evidence (the name and birth date linked to Gasper's Snapchat account, the IP address, and his home address) would have provided probable cause for the issuance of a search warrant not only to view the video, but also to search Gasper's home and electronic devices for CSAM. It is probable that an individual who has placed a file in his ESP account has duplicate or original copies of the file on a cell phone or other device used to access the account (as explained in the affidavit, this is the case even if the files are deleted from the device). Thus, although the detailed description of the video in the search warrant affidavit

*Appendix A*

was highly probative in establishing probable cause, I conclude that the probable cause standard was met even without that description. Because the evidence obtained from the lawful search pursuant to the warrant was obtained independently from the constitutional violation, it need not be excluded.

\* \* \*

¶138 ESPs have many reasons for wanting to keep their platforms free of harmful and inappropriate content like CSAM, and many utilize software to monitor and prevent it. However, those efforts do not open the door to warrantless searches by the government of ESP users' private, password-protected data. By opening and viewing Gasper's video without a search warrant, the State exceeded the bounds of the ESP's private search. The State did not do so with the virtual certainty that it would find nothing of significance in the file. Its visual examination of the video not only confirmed that the file contained CSAM, but it revealed specific images that the State described in detail in the search warrant affidavit. Because the State's decision to forego a search warrant before opening and viewing the video cannot be excused under the good-faith exception, the evidence obtained from the warrantless viewing should have been suppressed. Nevertheless, I would hold that the CSAM found during the execution of the search warrant need not be suppressed because the warrant was supported by sufficient untainted evidence.

¶139 For the foregoing reasons, I concur in part and dissent in part.

**APPENDIX B — OPINION OF THE COURT OF  
APPEALS FOR THE STATE OF WISCONSIN,  
DISTRICT II, FILED OCTOBER 30, 2024**

STATE OF WISCONSIN  
IN COURT OF APPEALS  
DISTRICT II

Appeal No. 2023AP2319-CR  
Cir. Ct. No. 2023CF470

STATE OF WISCONSIN,

*Plaintiff-Appellant,*

v.

MICHAEL JOSEPH GASPER,

*Defendant-Respondent.*

Filed October 30, 2024

APPEAL from an order of the circuit court for Waukesha County: SHELLEY J. GAYLORD, Reserve Judge. *Reversed and cause remanded.*

Before Gundrum, P.J., Neubauer and Lazar, JJ.

¶1 NEUBAUER, J. The State of Wisconsin appeals from an order granting Michael Joseph Gasper's motion to suppress. The primary issue is whether a law enforcement officer's warrantless inspection of a cyber tip

*Appendix B*

digital video file provided to the officer and identified as child pornography by a private internet service provider constituted an unreasonable search in violation of the Fourth Amendment. 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. Accordingly, we reverse the suppression order and remand this matter for further proceedings consistent with this opinion.

**BACKGROUND**

¶2 On January 13, 2023, the electronic service provider (ESP) Snapchat<sup>1</sup> submitted a report to the CyberTipline of the National Center for Missing and Exploited Children (“NCMEC”), as required by federal law.<sup>2</sup> Snapchat detected a child pornography video that had

---

1. Snapchat is a social media platform where users can “share text, photographs, and video recordings, collectively known as ‘snaps.’” *Commonwealth v. Carrasquillo*, 489 Mass. 107, 179 N.E.3d 1104, 1109 (2022). While Snap, Inc. is the entity identified in Snapchat’s terms of service and incorporation documents discussed herein, for ease of reading we refer to both the platform and entity as Snapchat.

2. “In order to reduce . . . and . . . prevent the online sexual exploitation of children,” federal law requires ESPs like Snapchat to report to NCMEC “any facts or circumstances from which there is an apparent violation of . . . child pornography [statutes]” “as soon as reasonably possible after obtaining actual knowledge of any [such] facts or circumstances.” 18 U.S.C. §§ 2258A(a)(1)(A)(i), (a)(2)(A), 2510(15), 2258E. The contents of that report are left to the discretion of the provider but may include, inter alia, email addresses, internet protocol (IP) addresses, geographic location information, and

*Appendix B*

been “saved, shared, or uploaded” to Gasper’s Snapchat account. The video was not made public, and no one else saw it. Snapchat detected the video using Microsoft’s PhotoDNA program that scans files to determine if they are copies of known and reported child pornography based on their “hash values.”<sup>3</sup> The submission to NCMEC indicated the presence of “Apparent Child Pornography” stored in the Snapchat user account and listed Gasper’s

---

descriptions of the identified images. *Id.* § 2258A(b). NCMEC then forwards the CyberTip report to the appropriate law enforcement agency for possible investigation. *Id.* § 2258A(c).

3. “A hash value is an algorithmic calculation that yields an alphanumeric value for a file.” *United States v. Stevenson*, 727 F.3d 826, 828 (8th Cir. 2013). We have described hash values as a “digital signature.” *State v. Baric*, 2018 WI App 63, ¶15, 384 Wis. 2d 359, 919 N.W.2d 221. The algorithm derives the hash value by analyzing all the “bits” of data in a particular file. Software programs can scan a file, derive its hash value, and compare that hash value to a database of hash values of known child pornography files. *See id.*, ¶16 (describing such a program). PhotoDNA can detect slightly altered copies of known child pornography files. The CyberTip report indicated that the video linked to Gasper’s Snapchat account was a hash match of a file containing child pornography.

As the federal district court in *United States v. Lowers*, 715 F. Supp. 3d 741, 748 (E.D.N.C. 2024), recently explained:

As for a hash search’s capacity to identify contraband, “hash searches are like dog sniffs but even better.” Dennis Martin, *Demystifying Hash Searches*, 70 Stan. L. Rev. 691, 717 (2018); *see also* Rebekah A. Branham, *Hash It Out: Fourth Amendment Protection of Electronically Stored Child Exploitation*, 53 Akron L. Rev. 217, 219 (2019) (citing evidence that the chance of two different files sharing the same hash value “is less than one in one billion”).

*Appendix B*

subscriber information—his username, IP address, email address, and date of birth. That same day, Snapchat locked Gasper’s account. No person from Snapchat or NCMEC opened the video.

¶3 NCMEC traced the IP address tied to Gasper’s account to Wisconsin and thus sent the CyberTip report to the Wisconsin Department of Justice (DOJ). Other than the video, the CyberTip did not include any content from Gasper’s account. A DOJ policy analyst opened the video and prepared and submitted an administrative subpoena to Gasper’s internet service provider seeking the name and mailing address associated with Gasper’s IP address.

¶4 Detective David Schroeder then received a copy of the CyberTip video. He opened the single video and confirmed that it depicted child pornography. Schroeder confirmed that Gasper occupied the residence connected to the IP address and that the available Wi-Fi networks outside Gasper’s home were password protected and not publicly accessible. Using the information learned from the CyberTip video, Schroeder prepared and executed a search warrant at Gasper’s home. Police seized electronic devices from Gasper’s home and took him into custody. Gasper waived his *Miranda*<sup>4</sup> rights and admitted that he had accessed additional child pornography files on his phone.

---

4. *Miranda v. Arizona*, 384 U.S. 436, 86 S.Ct. 1602, 16 L.Ed.2d 694 (1966).

*Appendix B*

¶5 Gasper was charged with ten counts of possessing child pornography.<sup>5</sup> He filed a motion to suppress seeking exclusion of the Snapchat video because Schroeder opened it without a warrant or exception. He also sought to suppress the other child pornography evidence recovered from the search of his home as the fruit of a warrantless unconstitutional search of the Snapchat video.

¶6 Schroeder was the only witness to testify at the hearing on Gasper's motion to suppress. Schroeder described how PhotoDNA operates and recounted how he responded to the CyberTip. The State submitted into evidence Snapchat policies and guidelines that govern a user's use of Snapchat and that all users, including Gasper, must agree to upon creating a Snapchat account. These policies banned child pornography and informed users that Snapchat was actively scanning for child pornography and that Snapchat will report discovery of the same to NCMEC and law enforcement.

¶7 The circuit court granted Gasper's motion to suppress the video and all the child pornography evidence discovered pursuant to the warrant that relied on the video. The court determined that Gasper had a reasonable expectation of privacy because he used a cell phone to access Snapchat, citing *Riley v. California*, 573 U.S. 373, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014) and *Carpenter v. United States*, 585 U.S. 296, 138 S.Ct. 2206,

---

5. Gasper was also charged with nine counts of sexual exploitation of a child, although this appeal concerns only Gasper's claim that all child pornography evidence should be suppressed.

*Appendix B*

201 L.Ed.2d 507 (2018). The State appeals the order granting suppression.

**DISCUSSION****Gaspar Lacked a Reasonable Expectation of Privacy in a Child Pornography Video That He Uploaded to Snapchat in Violation of Its Terms of Service.**

¶18 Gaspar contends that the circuit court properly granted his motion to suppress because he had a reasonable expectation of privacy in the CyberTip video from his Snapchat account. The State contends that Gaspar failed to show an objectively reasonable expectation of privacy sufficient to establish that the search violated his Fourth Amendment rights. As we now explain, we agree that Gaspar failed to meet his burden to establish an objectively reasonable expectation of privacy in the video. Thus, Detective Schroeder's visual inspection of the video was not a search subject to the Fourth Amendment.

**I. Standard of Review**

¶19 On review of a motion to suppress evidence, we uphold the circuit court's factual findings unless they are clearly erroneous. *State v. Tentoni*, 2015 WI App 77, ¶16, 365 Wis. 2d 211, 871 N.W.2d 285. Whether the government conduct at issue constitutes a search, and if so, whether that search passes constitutional muster, are questions of law to be decided de novo. *Id.*; see also *State v. Garcia*, 195 Wis. 2d 68, 73, 535 N.W.2d 124 (Ct. App. 1995).

*Appendix B***II. Fourth Amendment Principles: Reasonable Expectation of Privacy**

¶10 The Fourth Amendment protects against unreasonable searches and seizures by the government. U.S. CONST. amend. IV; *see also* WIS. CONST. art. I, § 11.<sup>6</sup> Fourth Amendment rights are personal and may not be asserted vicariously. *State v. Bruski*, 2007 WI 25, ¶22 n.3, 299 Wis. 2d 177, 727 N.W.2d 503. A search occurs for the purpose of the Fourth Amendment “when an expectation of privacy that society is prepared to consider reasonable is infringed.” *State v. Purtell*, 2014 WI 101, ¶21, 358 Wis. 2d 212, 851 N.W.2d 417 (quoting *United States v. Jacobsen*, 466 U.S. 109, 113, 104 S.Ct. 1652, 80 L.Ed.2d 85 (1984)). Thus, a person challenging a search bears the burden of establishing by a preponderance of the evidence that he or she has a reasonable expectation of privacy in the area or object of the challenged search. *Tentoni*, 365 Wis. 2d 211, ¶7, 871 N.W.2d 285; *Bruski*, 299 Wis. 2d 177, ¶22, 727 N.W.2d 503. The privacy interest is both subjective and objective: a defendant must show he or she subjectively expected privacy in the area or object, and the expectation is one that society recognizes as reasonable. *Tentoni*, 365 Wis. 2d 211, ¶7, 871 N.W.2d 285. Failure to establish either defeats the defendant’s motion to suppress. *See State v. Baric*, 2018 WI App 63, ¶18 n.5, 384 Wis. 2d 359, 919 N.W.2d 221.

---

6. The Wisconsin Supreme Court “generally follows the United States Supreme Court’s interpretation of the search and seizure provision of the Fourth Amendment in construing Article I, Section 11 of the Wisconsin Constitution.” *State v. Bruski*, 2007 WI 25, ¶20 n.1, 299 Wis. 2d 177, 727 N.W.2d 503.

*Appendix B*

¶11 With regard to the objective prong, we consider the following nonexclusive factors in determining whether the totality of circumstances shows that a person has a reasonable expectation of privacy:

(1) whether the accused had a property interest in the premises; (2) whether the accused is legitimately (lawfully) on the premises; (3) whether the accused had complete dominion and control and the right to exclude others; (4) whether the accused took precautions customarily taken by those seeking privacy; (5) whether the property was put to some private use; [and] (6) whether the claim of privacy is consistent with historical notions of privacy.

*Bruski*, 299 Wis. 2d 177, ¶24, 727 N.W.2d 503 (citation omitted). “[T]he reasonableness of an expectation of privacy in digital files shared on electronic platforms is determined by considering the same factors as in any other Fourth Amendment context.” *Baric*, 384 Wis. 2d 359, ¶19, 919 N.W.2d 221.

### **III. Application to Gasper**

¶12 As an initial matter, we note that the circuit court did not address either the subjective or the objective inquiries in regard to the video in Gasper’s Snapchat account. Instead, the court relied on *Riley* (requiring a warrant to search arrestees’ cell phones) and *Carpenter* (requiring probable cause to obtain cell-site records) to conclude that Gasper had a reasonable expectation

*Appendix B*

of privacy in the video in his Snapchat account because he accessed it with his cell phone. However, Snapchat acquired the video from Gasper’s Snapchat account, not his phone. That made Gasper’s Snapchat account the relevant “area” that was searched. *See State v. Bowers*, 2023 WI App 4, ¶¶26, 44-45, 405 Wis. 2d 716, 985 N.W.2d 123 (2022).

¶13 In *Bowers*, we analyzed whether the defendant had a reasonable expectation of privacy in his Dropbox account, a cloud-based storage account that he created with his work email address. *Bowers*, 405 Wis. 2d 716, ¶¶1-3, 985 N.W.2d 123. We noted that the Dropbox account was a digital version of a physical storage container that could be accessed from “one device or a thousand devices.” *Id.*, ¶¶26-27. That conclusion turned on the features of the Dropbox account, not the device that Bowers used to access it. *See id.*, ¶¶20, 21-27, 40-42 (“We therefore address only whether Bowers’ expectation of privacy *in his [a]ccount* was objectively reasonable” (emphasis added)). The Dropbox account was not tied to a “‘physical device of any kind’ and was not stored on county property or controlled by the county.” *Id.*, ¶27. Because the cloud-based storage center was password protected, and Bowers did not share the content of his account with anyone other than those he chose to, we concluded that Bowers had a reasonable expectation of privacy. *See id.*, ¶¶21, 45.

¶14 As relevant here, we rejected the State’s argument that because Bowers created the account with his county government email address and his employer could access the Dropbox account through the email

*Appendix B*

address, Bowers lacked a reasonable expectation of privacy. *Id.*, ¶¶22, 42. We explained that the county “did not search its own devices to access the information in Bower’s [a]ccount; it used the internet as a tool to access the outside server on which the [a]ccount was located.” *Id.*, ¶42. Thus, the relevant “area” for purposes of determining whether Bowers had a reasonable expectation of privacy was the Dropbox account, not the device used by Bowers to access it. *See id.*, ¶¶17, 20, 40.

¶15 This analysis applies here. Snapchat did not access the video in Gasper’s account through his cell phone. Rather, the video was obtained directly from Gasper’s Snapchat account. Snapchat scanned the data held on its own servers and identified the child pornography video in Gasper’s account without accessing any of his devices. Thus, the relevant question is whether Gasper had a reasonable expectation of privacy in the video in his Snapchat account.

¶16 He did not. As noted above, at the motion to suppress hearing, the State introduced three documents that show that Snapchat informed Gasper that it would be scanning and accessing his account for content that violated its terms of service (such as child pornography) and would report violations to law enforcement: (1) the “Snap Inc. Terms of Service”; (2) Snapchat’s “Community Guidelines”; and (3) its “Sexual Content Community Guidelines Explainer Series” (the “Sexual Content Explainer”).

*Appendix B*

¶17 The Terms of Service forbid using Snapchat “in any way not expressly permitted by these Terms or [the] Community Guidelines.” They also forbid users from “violat[ing] any applicable law . . . in connection with [their] use of” Snapchat. By making an account, users specifically authorize Snapchat to “access, review, screen, and delete [their] content at any time and for any reason.” The Terms of Service also contain a section entitled “Safety” that provides that if a user fails to comply with the Terms of Service, Snapchat “reserve[s] 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.” At multiple points the Terms of Service contain a hyperlink to the Community Guidelines.

¶18 The Community Guidelines prohibit “any activity that involves sexual exploitation or abuse of a minor.” They require that users “[n]ever post, save, send, forward, distribute, or ask for nude or sexually explicit content involving anyone under the age of 18.” Snapchat explains that it will “report all instances of child sexual exploitation to authorities, including attempts to engage in such conduct.” The Community Guidelines refer users and provide a hyperlink to the Sexual Content Explainer “[f]or more information about sexual conduct and content that violates [the] Community Guidelines.”

¶19 The Sexual Content Explainer restates Snapchat’s prohibition on any content or activity related to the sexual exploitation of a child. It also has a paragraph

*Appendix B*

describing how it scans user accounts and reports child pornography to NCMEC, just as it did in this case:

Preventing, detecting, and eradicating Child Sexual Abuse Material (CSAM) on our platform is a top priority for us, and we continuously evolve our capabilities to address CSAM and other types of child sexually exploitative content. We report violations of these policies to [NCMEC], as required by law. NCMEC then, in turn, coordinates with domestic or international law enforcement, as required.

¶20 Gasper has failed to satisfy his burden to prove either his subjective or an objective expectation of privacy. First, as to any subjective expectation of privacy, Gasper did not testify, nor did he submit any admissible evidence to meet his burden to show that he believed the video downloaded on Snapchat was private.<sup>7</sup> Other than Schroeder's affidavit that established Gasper's Wi-Fi was password protected, there is no factual basis to conclude that Gasper had a subjective expectation of privacy in the video.

¶21 Even if Gasper had opted to testify to a subjective expectation, the Snapchat policies make it clear that any subjective expectation of privacy would be unfounded. This dooms Gasper's challenge. The evidence presented to the circuit court showed that Gasper agreed

---

7. While Gasper submitted an affidavit, the circuit court ruled that it was inadmissible. Gasper does not challenge that ruling on appeal, and thus, has abandoned any effort to rely on the affidavit.

*Appendix B*

to terms that he violated by saving, sharing, or uploading a child pornography video to his account. Snapchat informed him that it would be scanning and accessing his account for content that violated the terms of service like child pornography and would report violations to NCMEC, as required by federal law, and to law enforcement. The terms to which Gasper agreed vitiate any claimed subjective expectation of privacy.

¶22 To further explain, even if Gasper had attested to a subjective expectation of privacy in the Snapchat video, that expectation would be objectively unreasonable given Snapchat's policies regarding sexual content in general and sexually explicit content involving children in particular. As to the first two factors identified in *Bruski*, Snapchat's terms limited Gasper's property interest in his account, which prohibited him from saving, sharing, or uploading child pornography to his account. *See Bruski*, 299 Wis. 2d 177, ¶27, 727 N.W.2d 503 (considering property interest in the object of the search). That conduct was obviously unlawful.

¶23 As to the third factor, Snapchat's Terms of Service, Community Guidelines, and Sexual Content Explainer limited Gasper's dominion and control over his account when it came to child pornography. *See id.*, ¶¶27-28 (considering dominion, control, and the right to exclude others). Gasper agreed that Snapchat could monitor his account for content violations, and Snapchat reserved the right to access offending accounts, actively scan for child pornography, delete content and terminate his account, and advised that it would report child pornography to the

*Appendix B*

authorities. Thus, Gasper could not exclude Snapchat from his account when it came to child pornography.

¶24 As to the fourth and fifth factors, even if his account were password protected, Gasper acknowledged that Snapchat expressly denied him permission, control, or privacy with respect to child pornography, no matter what precautions he took. *See id.*, ¶¶24, 28 (considering “precautions customarily associated with those seeking privacy” and whether “property was put to some private use”). Finally, Gasper has failed to identify any historical notion of privacy for a child pornography video that has no lawful purpose. *See id.*, ¶30 (considering historical notions of privacy).

¶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. *See, e.g., United States v. Lowers*, 715 F. Supp. 3d 741, 753-54 (E.D.N.C. 2024) (collecting federal district court cases).

¶26 As one federal district court concluded, “given the prohibitions and reservations of rights in [Snapchat’s] Terms of Service and Community Standards, even for the CyberTips involving uploaded images and videos whose contents were not ‘publicly available,’ a reasonable person would not have viewed files containing prohibited

*Appendix B*

content as private.” *United States v. Tennant*, No. 23-CR-79, 2023 WL 6978405, at \*9 (N.D.N.Y. Oct. 10, 2023) (denying motion to suppress child pornography recovered in searches of defendant’s Snapchat and other social media accounts).

¶27 Another federal district court reached the same conclusion, reasoning that Yahoo’s and Google’s terms of service warned a defendant that he “risked being reported to law enforcement or NCMEC if either discovered that he sent, received, or distributed apparent child pornography. Even if Defendant believed that his [content was] private, society is not prepared to recognize that belief as reasonable given the Terms of Service. . . .” *United States v. Brillhart*, No. 22-CR-53, 2023 WL 3304278, at \*8 (M.D. Fla. May 7, 2023) (denying motion to suppress evidence of child pornography recovered from defendant’s Yahoo and Google accounts); *see also United States v. Colbert*, No. 23-CR-40019, 2024 WL 2091995, \*\*8-9 (D. Kan. May 9, 2024) (concluding that defendant lacked a reasonable expectation of privacy in child pornography on his Snapchat account because Snap, Inc.’s Terms of Service warned him that unlawful information related to his account could be released to law enforcement and its Community Guidelines warned him that child sexual exploitation would be reported to authorities); *but see United States v. Coyne*, 387 F. Supp. 3d 387, 396 (D. Vt. 2018) (concluding that defendant retained a reasonable expectation of privacy in his Microsoft, Yahoo, and Chatstep accounts because the user agreements failed to specifically inform him that his content would be disclosed “to NCMEC and its law enforcement partners”).

*Appendix B*

¶28 We agree with the conclusion reached in *Lowers, Tennant, Brillhart, and Colbert*. 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. Accordingly, Gasper has not met his burden in demonstrating that any expectation of privacy in the video was either subjectively or objectively reasonable.

**CONCLUSION**

¶29 Detective Schroeder’s viewing of the video that accompanied the CyberTip did not constitute a search under the Fourth Amendment. Because the viewing of the video was not subject to the Fourth Amendment, the search warrant subsequently issued based on the video was also valid. The suppression order is therefore reversed, and this case is remanded for further proceedings consistent with this opinion.<sup>8</sup>

*By the Court.*—Order reversed and cause remanded.

---

8. Because we determine that no Fourth Amendment “search” occurred, we need not reach the additional grounds the State sets forth for reversal, including an exception to the warrant requirement based on a private party search conducted by Snapchat and the good faith exception to the exclusionary rule. *See State v. Blalock*, 150 Wis. 2d 688, 703, 442 N.W.2d 514 (Ct. App. 1989) (cases should be decided on narrowest possible ground).

**APPENDIX C — OPINION OF THE CIRCUIT  
COURT FOR THE STATE OF WISCONSIN,  
WAUKESHA COUNTY, FILED OCTOBER 30, 2023**

STATE OF WISCONSIN  
CIRCUIT COURT  
WAUKESHA COUNTY

Case No. 23 CF 470

STATE OF WISCONSIN,

*Plaintiff,*

v.

MICHAEL GASPER,

*Defendant.*

Filed October 30, 2023

**DECISION AND ORDER**

The parties and respective counsel appeared on October 2, 2023 to present evidence on defendant's motions to suppress.<sup>1</sup> There were extensive briefs. This court considered some law review articles to get a sense of the problem that has lead federal circuit courts to

---

1. Please pardon typos, formatting, incomplete citations etc. Reserve judges do not have access to circuit judge's research tools, dashboard, and hardware.

*Appendix C*

differing conclusions.<sup>2</sup> This case presents the problem of the intersection of legitimate cell phone privacy issues and prosecuting child pornography circulating on the internet. The federal circuit courts are split. The Supreme Court of the United States (SCOTUS), the 7th Circuit and the Wisconsin Supreme Court have not ruled *directly* on the issue in this case. However, current SCOTUS cases do not allow for the government's proposed expansion of the private party search doctrine. That doctrine demands that a human being actually view *defendant's* image. Because SNAPCHAT did not view Gasper's video, current law means law enforcement needed a warrant before viewing it. Further, even if this court were to adopt the reasoning of cases extending the doctrine as the DA urges, the facts of the case undermine the reliability of the technology used. Either flaw requires granting the motions to suppress the warrantless search. The remainder of the evidence is fruit of the poisonous tree., demanding suppression. There is no doubt there is a crucial public interest in detecting and prosecuting child sexual abuse material and private parties play a big role in helping with that. However, requiring a warrant does not meaningfully interfere with the help private parties provide. The motions are granted.

---

2. (See 69 Stanford Law Review 2017 What is 4th Amendment Contraband; Hastings Law Journal:Sponsored Hash Searches & the Reasonable Expectation of Privacy; Volume 53, Issue 1, Article 16, University of Pacific Law Review: Two Models of the Fourth Amendment and Hashing to Investigate Child Sexual Abuse Material; Volume 30, February 2018 Stanford Law Review, Demystifying Hash Searches; Searches and Seizures in a Digital World.)

*Appendix C***I. BACKGROUND**

The important facts are not in dispute. Gasper used Century Link as his internet service provider (ISP) and a SNAPCHAT cell phone app. According to the terms of service (TOS) and community guidelines (CG), users are on notice SNAPCHAT will scan all user content using Microsoft's PhotoDNA program to detect SCSAM (suspected child sexual abuse material) and report it to authorities. (Exhibits 6 & 7.) On January 13, 2023 SNAPCHAT closed Gasper's account after Microsoft's PhotoDNA algorithm matched one set of identifying data of a video to a database of the identifying data of SCSAM. This identifying data is in the form of "hash" values, which is a string of numbers and letters, akin to a unique social security number. "Hash" values are discussed more fully below. That string is not the actual image and does not include a description of the image.

SNAPCHAT is not required to surveil user content. However, 18 USC 2258A required SNAPCHAT to forward Gasper's SCSAM information via a CyberTip to the National Center for Missing and Exploited Children (NCMEC). (Exhibit 3) The long and the short of the remaining facts is this: NCMEC didn't view the video and forwarded relevant information to the Wisconsin DOJ. The DOJ issued a Wis. Stat. s. 165.505 administrative subpoena to Gasper's ISP, Century Link.<sup>3</sup> The Wisconsin

---

3. Gasper claimed the s. 165.505(2) administrative subpoena wasn't done properly, but it was in full compliance. Gasper also claimed that statute allows an unconstitutional based on reasonableness instead of probable cause. The court doesn't have to

*Appendix C*

DOJ converted the digital information into an mp4 file and viewed the video without a warrant. The DOJ sent Gasper's identifying information from Century Link and the mp4 file to the Waukesha County Sheriff. (Exhibit 16 email.)<sup>4</sup> The Sheriff viewed the video, again without a warrant. March 20, 2023, the Sheriff used the detailed description of the contents of the video to get a search warrant for Gasper's home and took Gasper into custody. (Exhibit 11.) March 26, 2023, Plaintiff obtained a search warrant for SNAPCHAT, based in large part on viewing the video. (Exhibit 18, Attachment A.)

**II. DISCUSSION**

The 4th Amendment protects parties from governmental searches. Private searches do not implicate the 4th Amendment.<sup>5</sup> However, the governmental search cannot go beyond what the private party discovered. Federal circuit courts are struggling with the 4th

---

decide that issue, but see the reasoning in *Carpenter*, that probable cause is not always needed and a reasonable bases will suffice.

4. Clearly, the information Century Link provided was within its own business records and the limited information is not particularly sensitive. (See **Smith** and **Miller** SCOTUS decisions below.)

5. SNAPCHAT's terms of service warn SNAPCHAT will surveil user content. That doesn't waive the 4th Am. private party search doctrine protections vis a vis the government and the user. "But the fact of diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely." *Riley*, 573 U. S., at \_\_\_ (slip op., at 16)." Cited in **Carpenter**.

*Appendix C*

Amendment and the private party search and related doctrines in the context of suspected child sexual abuse material (SCSAM).<sup>6</sup> However, it's clear that cell phone searches are of particular 4th Amendment privacy concern. (See **State v. Carroll, Riley and Carpenter**.) Exceptions to the warrant requirement are jealousy guarded and narrowly defined.

Under the private party search doctrine, the government is not required to “avert its eyes” from information a private party provides, because the expectation of privacy has already been frustrated. **Coolidge v. New Hampshire** (S. Ct. 1971). More specifically, the privacy expectation has already been frustrated *because the same image was privately viewed*. *Further, the doctrine does not allow the government to exceed the scope of the private party discovery*. But what does **“the same image was privately viewed” mean?** SCOTUS tells us: if the private party actually “eyeballed” the *defendant’s* contraband (Gasper’s video) and if the government only viewed that contraband and nothing else, no warrant is needed; if that person did not “eyeball” defendant’s contraband or if the government exceeded the scope of what that person discovered, a warrant is needed. In Gasper’s case, SNAPCHAT, the relevant private party, did not “eyeball” the actual video.

As the DA points out, some jurisdictions expand upon that distinction by relying on a data base and computer algorithms to detect matches of SCSAM. (See **U.S. v.**

---

6. This court isn’t bound by those federal district courts.

*Appendix C*

**Miller** (6th Cir. 2020) below and similar cases cited by Plaintiff.) The data base is created when some unknown person (“proxy”) identifies an image as SCSAM. That image is then turned into an identifying string of numbers and letters called “hash values.” A hash value isn’t an actual image, can’t be simply reversed into the image and provides no description of the image. (Exhibit 2.) Only the hash value is put into a data base. SNAPCHAT surveils user images using Microsoft’s PhotoDNA algorithm. PhotoDNA assigns hash values to a user’s image, like Gasper’s video.<sup>7</sup> If the PhotoDNA hash value matches the database hash value, PhotoDNA alerts to the presence of SCSAM. That entire process does **not** involve a person ever putting eyeballs on Gasper’s video. Nor is the person involved in creating the data base in any way related to Gasper. Instead, both the private person and the hash values serve as proxies for a person actually seeing defendant’s video. The cases the DA cite rely on two things: substituting the proxy process for a person laying eyeballs on defendant’s SCSAM **and** the reliability of the hash process. Importantly, that proxy process has not been adopted by SCOTUS and, in this case, the reliability of the hash values is undermined. Therefore, DOJ and the Sheriff needed a warrant. This is explained below.

---

7. Not all hash programs are valid. Some do not detect enough points on images leading to false positives or “collisions.” Therefore, they risk revealing innocuous material, exactly what the private search doctrine protects against.

*Appendix C***A. The US Supreme Court hasn't expanded the law**

SCOTUS has **not** recognized the warrantless federal circuit court cases the DA cites. Therefore, it's important to apply what we do about basic 4th Amendment principles and warrantless searches. The reasonable expectation of privacy standard has long been recognized. (**U.S. v. Katz**, (Sp. Ct. 1967.) The privacy interest must be societally legitimate.<sup>8</sup> There is a legitimate privacy interest in cell phones. **Carpenter** (S. Ct. 2018). Therefore, searches involving cell phones require careful analysis.

**Some cases the D.A. cited allowing warrantless searches:**<sup>9</sup>

- **U.S. V. Miller** (S. Ct. 1976) and **Smith v. Maryland** (S. Ct. 1979). Bank checks and phone records. Defendant's bank, the check recipient, the phone company each directly "eyeballed" the items.

---

8. The DA cited **Illinois v. Caballes** (S. Ct. 2005) out of context. There, the court held defendant did not have a legitimate privacy interest in drug contraband in the context of a traffic stop and a dog sniff. Here, we have cell phone and a hash of a video implicating different interests.

9. There's no need to go through every case cited in the briefs. The principles are the same in terms of distinguishing them, often because the core issue wasn't the same. For example the DA recognized that **U.S. v. Bebris** (7th Cir. 2021) didn't focus on the exact issue here.

*Appendix C*

- **U.S. v. Jacobson** (S. Ct. 1984). FedEx opened a damaged package and “eyeballed” white powder. FBI field tested the powder. Field testing was not a separate search, because it could not uncover private information identifying exactly what the powder was (talc, sugar?). This is like the dog sniff cases. Contrast this with the information an image reveals: person(s) in the room who may not be involved in sexual acts, private personal items in the room, etc. In any event it’s more than hash values.
- **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.
- **U.S. v. Miller**, (6th Cir. 2020) SCAM private search and virtual certainty.  
Unclear if GOOGLE’s hash technology and process challenged.

**Cases defendant cited requiring a warrant:**

- **Walter v. U.S.** (S. Ct. 1980) exceeded private party search when FBI viewed films after private party saw suspicious label, but not the films
- **U.S. v. Wilson**, (9th Cir. 2021) reliability of GOOGLE’s SCSAM match process unproven; GOOGLE did not “eyeball” defendant’s email; law enforcement learned much more than GOOGLE had, exceeding scope.

*Appendix C*

- **Ackerman** (10th Cir. 2016) government exceeded scope by opening items the private party had not: the email and 3 more images. Here, the sole image was opened so the case is distinguishable.
- **Carpenter** (S. Ct. 2018). 127 continuous days tracking cell phone tower location data required warrant *even though* defendant was visible and seen by private parties while traveling around. Distinguishable *in part*: location data over extended period of time. Case didn't mention CSAM issues and was carefully circumscribed.

The next task is to analyze both **Miller** decisions, **Smith, Walter, and Wilson**.

**Miller** (6th Cir 2020.), and similar cases the DA cites, applies a **broader view** of who the “private party” is and what comprises the “same image.” In **Miller**, (6th Cir. 2020) the court was satisfied that the proxy private party who originally identified SCSAM placed in a data base, serves as the “private party.” Further, the court found the “hashing” process, so reliable that it substituted for actually viewing SCSAM. Therefore, when law enforcement subsequently viewed defendant’s image, it was a “virtual certainty” that it matched the proxy private party’s image. The warrantless search was allowed. That broader rationale is not recognized by SCOTUS yet, as shown next.

In contrast, **Miller** (S.Ct. 1976), **Smith** (S. Ct 1979.) **Walter** (S. Ct.) and **Wilson** (9th Cir.) take a narrower view. The **Miller** and **Smith** decisions involved private

*Appendix C*

persons who actually “eyeballed” defendant’s bank checks and phone records. There were no proxies or algorithms involved. **Walter** is consistent with these cases. The court held that even though the labels on the film container made it rather likely the contents included illegal pornography, (but not virtually certain), the private party did not see the films. Therefore, when the FBI viewed the films, it should have had a warrant.

Similarly in **Wilson**, GOOGLE staff did not eyeball the SCSAM mage. The court wrote extensively that the evidence GOOGLE’s process identifying suspect CSAM was too vague. This is similar to Gasper’s case, as shown in section (B) below. More importantly, the **Wilson** court required direct viewing of defendant’s images and not just the images in the database, however good the matching may be:

Because Google had not viewed them specifically and even if they had, and even if they were duplicates, such viewing of others ‘digital communications would not have violated Wilson’s expectation of privacy in his images, as Fourth Amendment rights are personal.

The court explained it as follows:

If, for example, police officers search someone else’s house and find documents evidencing wrongdoing along with notes indicating that I have identical documents in my house, they cannot, without a warrant or some distinct

*Appendix C*

exception to the warrant requirement, seize my copies. I would retain a personal expectation of privacy in them, and in my connection to them, even if law enforcement had a strong basis for anticipating what my copies would contain.

Here, substitute cell phones for the example of the houses. As many cases, including **Wilson**, note, it's not difficult to get a warrant. That case provides a roadmap for showing probable cause for a warrant. **Wilson**, is consistent with the narrower, current SCOTUS view requiring direct viewing of defendants' images. That wasn't done here, so law enforcement needed a warrant.

Plaintiff urges policy reasons to support broadening the private party search doctrine so that SNAPCHAT employees do not have to view defendant's image. It's true there is real harm to private parties viewing CSAM. But broadening the private party doctrine is clearly not the *sole* route to discovering and successfully prosecuting CSAM. The alternate route avoids that problem: get a warrant. Further, as laudable as such a policy determination is, it's not for trial courts to make policy. Higher courts might, especially in the context of the billions if not trillions of images floating around endlessly on the internet crying out for efficient detection and prosecution. It is exceedingly tempting to rule that SCOTUS, the 7th Circuit or Wisconsin Supreme Court *might* expand the private search doctrine as held in **Miller** (6th Cir.) But lower courts are bound by **existing precedent**.

*Appendix C***B. Even if the broader view is used, a warrant was needed**

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 Plaintiff's 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.

**III. CONCLUSION**

The motions to suppress are granted. This case shows why proving probable cause on a case by case basis remains important. Relying on algorithms and computer programs as a basis for avoiding warrants is like relying on the ever changing waters of a river because technology and its limits change so fast. Ultimately, such reliance that expands the existing private/third party doctrine is for higher courts to decide.

118a

**APPENDIX D — ORDER OF THE CIRCUIT  
COURT FOR THE STATE OF WISCONSIN,  
WAUKESHA COUNTY, FILED FEBRUARY 16, 2024**

STATE OF WISCONSIN  
CIRCUIT COURT  
WAUKESHA COUNTY

DA Case No.: 2023WK001433  
Assigned DA/ADA: Kristina J Gordon  
Agency Case No.: W23014300  
Court Case No.: 2023CF000470

STATE OF WISCONSIN,

*Plaintiff,*

v.

MICHAEL JOSEPH GASPER,

*Defendant.*

**ORDER**

Filed February 16, 2024

For the reasons outlined in the written decision on October 30, 2023, the defendant's motion to suppress is granted. This is a final order for purposes of appeal.

/s/ Shelley J. Gaylord

Reserve Judge Shelley J. Gaylord  
Signed: 14th day of February, 2024

119a

**APPENDIX E — DEFENDANT’S MOTION TO  
SUPPRESS EVIDENCE AND DERIVATIVE  
FRUITS OF SEARCH OF PREMISES AND  
ELECTRONIC DEVICES DATED MAY 10, 2023**

STATE OF WISCONSIN      WAUKESHA COUNTY  
CIRCUIT COURT

23-CF-000470

STATE OF WISCONSIN,

*Plaintiff,*

-vs.-

MICHAEL JOSEPH GASPER,

*Defendant.*

Filed May 10, 2023

**DEFENDANT’S MOTION TO  
SUPPRESS EVIDENCE AND DERIVATIVE  
FRUITS OF SEARCH OF PREMISES  
AND ELECTRONIC DEVICES**

The defendant, Michael J. Gasper, appearing specially by the Law Offices of Joseph F. Owens, LLC, by Attorney Joseph F. Owens, and reserving the right to challenge the court’s jurisdiction, moves the court for an order excluding all evidence obtained in violation of his constitutional rights, including but not limited to the following: all documents, all cellphones, all computers,

*Appendix E*

and all data storage devices, including the entirety of the information, contents, communications and video / audio recordings contained therein, and all data of any sort or kind contained in all cellphones, computers and data storage devices seized.

The defendant brings this motion pursuant to *Wis. Stat. § 971.31(2)* and *(5)* on the grounds that the above-referenced evidence was seized from the premises occupied by the defendant which is his private residence located at W362 S2521 Lisa Lane, Dousman, Wisconsin 53118, the contents of which residence were property in which he has a reasonable expectation of privacy and included documents, records, cellphones, computers and data storage devices, which were repositories of information and communications as to which the defendant has a reasonable expectation of privacy, all in violation of the rights guaranteed the defendant under U.S. Const. Amends. IV, V, and XIV; Wis. Const. Art. I, §§ 1, 2, 9, and 11; Wis. Stat. Ch. 968; and *Arizona v. Gant*, 556 U.S. 332 (2009), *Chimel v. California*, 395 U.S. 752 (1969), *Terry v. Ohio*, 392 U.S. 1 (1968), *Katz v. United States*, 389 U.S. 347 (1967), and *Mapp v. Ohio*, 367 U.S. 643 (1961).

Further, the defendant moves for exclusion from use as evidence all derivative evidence resulting from the execution of the search warrant issued herein, the search and seizure of the foregoing described premises and property, and includes all statements of the defendant made by him following execution of the search warrant and his arrest. *Taylor v. Alabama*, 457 U.S. 687 (1982); *Dunaway v. New York*, 442 U.S. 200 (1979); *Brown v.*

*Appendix E*

*Illinois*, 422 U.S. 590 (1975); *Davis v. Mississippi*, 394 U.S. 721 (1969); *Wong Sun v. United States*, 371 U.S. 471 (1963); *State v. Knapp*, 2005 WI 127, 285 Wis. 2d 86, 700 N.W.2d 899; *State v. Harris*, 199 Wis. 2d 227, 544 N.W.2d 545 (1996).

IN FURTHER SUPPORT of this Motion, the defendant asserts the following allegations, made upon information and belief:

1. Snapchat allegedly reported to the National Center For Missing And Exploited Children [NCMEC] an upload of a video of “apparent child pornography.” NCMEC is a governmental entity per *United States v. Ackerman*, 831 F.3d 1292, at 1308 (10th Cir. 2016).

2. NCMEC was informed by Snapchat that a particular “username” with a specified e-mail address and a specified “IP Address” was associated with this upload. NCMEC used Geo-Lookup to identify the “IP Address” as located somewhere in the State of Wisconsin, and the name of the internet service provider as “Century Link.” NCMEC then provided all of this information to the Wisconsin Department of Justice.

3. The Wisconsin Department of Justice, upon information and belief, issued an “Administrative Subpoena,” ostensibly per *Wis. Stat. §165.505(2)*, to Century Link, compelling Century Link to provide the personal identity and home address of the Century Link subscriber to be, Michael Gasper; disclosure of which is the type of information to which the defendant had a

*Appendix E*

reasonable expectation of privacy. [See: *United States v. Ackerman*, 831 F.3d 1292, 1308 (10th Cir. 2016)]. *Wis. Stat. §165.505* is facially unconstitutional as authorizing a search warrant which violates the Fourth and Fourteenth Amendments to the United States Constitution and Article I. §1,2,9, and §11 of the Wisconsin Constitution as set forth more particularly above on pages 1 and 2 of this Motion.

4. The “Administrative Subpoena” issued pursuant to *Wis. Stat. §165.505* to Century Link by a bureaucrat in the Wisconsin Department of Justice to compel the production of the identity and address of the defendant, Michael Gasper, upon information and belief: (a) did not satisfy the “probable cause” constitutional requirements of all search warrants set forth in the Fourth and Fourteenth Amendments to the Constitution of the United States and Article I. §1,2,9, and §11 of the Wisconsin Constitution and, (b) did not conform to the requirements of *Wis. Stat. §885.02* as required by *Wis. Stat. §165.505*. [See: *State v. Popenhagen*, 2008 WI 55, 309 Wis.2d 601 at 608, 749 N.W.2d 611,(2008).]

5. Following receipt by the Waukesha County Sheriff’s Department of the materials provided to the Wisconsin Department of Justice from the National Center For Missing And Exploited Children [NCMEC] and Century Link pursuant to the Department of Justice “Administrative Subpoena”, Waukesha County Sheriff Department Detective Schroeder opened and viewed the 16 second video of “apparent child pornography” without a search warrant This constituted information attached

*Appendix E*

to a Century Link internet subscriber's IP Address, as to which information the defendant, Michael Gasper, as the subscriber, had a reasonable expectation of privacy. [See: *United States v. Wilson*, 13 F.4th 961 at 964(2021), See also: *United States v. Ackerman*, 831 F.3d 1292, 1308 (10th Cir. 2016) Gorsuch, J., holding that when the government views email attachments it is a "search" for Fourth Amendment purposes under both an expectation-of-privacy and a trespass-to-chattels theory. *Kyllo v. United States*, 533 U.S. 27, 33, 121 S.C. 2038, 150 LED.2d 94 (2001) (citing *Katz v. United States*, 389 U.S. 347, 361, 88 S.C. 507, 19 LED.2d 576 (1967) (Harlan, J., concurring)); see also *United States v. Miller*, 982 F.3d 412, 427 (6th Cir. 2020).]

6. Following this warrantless search of the defendant's personal information by Detective Schroeder, the Waukesha County Sheriff's Department, upon information and belief, and in reliance thereon, requested and executed a search warrant of the defendant's home and seizure of specified property, including enumerated electronic devices, but which search warrant did **not** authorize searching the contents of the items seized. [See: *State v. Lancial*, 2023 WI App 11 at ¶30 - ¶36, 986 N.W.2d 572 (unpublished op. January 5, 2023 - copy attached)].

7. Following seizure of the items enumerated in the search warrant that was issued and executed herein at the defendant's home, Detective Schroeder, without a separate warrant, opened and searched the contents of the various items seized at the defendant's home for information and data, as to all of which items and their contents, the defendant had a reasonable expectation of privacy.

124a

*Appendix E*

8. All of the acts and omissions alleged in paragraphs 1. through 7. above constitute illegal and unconstitutional searches and seizures, which illegal and unconstitutional acts and the derivative “fruits” of same, violated the constitutional rights of the defendant, Michael Gasper, and accordingly are not admissible evidence in these criminal proceedings against him.

Dated the 10<sup>th</sup> day of May, 2023.

Law Offices of Joseph F. Owens, LLC  
Attorneys for Defendant, Michael J. Gasper

*Electronically Signed By:*

/s/ Joseph F. Owens

Joseph F. Owens

State Bar No.: 1016240

Mailing Address:

2665 S. Moorland Rd., Suite 200

New Berlin, WI 53151

Phone: (262)785-0320

Fax: (262) 785-1729

aolaw@bizwi.rr.com