STATE OF WISCONSIN
SUPREME COURT

STATE OF WISCONSIN,

Plaintiff-Appellant,

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

MICHAEL JOSEPH GASPER,

Defendant-Respondent-Petitioner.

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

---

DEFENDANT-RESPONDENT-PETITIONER'S REPLY BRIEF

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

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

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES CITED

Page No.

STATUTES CITED

OTHER AUTHORITIES

OVERVIEW

The State's Brief and the Court of Appeals' decision in this case rely on two basic theories. The first theory is that no person can have a "reasonable expectation of privacy" in their ESP account to the extent that it contains prohibited illegal contraband. This theory is predicated on notions akin to "informed consent" (sounding in tort) and "waiver" (sounding in contract). Under this theory, the inquiry focuses on the informative sufficiency of notice given by one party and the degree of knowing consent by the other party. This theory entirely bypasses any constitutional law principles governing knowing, voluntary and intelligent waiver of Fourth Amendment rights.

The second theory espoused by the State and the Court of Appeals' decision posits that the warrantless opening and physical viewing of previously unviewed "hashtag" coded cyberdata of "suspected" child pornography in a CyberTip, by the Wisconsin Attorney General's Office, and by Waukesha County Sheriff Detective Schroeder, was not an expansion of the "private search" conducted by Snapchat's computer "hashtag" scanning program.

The State's Brief then concludes by contending that its conduct, despite being constitutionally violative of the Fourth Amendment, should not be subject to the exclusionary area under the "good faith" exception.

ARGUMENT

I. Gasper Had A Sufficient "Reasonable Expectation Of Privacy" In The Cyberdata Uploaded From His Cellphone To His Snapchat Account To Afford Him The Protection Of The Fourth Amendment Against A Governmental Warrantless Search And Seizure Of Content Extracted From His Snapchat Account.

The State begins its Brief on p. 17-18 by deftly touching on the presumed prurient nature of the alleged contraband video before moving into the issues revolving around the legal efficacy of Snapchat's service provider documents.

The State's Brief endorses the Court of Appeals' position that Snapchat's unilateral policy statements prohibit posting of suspected child pornography, and

warn users that it reserves the right to report to law enforcement what it suspects may be illegal content. The State and Court of Appeals contend that these unilateral statements of corporate policy waive any user's objective or subjective "reasonable expectation of privacy" vis-à-vis the government for Fourth Amendment purposes. However, this position avoids careful dissection of the actual language in Snapchat's Terms of Service in which Snapchat does not tell its customers that the specific content of their accounts will be provided to law enforcement. Instead, there is only a vague statement that "… information relating to your account …" will be provided to law enforcement." This latent ambiguity is carefully explicated in the Defendant-Respondent-Appellant's Brief at page 30.

The State's Brief moves into a confusing discussion of bailment law. That body of law contradicts the State's position and actually appears to support the proposition that a warrant is required in the absence of unequivocal abandonment or the non-existence of a bailor's rights in bailed property. The State cites Justice Gorsuch's dissent in *Carpenter v. U.S.*, 585 U.S. 296, 399-400, 138 S.Ct. 2206 (2018), but misses the point that the Gorsuch dissent begins with the proposition that "Under this more traditional approach, Fourth Amendment protections for your papers and effects do not automatically disappear just because you share them with third parties." [*Carpenter*, *supra*, 138 S.Ct. 2206, 2268.]

The State's Brief on page 23 moves to the Snapchat Terms of Service which prohibits posting child pornography on its servers. The State posits that this unilateral private corporate policy statement entirely voids any "reasonable expectation of privacy" by a Snapchat accountholder.

The State's Brief on page 26 reasserts the erroneous proposition that Gasper did not preserve on appeal the offer of proof made in the circuit court as to the hearsay admissibility of his Affidavit describing his subjective expectation of privacy in his Snapchat account. To the contrary, that issue was preserved on pages 21-22 of Gasper's Court of Appeals Brief and reiterated on page 16 of Gasper's

Brief in this Court. [*See also: U.S. v. Raddatz*, 447 U.S. 667, 679, 100 S.Ct. 2406 (1980).]

What is completely missing from the State's Brief and the Court of Appeals Decision is evidence that Gasper, as a Snapchat accountholder, read or understood Snapchat's unilateral policy statements, or their import. It is elemental contract law that there must be a "meeting of the minds" on the essential terms of the parties' agreement. *Goossen, et al. v. Estate of Standaert, et al.*, 189 Wis.2d 237, 246, 525 N.W.2d 314 (WI App. 1994); RESTATEMENT (SECOND) OF CONTRACTS §3, at 13 (1981). As stated by the Court of Appeals in *Goossen:*

> For a term to be a part of a contract, the term must have been in the contemplation of the parties; it must have been the parties' intent to contract for it; and the parties must have had a meeting of the minds as to the term. [*Goossen, supra,* 189 Wis.2d at 246]

There is no explicit Snapchat policy statement that the accountholder agrees to waive all Fourth Amendment rights under the Constitution of the United States relative to the specific content of his or her account. There is only vague language that Snapchat "reserves the right" to report "information relating to your account" to law enforcement.

The State did not offer any proof that Gasper did more than click a button acknowledging that he had "read" only the Snapchat "Privacy Policy"; but nevertheless somehow "agreed" to Snapchat's "Terms of Service". There is absolutely no affirmation that he had read or been provided Snapchat's "Terms of Service," its "Community Guidelines," or its "Sexual Content Explainer."

This process was described by Detective Schroeder at the suppression hearing as follows: [R-60, pp. 54-55.]

BY MS. GORDON:

Q I think this Exhibit Number 9. Detective Schroeder, you previously said that you created a Snapchat Account to learn how the Terms of Service asks the user to acknowledge them?

A That's correct.

* * * * * * * * * *

Q Detective, what do you see on your screen here related to the Terms of Service?

A It's asking for a first and last name. Directly underneath it, it states, "By tapping sign up and accept or go, you acknowledge that you have read the Privacy Policy and agree to the Terms of Service."

Detective Schroeder continued to explain that in order to obtain these additional documents, the user has to either hit an additional hyperlink button or engage in a separate Google search: [R-60, p. 56.]

Q Okay. I'm going to show you what will be marked as Exhibit Number 10. And before I get to Exhibit Number 10, Detective, are the Terms of Service and Community Guidelines, are those available on the internet?

A Yes, ma'am.

Q In addition to when you sign up, being able to click the hyperlink, they would be able to the user elsewhere?

A Yes, ma'am.

Q Now, as part of your investigation into this particular case related to Mr. Gasper, did you look into Snapchat's Community Guidelines any further to determine exactly what information is on the Internet for users related to their Community Guidelines?

A I did a Google search and reviewed the terms and guidelines as I could see them, yes.

In the vernacular of the industry there are two dominant types of online website service agreements:

A. "Browsewrap" agreements: The applicable Terms of which are disclosed only through a hyperlink (often in the footer of a website). The user assents to the Terms by browsing the site or using the App. No clicking or other action is required to accept the terms;

B. "Clickwrap" agreements: The user accepts the applicable Terms by checking a box that states that the user agrees to the Terms before the user can continue using the site or app or complete the applicable user flow.

The Snapchat agreement appears to fall somewhere between the "Browsewrap" category and the "Clickwrap" category. Both are subject to heightened scrutiny by courts analyzing enforceability against individuals under traditional norms of actual and constructive notice found in civil contract law. [*See: Nguyen v. Barnes & Noble, Inc.*, 763 F.3d 1171, 1175-1176 (9th Cir. 2014) and *Specht v. Netscape Communications Corp.* 306 F.3d 17, 23, 32 (2nd Cir. 2002) authored by then Circuit Judge Sotomayor.] The Snapchat online agreement described by Detective Schroeder in 2023 does not appear to satisfy the notice and consent requirements of enforceability under these civil contract cases.

Parenthetically, Professor Orin S. Kerr, in his article in the University of Pennsylvania Law Review entitled "Terms of Service and Fourth Amendment Rights" [Vol. 172, No. 2, pp. 287-328, January 2024], references several empirical research studies illustrating that internet provider Terms of Service are rarely read.

In one study, researchers created a fake social media site called NameDrop, Inc. The focus of the study was to see how many people actually read the Terms of Service, and how many understood what they read. The website, however, contained an extraordinary Term whereby all users of NameDrop agreed "to immediately assign their first-born child to NameDrop, Inc." Seventy-Four percent of users did not view the Terms of Service, and most who viewed them scrolled through the legalese too quickly to understand them. Only about 7% of site users actually objected to the term. [Kerr, "Terms of Service and Fourth Amendment Rights," U. of Penn. L.Rev., *supra* at p. 325.]

The State in its Brief and the Court of Appeals' decision nevertheless myopically apply a civil contractual theory of "waiver" from Snapchat's online adhesion contract in an attempt to void Gasper's right to constitutional Fourth Amendment protection against a governmental warrantless search of his private Snapchat account. Under black letter contract law in Wisconsin, "a waiver is the voluntary and intentional relinquishment of a known right." *Nolop v. Spettel*, 267 Wis. 245, 249, 64 N.W.2d 859, 862 (1954). Snapchat's online contract methodology utterly fails to meet the civil contract law standard of waiver.

II. The Warrantless Opening And Viewing Of The CyberTip "Hash" Imagery By Wisconsin Department Of Justice Personnel And Detective Schroeder Does Not Meet The "Private Search" Exception To The Fourth Amendment Warrant Requirements.

The State's Brief at p. 17 correctly identifies the standard of appellate review in this Court when reviewing a suppression order as "… independently applying constitutional principles to those facts …" found by the circuit court, citing *State v. Tullberg*, 2014 WI 134 ¶27, 359 Wis.2d 421, 857 N.W.2d 120. The Court of Appeals here did not disturb the circuit court factual findings, ruling as a matter of law, that Gasper had no "reasonable expectation of privacy" in suspected contraband in his Snapchat account. That legal decision is subject to *de novo* review in this Court without deference, and this Court should "independently apply constitutional principles to the facts as found by the circuit court." *Tullberg, Id.*

In anticipation of this Court following this standard of review, the State's Brief in pages 29 through 44 argues that the government's actions here fall within the "private search" exception to the Fourth Amendment warrant requirements.

The State correctly observes that there is a split in the federal circuits on whether law enforcement needs to obtain a warrant before opening and viewing cyberdata contained in a CyberTip from the National Center for Missing and Exploited Children. The older appellate cases of *U.S. v. Reddick*, 900 F.3d 636 (5th Cir. 2018) and *U.S. v. Miller*, 932 F.3d 412 (6th Cir. 2020) support applying the

"private search" exception. The newer cases of *U.S. v. Wilson*, 13 F.4th 961 (9th Cir. 2021); *U.S. v. Holmes*, 121 F.4th 727 (9th Cir. 2024) and *U.S. v. Maher*, 120 F.4th 297 (2nd Cir. 2024) reject application of the "private search" exception to the Fourth Amendment warrant requirement.

The State begins its analysis of Supreme Court precedent on the "private search" exception by reference to *Walter v. United States*, 447 U.S. 649, 100 S.Ct. 2395 (1980) and *United States v. Jacobsen*, 466 U.S. 109, 104 S.Ct. 1652 (1984).

The facts in *Walter* closely mirror those in *Gasper* because the "private search" of opening a misdelivered film package by a private party did not involve physically viewing the film by the private party using a movie projector. However, the FBI did physically view the films using a movie projector without first obtaining a warrant. This degree of intrusion is similar to the governmental decoding, downloading and physical viewing the CyberTip of Gasper's "hash" data on a computer screen. Mechanical manipulation and projection of the film imagery for viewing by the FBI in *Walter* was a "significant expansion" of the "private search" conducted by the private party who had only observed "suggestive drawings" and "explicit descriptions" on the film boxes. The State's Brief quotes the lead opinion authored by Justice Stevens: ". . . prior to the Government screening one could only draw inferences about what was on the films." (emphasis added) *Walter v. U.S., supra,* 447 U.S. 649 at 650. Justice White's concurring opinion, joined by Justice Brennan, differed only slightly in context but agreed with the Stevens opinion that constitutional judicial scrutiny is on whether the scope of a subsequent governmental search exceeded the private party's search.

The State's Brief then turns to *U.S. v. Jacobsen*, where the Court's majority opinion, again authored by Justice Stevens, focused on the "*de minimis*" intrusion of scientific binary testing of the white powder which the private party had found in a damaged Federal Express package. The Supreme Court instructs us that subsequent chemical testing of the white powder did not involve any additional intrusion into the defendant's protected privacy rights in the package. The binary

chemical test merely disclosed whether the substance already discovered by the private party was cocaine. The test did not constitute additional intrusive conduct by the government. That is the core definitive distinction between the Court's decision to suppress in *Walter* and the decision not to suppress in *Jacobsen*.

The Court of Appeals in *U.S. v. Maher*, 120 F.4th 297 (2nd Cir. 2024) applied the correct analytical methodology to circumstances where an ESP sent an unviewed coded "hash" match of suspected SCAM on its servers to the National Center for Missing and Exploited Children, which in turn, sent the unopened CyberTip in encoded "hash" data to law enforcement. Following receipt of the CyberTip, law enforcement decoded, downloaded and visually reviewed the decoded algorithm of previously unviewed pixel imagery. This additional step necessarily exceeded the scope of a purely algorithmic private computer "hash value" scan.

The private computer search by Snapchat and NCMEC in Gasper also was limited to cybernetically matching the "hash value" of an image uploaded from Gasper's cellphone into his Snapchat account with the "hash value" of an image some unknown person had previously identified as child pornography and placed into Snapchat's or NCMEC's database. That is all the information that a CyberTip itself conveys. Until the unopened CyberTip data is decoded, opened and physically viewed, the actual image itself in the user's account is unknown. Furthermore, the unknown image to which it is matched is also unknown. Accordingly, opening, decoding and viewing a pixilated image of the coded cyberdata "hash" contained within the CyberTip necessarily constitutes a major expansion of the scope of the purely technological "hash value" scan conducted by Snapchat and NCMEC.

The State's Brief [pp. 33-34] contains several references to the "virtual certainty" of computerized "hash" matching technology as being sufficient to have established "probable cause" for issuance of a search warrant (had one been sought); implicitly suggesting that this Court retroactively validate an invalid warrantless search. As explained in *Katz v. U.S.*, 393 U.S. 347, 356-358, 88 S.Ct. 507 (1967): "That we cannot do." (emphasis added)

III. The Exclusionary Rule Should Apply.

The Wisconsin Attorney General's Office avoids the uncontroverted fact that it was the first law enforcement agency to open and view the CyberTip of imagery uploaded from Gasper's cellphone to his Snapchat account - without a warrant. The Wisconsin Attorney General's Office is *ex officio* intimately familiar with the Fourth Amendment warrant requirements contained in the U.S. Supreme Court precedents in *Riley v. California*, 573 U.S. 373, 134 S.Ct. 2473 (2014) and *U.S. v. Wilson*, 13F.4th 961 (9th Cir. 2021) and *Carpenter v. United States,* 585 U.S. 296*,* 138 S.Ct. 2206 (2018). In both cases, Chief Justice John Roberts squarely instructed law enforcement of the Court's public policy decision that in cases of doubt as to the reach of Fourth Amendment cyberdata searches of cellphone content, whether in "the cloud" or in a cellphone device, is to "get a warrant". The Court of Appeals in *U.S. v. Holmes,* 121 F.4th 727, 734-737 (9th Cir. 2024) applied this rule in suppressing evidence resulting from a warrantless viewing of CyberTip imagery by law enforcement and refusing to apply the "good faith exception". The Gasper case exemplifies the Wisconsin Attorney General Office's deliberate and intentional systemic decision to defy that constitutional mandate itself, and to instruct Wisconsin law enforcement personnel, including Detective Schroeder, not to follow that unequivocal constitutional mandate.

This is exactly the kind of systemic violation of the Fourth Amendment that the Supreme Court identified in *Riley* and *Carpenter* as requiring application of the exclusionary rule. To do otherwise tacitly endorses deliberate rejection of the Supreme Court's mandate to law enforcement authorities to "get a warrant" in cellphone internet cyberdata search cases.

CONCLUSION

The published Court of Appeals decision in the Gasper case should be overruled *in toto* and the circuit court's suppression order affirmed. This Court should announce that in the absence of a full, knowing, voluntary and unambiguous

waiver of constitutional rights under the Fourth Amendment, all ESP accountholders retain a "reasonable expectation of privacy" in their electronic accounts as to the government. Concurrently, this Court should hold that a constitutionally sufficient search warrant issued by a neutral and detached judicial officer is required prior to any governmental agent having access to user accounts of Electronic Service Providers.

Respectfully submitted this 30th day of July, 2025.

Attorneys for Defendant-Respondent-Petitioner:

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

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

CERTIFICATION AS TO FORM AND LENGTH OF BRIEF

I hereby certify that this Reply Brief conforms to the rules contained in Wis. Stat. §§ 809.19(8)(b)(bm), and (c) for a Reply Brief. The length of this brief is 2,995 words.

Dated at New Berlin, Wisconsin on July 30, 2025.

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