No. 2023AP002319-CR

In the Supreme Court of Wisconsin

STATE OF WISCONSIN,
Plaintiff-Appellant,

v.

MICHAEL JOSEPH GASPER,
Defendant-Respondent-Petitioner.

BRIEF OF NON-PARTY PROJECT FOR PRIVACY & SURVEILLANCE ACCOUNTABILITY, INC. AS *AMICUS CURIAE* IN SUPPORT OF DEFENDANT-RESPONDENT-PETITIONER

Gene C. Schaerr*
gschaerr@schaerr-jaffe.com
SCHAERR | JAFFE LLP
1717 K Street NW, Suite 900
Washington, DC 20006
Telephone: (202) 787-1060

**Pro hac vice* application pending

Caleb R. Gerbitz
(State Bar No. 1122558)
crg@mtfn.com
MEISSNER TIERNEY FISHER & NICHOLS S.C.
111 East Kilbourn Avenue
19th Floor
Milwaukee, WI 53202
Telephone: (414) 273-1300
Facsimile: (414) 273-5840

Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Constitutional Provision

Statutes

Other Authorities

INTRODUCTION AND INTEREST OF *AMICUS CURIAE*

The Fourth Amendment, properly understood, protects the public from warrantless searches of their data stored on a third party's server. Getting that question right is important to every Wisconsinite and to *amicus curiae* Project for Privacy & Surveillance Accountability, Inc. ("PPSA"), a nonprofit, nonpartisan organization dedicated to protecting privacy rights and guarding against an expansive surveillance state.

This Court will consider that question here and in *State v. Sharak*, No. 2024AP000469-CR. But these cases aren't quite identical twins. Here, unlike in *Sharak*, the government performed the first human search of any files. So even if the automated search performed by other parties was truly private, there was still a warrantless search here.

And allowing that warrantless search to stand could imperil the rights of nearly every Wisconsinite given the ubiquitous use of cloud storage. The Court of Appeals' conclusion here that Petitioner Michael Gasper lacked a reasonable expectation of privacy in data he uploaded to the cloud undermines the core policy concerns of the Fourth Amendment and is in tension with United States Supreme Court precedent, which has long condemned overbroad interpretations of the third-party doctrine—particularly regarding electronic data—in a line of cases culminating in *Carpenter v. United States*, 585 U.S. 296 (2018).

Carpenter recognized that the Fourth Amendment protects privacy interests that would have been recognized as reasonable at the Founding notwithstanding advances in technology that make such encroachments easier to do. *Id.* at 305, 316. Applying Founding Era privacy expectations, there can be no question that a person's merely storing property or information with third parties does not vitiate reasonable expectations of privacy against the government.

Nor can the government evade these expectations of privacy with shell games. When the government strongly incentivizes private actors to perform searches with one statute and mandates the reporting of suspicious results with another, a warning by the private third-party actor that it will comply with the law does not eliminate the reasonable expectation of privacy of cloud storage users. But even if it did, it would be irrelevant when, as here, the government expands beyond the scope of the nominally private search. And because Gasper had expectations of privacy in his data, no matter the seriousness of his crime, the Fourth Amendment required the government or its agents to obtain a warrant before searching it. This Court should reverse the lower court's contrary conclusion in an opinion that makes clear that the Fourth Amendment continues to place meaningful constraints on government overreach in the 21st Century.

STATEMENT

The facts here are initially almost identical to those in *Sharak*. Petitioner Michael Gasper had an account on Snapchat, *State of Wis. v. Gasper,* No. 2023AP2319-CR, slip. op. ¶2 (Wis. Ct. App. Oct. 30, 2024), a privacy-focused social media app with a distinguishing feature of automatically disappearing messages.[1] To use Snapchat, a user must check a box agreeing to a Terms of Service ("Terms") contract. Slip Op. ¶6. Had Gasper clicked an extra button during signup to open the Terms and read the 16-page agreement[2] very carefully, he would have found a buried warning: Snapchat will comply with a federal law mandating reporting child sexual abuse material ("CSAM") to the National Center for Missing and Exploited Children ("NCMEC"). *Id.* ¶¶6, 16-19.

The cases diverge after Snapchat's automated scans flagged a file Gasper uploaded as likely CSAM, Snapchat forwarded that file to NCMEC, and the NCMEC forwarded the file to law enforcement, *id.* ¶¶2-4. Unlike in *Sharak*, law enforcement was the first actor to perform a human review of the flagged file—though they similarly did so without

---

[1] *Snapchat Support, My Privacy, When does Snapchat delete Snaps and Chats?,* Snapchat, https://tinyurl.com/3u4x5xh4 (last visited June 24, 2025).

[2] *See* Gasper Br. at 29 (noting the "Terms of Service" are found in the record at "R-41, pp. 1-16").

obtaining a warrant. *Id.* ¶4. Based partially on this review, Gasper was arrested and charged with counts related to possession of CSAM. *Id.* ¶¶4-5.

Gasper moved to suppress the evidence from this search, arguing that the Fourth Amendment required the government to seek a warrant before searching his data. *Id.* ¶5. The trial court granted the motion, *id.* ¶7, but the Court of Appeals reversed, holding that Gasper lacked an expectation of privacy in files placed on his Snapchat account—particularly given the warnings of legal compliance in Snapchat's Terms. *Id.* ¶¶28-29.

ARGUMENT

Amicus agrees that Gasper's Fourth Amendment rights were violated. It separately emphasizes two points. First, the Fourth Amendment protects the degree of privacy that existed at the Founding despite advances in technology. *Carpenter*, 585 U.S. at 316. Because use of third-party electronic service providers ("ESPs") to store private information is ubiquitous, and resembles use of early mail and bailment services, there is a reasonable expectation of privacy in such information. An announcement by the third-party service provider that it will report illegal content stored with it—even content found pursuant to a private search—does not extinguish this expectation of privacy when the

reporting is legally mandatory. Second, and relatedly, when private reporting is mandated with significant penalties for noncompliance, such reports are state action, not private searches. But even if they *were* private searches, law enforcement cannot use them as a stepping-stone to later, more expansive searches without complying with the Fourth Amendment.

I. Snapchat Users—Like Users of Other Online Storage Applications—Have a Reasonable Expectation of Privacy in Their Account Information and Files.

Entrusting confidential communications to a third-party is a practice that predates the establishment of the first postal offices, and those who participate in that practice do not relinquish any reasonable expectation of privacy in the contents of those communications.

A. The Fourth Amendment reasonableness inquiry is historically grounded and accounts for advances in technology.

The analysis begins with the Fourth Amendment, which by its terms prohibits "unreasonable searches." U.S. Const. amend. IV. A Fourth Amendment search occurs when the government gets access to information or items over which a person has a subjective expectation of privacy if that expectation is objectively reasonable. *See Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The bar for a subjective expectation is so low it is rarely litigated; virtually any effort

at concealment suffices. *See Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978).

As to the objective expectation of privacy, reasonableness is "the ultimate touchstone." *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006) (citations omitted). The reasonableness inquiry, however, is not "open-ended." *Crawford v. Washington*, 541 U.S. 36, 67-68 (2004). A judge cannot, for example, "make difficult empirical judgments about the costs and benefits of [privacy] restrictions[.]" *Cf. N.Y. State Rifle & Pistol Ass'n, Inc. v. Bruen*, 597 U.S. 1, 25 (2022) (cleaned up). Rather, compliance with the Fourth Amendment "is measured in objective terms," *Ohio v. Robinette*, 519 U.S. 33, 39 (1996), and, as with other constitutional rights, is governed by the "historically fixed meaning" of a given right as "applie[d] to new circumstances," *Bruen*, 597 U.S. at 28. Put differently, the Fourth Amendment protects "that degree of privacy against government that existed when the Fourth Amendment was adopted," *Carpenter*, 585 U.S. at 305 (citation omitted), while applying that standard to new technology, *id.* at 313.

B. Disclosure to a third party is merely one factor in this reasonableness inquiry.

In addressing this historically grounded inquiry into reasonable expectations of privacy, *Carpenter* clarified that disclosure to a third

party does not automatically vitiate such expectations or the accompanying Fourth Amendment protections. 585 U.S. at 314. While the Court recognized that disclosing data to a third party can sometimes *diminish* an expectation of privacy over that data, even then the Court rejected any suggestion that "the fact of diminished privacy interests" meant that "the Fourth Amendment falls out of the picture entirely." *Ibid.* (cleaned up).

Carpenter also clarified that earlier third-party doctrine cases treated disclosure only as a relevant—though not dispositive—factor in the privacy inquiry. *See ibid.* (discussing *Smith v. Maryland*, 442 U.S. 735 (1979); then discussing *United States v. Miller*, 425 U.S. 435 (1976)).

C. Under the totality of the circumstances, social media users have a reasonable expectation of privacy in their private files and conversations.

At the Founding, entrusting property to third parties for a limited use, or "bailment," was common.[3] And there can be no question that—at the Founding—bailors as property owners maintained an expectation of privacy over property, including documents, entrusted to a bailee.[4]

---

[3] *See Carpenter*, 585 U.S. at 399-400 (Gorsuch, J., dissenting) (discussing "[t]hese ancient principles" (citing Joseph Story, *Commentaries on the Law of Bailments* §2 (Cambridge, Hilliard & Brown 1832))).

[4] *See* Br. for *Amicus Curiae* Professor Adam J. MacLeod, *Harper v. Faulkender*, No. 24-922 (U.S. Mar. 28, 2025), https://tinyurl.com/bdctth2r.

Indeed, one example of bailment involved use of the mails for private communications, the contents of which have long been recognized as protected by the Fourth Amendment. *Ex parte Jackson*, 96 U.S. 727, 733 (1877) ("Whilst in the mail, they can only be opened and examined under like warrant, ... as is required when papers are subjected to search in one's own household.").

As a growing chorus of federal courts have recognized, information stored online is analogous. Here, using Snapchat, distinguished by automatically-disappearing messages, establishes a subjective expectation of privacy. And that subjective expectation is objectively reasonable; users entrust private messages and media to platforms like Snapchat, expecting protection for their "confidential communications." *Heidi Grp., Inc. v. Tex. Health & Hum. Servs. Comm'n*, 138 F.4th 920, 935 (5th Cir. 2025); *see United States v. Zelaya-Veliz*, 94 F.4th 321, 333-34 (4th Cir. 2024) (private social media messages protected), *cert. denied mem.,* 145 S. Ct. 571 (2024); *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (emails protected).[5] This Court should join those courts and ensure that the privacy of Wisconsinites—and of all Americans—is

[5] *United States v. Miller,* 982 F.3d 412 (6th Cir. 2020), is not to the contrary. Indeed, the *Miller* court noted that it "would be rare" that any subscriber agreement defeats the expectation of privacy in email, before resolving the issue on private-search doctrine grounds. *Id.* at 426-27 (discussing *Warshak,* 631 F.3d at 286).

protected in the digital age like it was at the Founding rather than left "at the mercy of advancing technology" which enables automating even the most invasive of searches. *Carpenter*, 585 U.S. at 305 (citation omitted).

II. Snapchat's Warning That It Will Comply with Federal Law Does Not Extinguish the Reasonable Expectation of Privacy Over User Data.

There are two main reasons this Court should reject the State's contention that the warning in Snapchat's Terms that it scans for CSAM and will report what it finds to NCMEC extinguishes any privacy expectation. *See* State Reply Br. at 9, No. 2023AP2319-CR (Wis. Ct. App. May 7, 2024). First, the government should not be allowed to negate privacy expectations by mandating or coercing private actors to search and then hiding behind statements from those private actors that they will heed that mandate. Second, users retain privacy expectations even if a given provider's terms of service warn of intent to comply with laws requiring them to search their users' accounts. The government cannot, through a third party, condition using digital services essential to modern life on renunciation of Fourth Amendment rights.

A. The government cannot use private disclosure of a government mandate as an end-run around the Fourth Amendment.

As to the first point, if Snapchat's warning of its intent to comply with federal legal obligations eliminated that expectation of privacy, this would create easy end-runs around the Fourth Amendment. If the State were correct, although the government itself cannot announce it will search an area to eliminate privacy expectations, it could achieve the same result by mandating searches by private parties so long as they announce their compliance with the mandate.

Such a conclusion, however, is not—and cannot be—the law. It runs headlong into the general rule that the government cannot do indirectly what it cannot do directly. *See Students for Fair Admissions, Inc. v. President & Fellows of Harvard Coll.*, 600 U.S. 181, 230 (2023).

B. The government cannot require renunciation of Fourth Amendment rights to participate in essential aspects of modern life.

As to the second point, if the State were correct, one must surrender Fourth Amendment rights in digital data to use any provider subject to 18 U.S.C. §2258A. But the services offered by such providers are necessary for modern life, and the government may not condition access to such necessities on the renunciation of constitutional rights. *See, e.g.*, *Koontz v. St. Johns River Water Mgmt. Dist.*, 570 U.S. 595, 604

(2013) (collecting cases). While this doctrine has historically been applied to government services, the Supreme Court has emphasized in recent cases that the government may not require the renunciation of Fourth Amendment rights to participate in normal modern life. *See, e.g.*, *Carpenter,* 585 U.S. at 315 ("[C]ell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." (citation omitted)).

ESPs such as snapchat are both indispensable to modern life and contain vast amounts of intimate information, and thus fall squarely within this recent rule, especially given that social media is intertwined with First Amendment expressive rights as well. *See Packingham v. North Carolina*, 582 U.S. 98, 107 (2017) (recognizing the internet as a "modern public square" essential to First Amendment rights); *Stanford v. Texas*, 379 U.S. 476, 484-85 (1965) (noting First Amendment concerns result in heightened Fourth Amendment concerns).

III. The Search Here Was Not Private.

The government meaningfully expanded on the scope of the search by Snapchat and NCMEC by performing the first human review, and so even if the original automated scan was private, this human review was state action. And Snapchat's search here was not truly private, but

rather involved Snapchat acting as a government agent, for the same reasons that Google's search was government action in the *Sharak* case.[6]

A. When the government meaningfully expands on a private search, it must do so in compliance with the Fourth Amendment.

When a search is truly private, "authorities typically may repeat a private search already conducted by a third party but may not expand on it" without complying with the strictures of the Fourth Amendment. *United States v. Bebris*, 4 F.4th 551, 560 (7th Cir. 2021). But it is undisputed here that law enforcement performed the first human inspection of the files flagged by Snapchat. And even when files stored with Snapchat are scanned automatically, they are not exposed to human "employees in the ordinary course of business," and thus retain their general confidentiality against human review. *Heidi Grp.*, 138 F.4th at 935 (quoting *Miller*, 425 U.S. at 442).[7]

This human review "exceed[ed] the scope of the" initial scan by the ESP, transforming it into state action. *See, e.g., United States v.*

---

[6] *See* Br. of Non-Party Project for Privacy & Surveillance Accountability, Inc. as *Amicus Curiae* in Support of Def.-Appellant-Pet'r, *State v. Sharak,* No. 2024AP000469-CR (Wis. June 27, 2025) ("PPSA *Sharak* Br."), https://tinyurl.com/4zr27nd5.

[7] *Accord* Orin S. Kerr, *Data Scanning and the Fourth Amendment* 44-45 (Stanford L. Sch. Pub. L. & Legal Theory Rsch. Paper Series Working Paper, May 10, 2025), https://tinyurl.com/298pspym (arguing the scope of a Fourth Amendment search depends on what the "human observer [has] seen" or may infer).

Jacobsen, 466 U.S. 109, 116 (1984). Multiple federal courts have reached this same conclusion in nearly identical circumstances. *See, e.g.*, *United States v. Maher*, 120 F.4th 297, 314 (2d Cir. 2024) (holding that "the private search doctrine does not authorize a warrantless visual examination of that computer-matched image"); *United States v. Wilson*, 13 F.4th 961, 973 (9th Cir. 2021) (NCMEC); *United States v. Ackerman*, 831 F.3d 1292, 1306 (10th Cir. 2016) (NCMEC); *United States v. Lichtenberger*, 786 F.3d 478, 485 (6th Cir. 2015) (search by girlfriend of laptop); *United States v. Sparks*, 806 F.3d 1323, 1336 (11th Cir. 2015), *overruled on other grounds by United States v. Ross*, 963 F.3d 1056 (11th Cir. 2020).

This Court should join those courts and ensure that the rights of all Wisconsinites who use cloud storage are meaningfully protected, while "confident that NCMEC's law enforcement partners will struggle not at all to obtain warrants to open emails when the facts in hand suggest, … that a crime against a child has taken place." *Ackerman*, 831 F.3d at 1309.

B. Searches performed in compliance with an onerous government mandate are not private searches.

Further, as in *Sharak,* the initial automated search here was not truly private, but rather state action subject to the Fourth Amendment.

In short, 18 U.S.C. §2258A(e) imposes substantial fines—up to $850,000 per initial violation and up to $1 million for each subsequent violation—for failure to report CSAM detected by automated scans. And other laws, state and federal, effectively mandate the scanning that would detect them. *See, e.g.,* PPSA *Sharak* Br. at 17-19; *Doe #1 v. MG Freesites, LTD*, 676 F. Supp. 3d 1136, 1154-59 (N.D. Ala. 2022) (collecting cases noting it is unsettled if 18 U.S.C. §1595 imposes liability for hosting illegal content if the ESP "should have known" of it.).

Because both the scanning and reporting are required, *Skinner v. Ry. Lab. Execs.' Ass'n*, 489 U.S. 602, 614 (1989), and because "the immediate objective of the searches [is] to generate evidence for law enforcement purposes," *Ferguson v. City of Charleston*, 532 U.S. 67, 83-84 (2001), Snapchat's initial automated scans and reports are not private searches, but state action subject to the Fourth Amendment.

CONCLUSION

Protecting children from exploitation and abuse is a noble goal that can be accomplished by obtaining warrants when needed rather than by subjecting all Americans' private digital data to warrantless searches. Because the holding below could lead to that result, it should be reversed and the evidence from the warrantless search suppressed.

Respectfully submitted this 18th day of July, 2025.

Electronically Signed By

Caleb R. Gerbitz
Caleb R. Gerbitz
(State Bar No. 1122558)
crg@mtfn.com
MEISSNER TIERNEY FISHER & NICHOLS S.C.
111 East Kilbourn Avenue
19th Floor
Milwaukee, WI 53202
Telephone: (414) 273-1300
Facsimile: (414) 273-5840

Gene C. Schaerr*
gschaerr@schaerr-jaffe.com
SCHAERR | JAFFE LLP
1717 K Street NW, Suite 900
Washington, DC 20006
Telephone: (202) 787-1060

**Pro hac vice* application pending

Counsel for Amicus Curiae Project for Privacy & Surveillance Accountability, Inc.

CERTIFICATE OF COMPLIANCE

Pursuant to Wisconsin Statute §809.19(8g), I hereby certify that this brief conforms to the rules in §809.19(8)(b), (bm), and (c) for a brief produced with a proportional serif font. The length of this brief is 2,995 words.

Dated: July 18, 2025

Electronically Signed By

Caleb R. Gerbitz
Caleb R. Gerbitz
(State Bar No. 1122558)