FILED
06-27-2025
CLERK OF WISCONSIN
SUPREME COURT

No. 2024AP000469-CR

In the Supreme Court of Wisconsin

STATE OF WISCONSIN,

Plaintiff-Respondent,

v.

ANDREAS W. RAUCH SHARAK,

Defendant-Appellant-Petitioner.

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

Treatise

Other Authorities

INTRODUCTION AND INTEREST OF *AMICUS CURIAE*

The Fourth Amendment, properly understood, protects from warrantless searches 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.

The Court of Appeals' conclusion that petitioner Andreas Rauch Sharak had an expectation of privacy in data he uploaded to Google Photos best fits United States Supreme Court precedent and protects the core policy concerns of the Fourth Amendment. The United States Supreme Court 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 encroachments upon such interests easier. *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 coerces private actors to perform searches with one statute and mandates the reporting of any suspicious results with another, a warning by the private third-party actor that it will comply with the law does not eliminate the reasonable expectations of privacy of cloud storage users. And because Sharak had reasonable 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 those data. This Court should reverse the trial court in an opinion that makes clear that the Fourth Amendment continues to place meaningful constraints on government overreach in the 21st Century.

STATEMENT

Petitioner Andreas W. Rauch Sharak had an account with Google, Sharak Br. at 13, an Electronic Service Provider ("ESP") which leverages cloud storage to provide services ranging from email to spreadsheets to entertainment.[1] Many of these features, such as Google Photos, require password-protected accounts.[2] Had Sharak carefully read the lengthy

[1] *See Products*, Google, https://about.google/products/ (last visited June 23, 2025).

[2] *See Google Account Help, What is a Google Account*, Google, https://support.google.com/accounts/answer/15277265?hl=en (last visited June 23, 2025).

terms of service when creating his account, he would have found a buried warning: Google complies with a federal law mandating reporting child sexual abuse material ("CSAM") to the National Center for Missing and Exploited Children ("NCMEC") and performs automated scans. State Br. at 14 (citing R-App. 3–4).

One such scan flagged a file Sharak uploaded as likely CSAM. After an employee review, Google forwarded that file to the NCMEC, which, in turn, reviewed it and forwarded the file to law enforcement, which then opened the flagged file. *See* Sharak Br. at 12. But no one in this process sought a warrant. *Id.* Based in part on this forwarded file, Sharak was arrested and charged with counts related to possession of CSAM. *Id*. at 12–13.

Sharak moved to suppress the evidence from this search, arguing that the Fourth Amendment required the government (and its agents) to seek a warrant before searching his data. The trial court denied Sharak's motion, but the Court of Appeals certified, explaining it would have ruled that Sharak had a reasonable expectation of privacy in the data he uploaded to his Google account. State Br. at 11–12.

ARGUMENT

Amicus agrees with Sharak that his Fourth Amendment rights were violated. *Amicus* writes separately to emphasize 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 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 does not extinguish this expectation of privacy when the reporting is legally mandatory. Second, and relatedly, when private searching and reporting is coerced via threat of significant penalties for noncompliance, such reports are state action, not private searches.

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

Entrusting confidential communications to third parties is a practice predating 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 forces 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, the Supreme Court has explained that 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. And, 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, cloud service users have a reasonable expectation of privacy in their private files and conversations

At the Founding, moreover, 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] 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. And here, using Google Photos, distinguished by password-protected accounts, establishes a subjective expectation of privacy. *See United States v. Warshak*, 631 F.3d 266, 287–88 (6th Cir. 2010). And that subjective expectation is objectively reasonable; users

[3] *See Carpenter,* 585 U.S. at 399–400 (Gorsuch, J., dissenting) (discussing "[t]hese ancient principles" and 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.

entrust private messages and media to platforms like Google, expecting companies to protect 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); *Warshak*, 631 F.3d at 288 (emails protected).[5] This Court should join those courts and ensure that the privacy of Wisconsinites—and of all Americans—is 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. Google'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, even if Google acted as a government agent,[6] the warning in Google's Terms of Service ("Terms") that it scans for CSAM and will report what it finds to NCMEC extinguishes any privacy

[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 could defeat 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).

[6] As explained in Section III, Google's search was not private.

expectation. *See* State Br. at 19, 24–27. 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 Google's warning of its intent to comply with federal legal obligations eliminated expectations 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) (citing *Cummings v. Missouri,* 71 U.S. (4 Wall.) 277, 325 (1866)). And it also raises numerous other constitutional questions, such as whether it could require the searching party to violate its own Fifth Amendment rights against self-incrimination. *See United States v. Weekley*, 389 F. Supp. 2d 1293, 1298–99 (S.D. Ala. 2005) (collecting cases holding a misprision statute's disclosure requirements unconstitutional), *aff'd*, 184 F. App'x 903 (11th Cir. 2006) (unpublished).

Moreover, even if some searches were private, the Terms do not distinguish between scans conducted for truly private purposes and those conducted under legal compulsion.

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's theory were correct, it would effectively require surrendering Fourth Amendment rights in digital data to use any provider subject to 18 U.S.C. § 2258A. *See* State Br. at 26 ("If Google acted as a government agent, then its Terms of Service constituted a government policy that explicitly restricted Rauch Sharak's expectation of privacy in his account."). But the services offered by such providers are necessary for modern life, and the government may not condition access to such necessities on renunciation of constitutional

rights, as has long been recognized. *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, directly or indirectly, renunciation of Fourth Amendment rights—at least as to significant amounts of information—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)); *Riley v. California*, 573 U.S. 373, 403 (2014) (smartphones "hold for many Americans 'the privacies of life'" (citation omitted)).

Electronic Service Providers such as Google are both indispensable to modern life and contain vast amounts of intimate information. Such services thus fall squarely within this 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"); *Stanford v. Texas*, 379 U.S. 476, 484–85 (1965) (finding First Amendment concerns created heightened Fourth Amendment concerns).

III. Searches Performed in Compliance with an Onerous Government Mandate Are Not Private Searches.

Binding precedent, moreover, shows that the search here was not a private search, but state action subject to the Fourth Amendment.

The Fourth Amendment prohibits unreasonable searches by the government *or* private parties acting as government agents. *Skinner v. Ry. Lab. Execs.' Ass'n*, 489 U.S. 602, 614 (1989). A private entity becomes a state actor when the government exercises "coercive power" or provides "significant encouragement, either overt or covert," that effectively directs the private action. *Peery v. Chi. Hous. Auth.*, 791 F.3d 788, 789 (7th Cir. 2015) (quoting *Blum v. Yaretsky*, 457 U.S. 991, 1004 (1982)).

Regarding coercion, *Skinner* itself is instructive. There, the Court held that mandatory drug testing by private railroads constituted a government search because the government's regulations left the railroads no discretion to opt out of the testing. 489 U.S. at 615–16. Similarly, 18 U.S.C. § 2258A operates as a sword of Damocles that 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. *Id.* § 2258A(e).

And while § 2258A handles the reporting half of that equation, other laws, at least in practice, require scans. For instance, it is unsettled

whether ESPS are liable for illegal content including (but not limited to) CSAM under 18 U.S.C. § 1595 if the ESP "should have known" of it. *Doe #1 v. MG Freesites, LTD*, 676 F. Supp. 3d 1136, 1154–59 (N.D. Ala. 2022) (collecting cases). And at least one court has held—applying state law, but for an actor far less sophisticated than Google—that *having* software which *can* detect CSAM, but not using it, provided constructive knowledge of what it *could* have detected. *Doe v. XYC Corp.*, 887 A.2d 1156, 1160, 1166 (N.J. Super. Ct. App. Div. 2005); *see also A.B. v. Salesforce, Inc.*, 123 F.4th 788, 798–99 (5th Cir. 2024) (allowing claims to proceed where defendant "knew (or should have known)" that it was "providing back-office business services to a company … engaged in sex trafficking").

Thus, when the State notes that § 2258A "expressly relieves ESPs" of duties to scan, State's Br. at 41, it ignores what the totality of the law practically requires. The government may not avoid the Fourth Amendment's requirements with divide-and-conquer tactics.

Moreover, there was an intermediary step here. When scans flag files as CSAM, that arguably creates "circumstances from which there is an apparent violation[.]" 18 U.S.C. § 2258A(a)(2)(A). So any later human review of flagged files that are not exposed to "employees in the ordinary course of business[,]" *Heidi Grp.*, 138 F.4th at 935 (quoting *Miller*, 425

U.S. at 442),[7] is presumably done under legal compulsion. Google's pre-report review was thus not a private search, even if the scan was.

As to encouragement, when nominally private searches are coordinated with the government for prosecutorial ends, they are Fourth Amendment searches. In *Ferguson v. City of Charleston*, for example, the Court treated a public hospital's drug testing, coordinated with police, as a search despite patients agreeing to the test. 532 U.S. 67, 76 & n.9 (2001). The Court noted that the "distinction [which] is critical" about the program was that "the immediate objective of the searches was to generate evidence *for law enforcement purposes*[.]" *Id.* at 83–84. The same is true of the mandated reports to NCMEC here.

These cases compel only one conclusion: Google's scanning and reporting are not independent business decisions; they are direct responses to § 2258A's legal compulsion which therefore constitute state action governed by the Fourth Amendment's requirements.

CONCLUSION

Protecting children from exploitation and abuse is an extremely noble goal, but it can be done by obtaining warrants when needed rather

[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 a Fourth Amendment search's scope depends on what the "human observer [has] seen" or may infer).

than by subjecting all Americans' private digital data to warrantless searches. The trial court's decision should thus be reversed.

Respectfully submitted this 27th day of June, 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

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 2,992 words.

Dated: June 27, 2025

Electronically signed by

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