FILED
07-31-2025
CLERK OF WISCONSIN
SUPREME COURT

No. 2023AP2319-CR

IN THE SUPREME COURT OF WISCONSIN

STATE OF WISCONSIN,

Plaintiff-Appellant,

v.

MICHAEL JOSEPH GASPER,

Defendant-Resondent-Petitioner

ON REVIEW FROM A DECISION OF THE WISCONSIN COURT OF APPEALS REVERSING AN ORDER GRANTING SUPRESSION ENTERED IN WAUKESHA COUNTY CIRCUIT COURT, THE HONORABLE SHELLY J. GAYLORD, PRESIDING

BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION FOUNDATION AND AMERICAN CIVIL LIBERTIES UNION OF WISCONSIN FOUNDATION

Jennifer Lynch
(*pro hac vice pending)*
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francico, CA 94109

Counsel for Amicus Curiae Electronic Frontier Foundation

R. Timothy Muth
Bar No. 1010710
ACLU OF WISCONSIN FOUNDATION

207 E. Buffalo Street, Suite 325
Milwaukee, WI 53202

Counsel for Amici American Civil Liberties Union Foundation And American Civil Liberties Union Of Wisconsin Foundation

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

Constitutional Provisions

INTRODUCTION

The Fourth Amendment protects electronic documents, communications, and other files as the modern-day equivalent of papers and effects. *See Carpenter v. United States*, 585 U.S. 296 (2018). This is true whether those files or communications are stored on an individual's personal computer or with a third party. Fifteen years ago, the federal Sixth Circuit Court of Appeals held in *United States v. Warshak* that email stored with a third-party service provider "is the technological scion of," and deserves the same Fourth Amendment protections as, "tangible mail." 631 F.3d 266, 286 (6th Cir. 2010). And in *Carpenter*, all nine Justices agreed, as every Justice authored or joined an opinion acknowledging, that the Fourth Amendment protects the content of digital files and communications stored online. *See* 585 U.S. at 319 (majority op., Roberts, C. J., joined by Ginsburg, Breyer, Sotomayor, and Kagan, JJ.); *id.* at 332 (Kennedy, J., dissenting, joined by Thomas and Alito, JJ.); *id.* at 387, 400 (Gorsuch, J., dissenting).

This case raises the question of whether providers' terms of service ("TOS")—the form contracts between providers and their users—can vitiate users' Fourth Amendment rights as to the government. Contrary to the Court of Appeals ruling below, and consistent with *Warshak* and *Carpenter*, they cannot. Like the email provider in *Warshak*, Snapchat and every other major commercial electronic communications provider inform their users that they reserve the right to access user information to protect their interests, rights, and property. *See* 631 F.3d at 286. Notwithstanding those boilerplate imposed terms, in *Warshak*, the Sixth Circuit concluded that this corporate reservation of rights did not defeat an

individual's reasonable expectation of privacy in email when it comes to government searches. *Id*. As the Fourth District Court of Appeals in *State v. Sharak* explained, "the *Gasper* court's analysis . . . is not only contrary to existing precedent and legally incorrect, but it also undermines Fourth Amendment protections and falls short of providing a workable framework to guide future cases." No. 2024AP469-CR, unpublished slip op., *1 (WI App. Jan. 16, 2025).

Although this case involves child sexual abuse material ("CSAM"), the appellate court's rationale cannot be cabined to CSAM files. Providers' terms broadly apply to all user content they store, not just individual files and not just contraband. Therefore, from a Fourth Amendment standpoint, there is no meaningful distinction between the privacy interests vis-à-vis the government in the video Snapchat forwarded to NCMEC and the rest of Mr. Gasper's account. If Snapchat's TOS alone defeated Mr. Gasper's expectation of privacy in the one video, it would necessarily defeat it as to his entire account. If the appellate court's rationale stands, it would give service providers the ultimate power to determine individuals' constitutional privacy and property interests in any electronic "papers and effects" stored with the provider. This would be inconsistent with public expectations and contrary to well-recognized Fourth Amendment case law and the stated positions of all Supreme Court justices in *Carpenter*.

In reviewing this case and *Sharak*, this Court should make clear that people have a reasonable expectation of privacy in all of their uploaded

documents, photos, and electronic files, even if contraband, and regardless of private companies' TOS.

ARGUMENT

I. Third Party Electronic Service Providers are a Necessary Part of Everyday Life and Require Users to "Agree" to Their TOS.

It is nearly impossible to live and communicate in the modern world without relying on third party service providers to store and transmit our digital "papers and effects." Years ago, email largely replaced postal mail as a primary means of communication.[1] Today, the vast majority of Americans use and communicate via some form of social media.[2] By 2024, nearly two-thirds of U.S. adults under 30 used Snapchat,[3] and the platform reports it has more than 900 million monthly users.[4] And society's reliance on digital communication and cloud-stored data will only continue to grow.

Any data stored with a third-party service provider, including family photos, personal communications, and private documents, is subject to terms of service similar to the terms at issue in this case. Providers use TOS to protect their

---

[1] *See* United States Postal Service Office of Inspector General, *Analysis of Historical Mail Volume Trends*, 1 (Sept. 4, 2024) https://www.uspsoig.gov/sites/default/files/reports/2024-09/risc-wp-24-008.pdf (noting the volume of first-class mail fell 50 percent between FY 2008 and FY 2023, largely due to " instantaneous electronic alternatives").

[2] Pew Research Center, *Americans' Social Media Use* (Jan. 31, 2024) https://www.pewresearch.org/internet/2024/01/31/americans-social-media-use/

[3] *Id.*

[4] *Snapchat Surpasses 900 Million Monthly Active Users*, (Apr. 29, 2025) https://newsroom.snap.com/q1-2025-monthly-active-users.

business interests. *See Warshak*, 631 F.3d at 286. These terms offer protection against contractual and litigation risk, protect the business's rights and property, and limit the company's liability.[5] Given these benefits, it is no surprise businesses draft the TOS to give themselves broad latitude. Yet, these reservations of rights are never negotiated, and users have no choice but to click "I agree" just to engage in activities fundamental to modern life. *Riley v. California*, 573 U.S. 373, 385 (2014).

As with nearly every commercial service, Snapchat's TOS prohibits certain actions by users and permits the company access to its users' stored data. Snapchat's TOS allows the company to "access, review, screen, and delete [users'] content at any time and for any reason." *State v. Gasper*, 2024 WI App 72, ¶17, 16 N.W.3d 279, 284, 414 Wis. 2d 532, 543. Its Community Guidelines prohibit any activity involving CSAM as well as legal but perhaps undesirable acts such as spreading false information, "pretending to be someone (or something) you're not," posting "undisclosed paid or sponsored conduct," and spreading hate speech on the basis of a broad array of identities and statuses.[6]

These provider terms are industry-standard. For example, Dropbox's terms state it "may review [users'] conduct and content for compliance with these

[5] Lawyer Monthly, *Why Do Companies Continuously Update Their Terms & Conditions?* (Jan. 31, 2017), https://www.lawyer-monthly.com/2017/02/why-do-companies-continuously-update-their-terms-conditions.

[6] Snap, *Community Guidelines*, https://values.snap.com/policy/policy-community-guidelines

Terms and our Acceptable Use Policy[,]" and its Acceptable Use Policy prohibits CSAM, as well as other activities like advocating for bigotry or hatred, sending unsolicited communications or promotions, and storing anything defamatory or misleading.[7] The TOS for Google Drive allows Google to "review content to determine whether it is illegal or violates our Program Policies."[8] Apple's iCloud terms allow Apple to "access, use, preserve and/or disclose [users'] Account information and Content to law enforcement authorities."[9] And similar TOS apply to data gathered by our cars, televisions, and security cameras.[10] Lawyers will continue to draft similarly broad TOS terms to protect companies' business interests.[11]

II. Courts Widely Recognize Fourth Amendment Protections for Digital Communications and Other Stored Documents, Even if Accessible to Third-Party Providers.

Most courts to address the question recognize that people have a Fourth

---

[7] *Dropbox Terms of Service* (Jan. 7, 2025) https://www.dropbox.com/terms; *Acceptable Use Policy*, https://www.dropbox.com/acceptable_use. *Cf. State v. Bowers*, 405 Wis. 2d 716 (2022) (recognizing users' privacy interest in files stored with Dropbox).

[8] Google Drive, *Google Drive Additional Terms of Service*, § 1 (Mar. 31, 2020), https://www.google.com/drive/terms-of-service/.

[9] Apple, *Welcome to iCloud*, § V(E) https://www.apple.com/legal/internet-services/icloud/en/terms.html.

[10] *See, e.g.,* Ring, *Ring Terms of Service ,* https://ring.com/terms ; Onstar, *User Terms*, https://static-content.onstar.com/OnStarMobileTerms/OnStarMobileTerms.htm; Samsung, *Terms of Service*, § 5.3, https://www.samsung.com/us/apps/samsung-members/terms-of-service/.

[11] *See* Lawyer Monthly, *supra* note 5.

Amendment interest in the contents of their digital communications and records, including those stored with or transmitted by third parties. *See, e.g.,City of Ontario v. Quon*, 560 U.S. 746, 760 (2010); *Riley*, 573 U.S. at 395; *State v. Bowers*, 2023 WI App 4, ¶45, 985 N.W.2d 123, 141, 405 Wis. 2d 716, 750 (user had reasonable expectation of privacy in Dropbox account); *United States v. Mohamud*, 843 F.3d 420, 442 (9th Cir. 2016) ("With respect to a U.S. person's privacy interest, we treat emails as letters."). Merely entrusting digital "papers" and "effects" to an intermediary does not defeat the reasonable expectation that the contents of the materials will remain private. *See Carpenter*, 585 U.S. at 319 ("If the third-party doctrine does not apply to the 'modern-day equivalents of an individual's own 'papers' or 'effects,'' then the clear implication is that the documents should receive full Fourth Amendment protection."); *United States v. Maher*, 120 F.4th 297 (2d Cir. 2024)(recognizing expectation of privacy in digital files stored with Google); *United States v. Ackerman*, 831 F.3d 1292, 1308 (10th Cir. 2016) (email attachments sent via AOL protected under both an expectation-of-privacy and a trespass-to-chattels theory). Because people now conduct much, if not all, of their personal and professional business electronically, courts recognize that obtaining access to a person's online files would allow the government to examine not just a handful of selected files in a file cabinet or photos in an album, but years' worth of highly personal information.

Historically, the Fourth Amendment protected physical mail despite the fact that at any point a mail carrier could open a letter and examine its contents.

See Warshak, 631 F.3d at 285 (*citing United States v. Jacobsen*, 466 U.S. 109, 114 (1984)). It similarly protected telephone conversations even though the telephone company could "listen in when reasonably necessary to 'protect themselves and their properties against the improper and illegal use of their facilities.'" *Id.,* 631 F.3d at 285, 287 (citing *Smith*, 442 U.S. at 746). Today's third-party electronic service providers like Snapchat are the "functional equivalent" of post offices and phone companies; they make "email [and other text-based] communication possible." *Id.* at 286.

As the *Warshak* and *Sharak* courts recognized, Fourth Amendment protection for private documents stored with third parties finds further support "in the application of Fourth Amendment doctrine to rented space." *Warshak* at 287; *Sharak,* No. 2024AP469-CR, *6. "Hotel guests, for example, have a reasonable expectation of privacy in their rooms . . . even though maids routinely enter hotel rooms to replace the towels and tidy the furniture."*Warshak* at 287 (citations omitted); *see also Stoner v. California*, 376 U.S. 483, 490 (1964); *Chapman v. United States*, 365 U.S. 610 (1961) (holding that a warrantless search of renter's house with only the landlord's consent was unconstitutional). A third party's ability to access private materials does not necessarily defeat the owner's privacy interest in those materials.

III. A Service Provider's TOS Does Not Defeat its Users' Reasonable Expectations of Privacy in Their Digital Papers.

The court below held that Mr. Gasper had no constitutionally protected

expectation of privacy in files stored with Snapchat because the company's TOS advised him that it prohibited illegal activity and permitted the company to access data at any time. However, while a private document like Snapchat's TOS may govern the provider's relationship with the user, it cannot vitiate the user's Fourth Amendment rights against the government. This is just as true for a single image that may be considered contraband as it is for all content in a user's account.

The expectation of privacy analysis is intended to describe "well-recognized Fourth Amendment freedoms," *Smith*, 442 U.S. at 740 n. 5, not the interests of private businesses as advanced by terms that are often buried on a website or in an app. The fact that a private entity reserves the right to interdict illegal activity to protect its own business interests does not enable the government to search emails and documents on the platform without a warrant.[12]

Just as in this case, in *Warshak*, the email service provider reserved the right to access emails under its Acceptable Use Policy. 631 F.3d at 287. Nevertheless, the Sixth Circuit found that provision did not impact Warshak's

[12] When a private company acting on its own discovers contraband and reports it to law enforcement, courts allow the government to review the disclosed information without first obtaining a warrant as long as the government's access does not exceed the scope of the private search. *See United States v. Ackerman*, 831 F.3d 1292, 1305 (10th Cir. 2016); *see also United States v. Wilson*, 13 F.4th 961, 974 (9th Cir. 2021) (government search exceeded scope of private search); *United States v. Maher*, 120 F.4th 297 (2d Cir. 2024) (same). But the reservation of a right to access user content by a private company does not give the *government* the ability to conduct its own warrantless search to seek information that has not already been lawfully provided to it.

reasonable expectation of privacy in his email. *Id.*[13] Similarly, in *Byrd v. United States*, 584 U.S. 395 (2018), the Supreme Court held that contractual terms in a rental car contract did not constrain privacy rights as against the government. Car-rental agreements are filled with long lists of restrictions that have nothing to do with a driver's reasonable expectation of privacy in the car. *Id*. at 407-08. Rental agreements, like terms of service, "concern risk allocation between private parties. . . . But that risk allocation has little to do with whether one would have a reasonable expectation of privacy in the rental car if, for example, he or she otherwise has lawful possession of and control over the car." *Id*.

Just as the Supreme Court has cautioned "that arcane distinctions developed in property and tort law" ought not to control the analysis of who has a "legally sufficient interest in a place" for Fourth Amendment purposes, *Rakas v. Illinois*, 439 U.S. 128, 142 (1978), courts have repeatedly declined to find private contracts to be dispositive of individuals' expectations of privacy. In *Smith*, for example, the Supreme Court noted, "[w]e are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation." *Smith*, 442 U.S. at

[13] Under the appellate court's reasoning, an online service provider is put to the untenable choice between protecting its users' privacy interests and its own business. If a provider chooses to police its platform for illegality or other misconduct, it vitiates its users'expectations of privacy and leaves them open to warrantless, suspicionless searches by the government. But if it chooses the alternative, the company could end up allowing criminal conduct to run on its service unabated.

745. Similarly, in *United States v. Owens*, the Tenth Circuit did not let a motel's private terms govern the lodger's expectation of privacy, noting, "[a]ll motel guests cannot be expected to be familiar with the detailed internal policies and bookkeeping procedures of the inns where they lodge." 782 F.2d 146, 150 (10th Cir. 1986); *see also State v. Subdiaz-Osorio*, 2014 WI 87, ¶61, 357 Wis. 2d 41, 77, 849 N.W.2d 748, 766 (Prosser, J.) ("It is untenable to contend that a search under the Fourth Amendment depends on the specific language in an individual's cell phone policy").

As all of these courts have well understood, privacy rights in electronic data stored with third parties are meaningless if a service provider's non-negotiated terms of service can subvert them. Endorsing the appellate court's reasoning below would not only conflict with prevailing and persuasive legal authority—it would create a patchwork of legal protections for users of any service that stores or transmits users' content. *See Warshak*, 631 F.32 at 287; *Smith*, 442 U.S. at 745 ("crazy quilt"). And the appellate court's rule would be an almost-impossible challenge to implement for both law enforcement and for service providers who operate across the entire United States, as Fourth Amendment protections would rise and fall depending on different courts' interpretations of different service providers' usage policies at different points in time. *See Riley*, 573 U.S. at 398 (Fourth Amendment favors "clear guidance to law enforcement through categorical rules"). Customers of one company would enjoy Fourth Amendment rights, while customers of another, would not. That approach is not workable for

the government or the public—and it is clear that the Fourth Amendment rejects it. *See Smith*, 442 U.S. at 745.

IV. A Rule Linking Users' Fourth Amendment Rights to Companies' TOS Cannot Be Cabined to Contraband Material.

The appellate court suggested that Snapchat's policies diminished Mr. Gasper's expectation of privacy *solely* in the illegal content in his account. *Gasper*, 2024 WI App 72, ¶28. But this distinction does not hold up to logical scrutiny. Snapchat's "Community Guidelines" are not limited to prohibiting "nude or sexually explicit content involving anyone under the age of 18;" *id.* at ¶18, they "apply to all users" and allow it access to "all content."[14] If Snapchat's TOS defeats a user's expectation of privacy, it would do so for *all* records and communications in the users' entire account, not just the contraband material. *See United States v. Maher*, 120 F.4th 297, 308 (2d Cir. 2024) (disagreeing with similar government argument and holding Google's TOS "did not extinguish Maher's reasonable expectation of privacy in that content as against the government").

Further, the search cannot be justified by the fact CSAM was identified. The Supreme Court has held that "a warrantless search [can]not be characterized as reasonable simply because, after the official invasion of privacy occurred, contraband is discovered." *Jacobsen*, 466 U.S. at 114. Individuals retain a

[14] Snap, *Community Guidelines*, https://values.snap.com/policy/policy-community-guidelines

reasonable expectation of privacy in their papers, effects, and houses even when criminal activity is ongoing. *See e.g. id.* (reasonable expectation of privacy in parcel containing cocaine); *Byrd*, 138 S. Ct. 1518 (reasonable expectation of privacy in rental car containing heroin); *Owens*, 782 F.2d at 150 (reasonable expectation of privacy in hotel room containing cocaine).

The same is true with Mr. Gasper's Snapchat account. There is no logical line to draw that leaves evidence of illegal activity outside of the Fourth Amendment, and the rest of the private, sensitive, intimate details of one's life held in an online account within its protections.

CONCLUSION

For the reasons above, the Court should decline to adopt the appellate court's reasoning and instead hold that Mr. Gasper had a reasonable expectation of privacy in all content stored in his Snapchat account.

Respectfully submitted,

Electronically signed by R. Timothy Muth
Bar No. 1010710
ACLU OF WISCONSIN FOUNDATION

Jennifer Lynch
(pro hac vice pending)
ELECTRONIC FRONTIER FOUNDATION

Counsel for Amici Electronic Frontier Foundation, American Civil Liberties Union Foundation And American Civil Liberties Union Of Wisconsin Foundation

FORM AND LENGTH CERTIFICATION

I hereby certify that this brief conforms to the rules contained in Wis. Stat. § 809.19 (8) (b), (bm), and (c) for a brief produced with serif font. The brief is set in 13-point Times New Roman font. The length of this brief is 2946 words.

EFILE/SERVICE CERTIFICATION

I certify that in compliance with Wis. Stat. § 801.18(6), I electronically filed this document with the clerk of court using the Wisconsin Supreme Court Electronic Filing System, which will accomplish electronic notice and service for all participants who are registered users.

Dated: July 31, 2025.

Electronically signed by:

/s/ R. Timothy Muth_____

R. Timothy Muth
State Bar. No. 1010710
ACLU of Wisconsin Foundation, Inc.
Counsel for amici