FILED
08-01-2025
CLERK OF WISCONSIN
SUPREME COURT

Supreme Court of Wisconsin

NO. 2023AP2319-CR

STATE OF WISCONSIN,

Plaintiff-Appellant,

v.

MICHAEL JOSEPH GASPER,

Defendant-Respondent-Petitioner.

Appeal No. 2023AP2319-CR
Waukesha County Circuit Court Case No. 2023CF470
Hon. Shelley J. Gaylord

NON-PARTY BRIEF OF *AMICI CURIAE* GOOGLE LLC, SNAP INC., AND MICROSOFT CORPORATION

Jeffrey L. Fisher*
O'MELVENY & MYERS LLP
2765 Sand Hill Road
Menlo Park, California 94025
Phone: (650) 473-2600
jfisher@omm.com

Jonathan P. Schneller*
Waseem Salahi*
O'MELVENY & MYERS LLP
400 South Hope Street
Los Angeles, California 90071
Phone: (213) 430-6000
jschneller@omm.com
wsalahi@omm.com

Counsel for Google LLC and Snap Inc.

Andrew T. Dufresne, SBN 1081409
PERKINS COIE LLP
33 E. Main Street, Suite 201
Madison, Wisconsin 53703
Phone: (608) 663-7460
adufresne@perkinscoie.com

Counsel for Google LLC, Snap Inc., and Microsoft Corporation

*admitted *pro hac vice*

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES (cont'd)

Page(s)

TABLE OF AUTHORITIES (cont'd)

Page(s)

OTHER AUTHORITIES

INTEREST OF *AMICI CURIAE*

Amici Google LLC ("Google"), Snap Inc. ("Snap"), and Microsoft Corporation ("Microsoft") submit this brief solely to address the legal question of how a service provider's terms of service ("ToS") fit into a Fourth Amendment analysis of digital searches. This question has widespread implications for digital services, users, and law enforcement. As leading global digital services providers and innovators in user privacy, security, and transparency, *Amici* have an interest in ensuring that the answer is principled, workable, and consistent with technological realities and user expectations of privacy vis-à-vis the government. Ultimately, *Amici* offer unique first-hand insight into the complex legal and practical issues raised by the interplay between ToS and privacy rights in relation to government actions.

In submitting this brief, *Amici* take no position on the conduct of this particular defendant or whether the record before the court establishes violations of the Fourth Amendment.

INTRODUCTION

ToS play a crucial role in the provision of digital services. They define the services offered by the provider and establish which uses of a digital platform are permissible and which are not. In short, they represent the ground rules for the provision and use of digital services.

This case asks what bearing those rules have on technology users' Fourth Amendment rights. The correct answer, both as a doctrinal matter and as a matter of good policy, is none. Individuals' reasonable privacy expectations vis-à-vis the government turn on historical precedents and societal understandings, not private contracts. ToS, which are functional agreements that set mutual expectations between private parties, therefore cannot dictate the Fourth Amendment's boundaries. Nor should they. Treating ToS as constitutionally dispositive would divorce Fourth Amendment law from settled social expectations and undermine values that are—and should remain—the foundation of digital services: security, transparency, innovation, and freedom of expression.

However it disposes of these cases, this Court should clarify that ToS have no bearing on Fourth Amendment rights.

ARGUMENT

The Fourth Amendment's protections do not turn on ToS. That is true under both a straightforward application of Fourth Amendment doctrine and as a matter of common sense and good policy.

I. ToS cannot define Fourth Amendment rights because they do not define reasonable privacy expectations vis-à-vis the government.

The Fourth Amendment provides "rights against the government," not private parties. *Hiibel v. Sixth Jud. Dist. Ct. Nev.*, 542 U.S. 177, 187 (2004). That distinction in one sense constrains the Amendment's protections by rendering it "wholly inapplicable" to unreasonable private searches. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). But in another sense, it operates as an important check on government: The "touchstone of Fourth Amendment analysis" is a person's "reasonable expectation of privacy.'" *Oliver v. United States*, 466 U.S. 170, 177 (1984) (quoting *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)). That

inquiry is not about privacy from just *anyone*. Rather, the key question is whether, "in light of all the circumstances," an individual has a "reasonable expectation of freedom from *governmental* intrusion." *Mancusi v. DeForte*, 392 U.S. 364, 368 (1968) (emphasis added); Orin S. Kerr, *Terms of Service and Fourth Amendment Rights*, 172 U. Pa. L. Rev. 287, 304–07 (2024).

Courts have thus held that an individual's Fourth Amendment rights are not extinguished by the individual sharing their space with or opening it up to other private parties. In *Mancusi*, for example, the Supreme Court held that an employee had a reasonable privacy expectation from government intrusion in his office, even though it "consisted of one large room, which he shared with several other union officials," and even though the government took records from a part of the office not "reserved for his exclusive personal use." 392 U.S. at 368. The Court explained that the employee "could reasonably have expected that only those persons and their personal or business guests would enter the office," which expectation "was inevitably defeated by the entrance of [and

search by] state officials." *Id.* at 369; *see In re John Doe Proceeding*, 272 Wis. 2d 208, 237 (2004) (applying *Mancusi* to digital records).

The distinction between expectations of privacy from private versus governmental parties is a touchstone of Fourth Amendment law. It explains why the Fourth Amendment protects privacy in hotel rooms, even if hotel staff are expected to enter. *See United States v. Allen*, 106 F.3d 695, 699 (6th Cir. 1997) (motel guest's reasonable privacy expectation was not vitiated by motel manager's ability to examine room); *United States v. Stokes*, 733 F.3d 438, 446 (2d Cir. 2013) (similar); *State v. Munroe*, 244 Wis. 2d 1, 8–9 (Wis. Ct. App. 2001) ("The protection afforded by [the Fourth Amendment] extends to hotels and motels . . . ."). And it explains why individuals can reasonably expect privacy from the government in shared domestic spaces, even if a housemate or landlord might enter at any time. *See Georgia v. Randolph*, 547 U.S. 103, 113–15 (2006); *O'Connor v. Ortega*, 480 U.S. 709, 730 (1987) (Scalia, J., concurring); *State v. Trecroci*, 246 Wis. 2d 261, 283–84 (Wis. Ct. App. 2001) (recognizing reasonable privacy expectation

in shared stairway of multi-dwelling unit). Even *Katz*, which created the "reasonable expectations" test, turned on this private-government distinction, recognizing the reasonable expectation that calls in public phone booths would be free from government intrusion, even though operators could listen in. *See* 389 U.S. at 511; *United States v. Warshak*, 631 F.3d 266, 287 (6th Cir. 2010) (discussing this aspect of *Katz*). In each of these contexts, courts recognized that privacy expectations against the government do not necessarily turn on expectations about private conduct. *See, e.g.*, *Katz*, 389 U.S. at 352 (citing other examples where individuals may expect privacy in shared spaces, including friend's apartment and taxicab).

That does not change when expectations about private conduct are formalized in a written agreement. Courts have thus rightly declined to allow agreements between private parties to define Fourth Amendment boundaries. In *Byrd v. United States*, 584 U.S. 395 (2018), for example, the Supreme Court rejected the government's theory that using a rental car in violation of the rental

agreement vitiated the driver's privacy expectations in the car, reasoning that because the contract "concern[ed] risk allocation *between private parties*," it "ha[d] little to do with whether one would have a reasonable expectation of privacy in the rental car." *Id.* at 408 (emphasis added). In *United States v. Washington*, 573 F.3d 279 (6th Cir. 2009), the Sixth Circuit applied a similar principle to an apartment lease. A tenant's privacy expectation in his apartment, it held, did not disappear merely because he used the apartment in violation of lease terms, including the requirement to pay rent. *Id.* at 284. The upshot is that functional agreements between private parties do not define their respective Fourth Amendment rights.

ToS should be treated no differently. To begin, electronic communications are "the modern-day equivalents of an individual's own papers and effects," and thus "should receive full Fourth Amendment protection." *Carpenter v. United States*, 585 U.S. 296, 313–16 (2018); *accord Warshak*, 631 F.3d at 286–87. Indeed, such communications bear all the hallmarks that led the U.S. Supreme

Court in *Carpenter* to recognize a privacy expectation in cellphone location records. An individual's messages on digital platforms can provide "an all-encompassing record" of her associations and activities, *Carpenter*, 585 U.S. at 311, spanning everything from her political leanings and religious beliefs to her dating life and consumer tastes, *see Warshak*, 631 F.3d at 284 ("Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button."). Such "an intimate window into a person's life," enabled by digital records that are "detailed, encyclopedic, and effortlessly compiled," *Carpenter*, 585 U.S. at 309, 311, "requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve," *Warshak*, 631 F.3d at 286.

An internet user's agreement to a platform's ToS does not change the well-founded expectation that such an extensive collection of sensitive communications will remain private from the government absent a warrant supported by probable cause. Like

leases and car rental agreements, ToS are functional, private agreements. Their purpose is to ensure platform safety, clarify permissible uses of the technology, and enable companies to maintain reliable and lawful services. They achieve that purpose by outlining platforms' expectations for users and users' expectations for platforms—*not* user expectations of privacy from the government. Google's ToS thus condition a user's "permission . . . to access and use [Google's] services" on compliance with the terms, which, among other things require "comply[ing] with applicable laws," *see* Google Terms of Service at 4, https://policies.google.com/terms; prohibit "abuse [of Google's] services," including "introducing malware" or "reverse engineering [its] services," *id.* at 5; and reserve Google's "right to take down . . . content in accordance with applicable law," *id.* at 15; *see also* Snap Terms of Service, §§ 8, 10 (similar), https://www.snap.com/terms; Snap Community Guidelines (providing "specific rules for [prohibited] content," detailing prohibition on illegal activities, and reserving Snap's "right to . . . remove any content"), https://values.snap.com/policy/policy-

community-guidelines; Microsoft Terms of Use, "Use of Services" (similar), https://www.microsoft.com/en-us/legal/terms-of-use. The ToS also inform users that Google may publish or reproduce user content, Google ToS at 7–8; or access user data to "creat[e] new features and functionalities," *id.* at 8; *see also* Snap Terms of Service, § 2 (similar); Snap Privacy Policy (describing how Snap uses user data), https://values.snap.com/privacy/privacy-policy. ToS thus set the terms of platforms' relationship with their users. Nowhere do those terms purport to define users' privacy relationships with the *government*.[1]

ToS thus fundamentally differ from the eviction orders to which the State analogizes them. App. Br. 24-25. An order of eviction entirely erases the tenant's right to exclude—and hence privacy expectations—as to the world at large. App. Br. 24-25. ToS, in stark contrast, grant a *private party* access to user data for a *limited, clearly defined set of purposes*, such as abuse detection,

[1] For the same reason, ToS play no role in determining the applicability of the private-search doctrine, which hinges on the *fact* of the previous search, not *permission* to conduct it. *See Jacobsen*, 466 U.S. at 121.

fraud prevention, internal diagnostics, or enforcement of community guidelines.[2] Just as arrangements allowing a landlord to inspect a unit or cotenants to access shared spaces do not vitiate Fourth Amendment rights, an agreement granting a *provider* limited access is not an invitation *to the government* to comb through a user's inbox.

Indeed, the Fifth Circuit recently held that even where a private party had agreed to contract terms granting *the government* "unrestricted access" to its private records, it would be "absurd to say that [the] contract" gave state officials an "unlimited right" to access the private party's online Dropbox folders at any time and in any way the government chose. *See Heidi Grp., Inc. v. Tex. Health & Hum. Servs.*, 138 F.4th 920, 936 (5th Cir. 2025). That absurdity—that a contractual right of access could so effortlessly

---

[2] *See, e.g.*, Google Drive Additional Terms of Service § 2 ("We may review content to determine whether it is illegal or violates our Program Policies . . . But that does not necessarily mean that we review content, so please don't assume that we do."), available at https://www.google.com/drive/terms-of-service/; Snap Terms of Service §§ 2, 10 (similar); Microsoft Terms of Use, "Use of Services" (similar).

vitiate an individual's Fourth Amendment rights—is amplified tenfold when the counterparty to the contract is not the government but the provider of an electronic communications service.

Nearly every major online platform has ToS permitting it to access user communications and, in appropriate circumstances, divulge those communications to law enforcement. Making those ToS constitutionally determinative would erode the Fourth Amendment's protections for the entire technology-using public, and with respect to communications that may provide "a detailed and comprehensive record" of a speaker's associations, activities, and beliefs. *Carpenter*, 585 U.S. at 309. It is implausible to suggest that by contracting with a private company to use technology that is "a pervasive and insistent part of daily life," *Riley v. California*, 573 U.S. 373, 385 (2014), the user forfeits their expectation that

such sensitive communications will be kept private from the government.[3]

In addition to unsettling reasonable privacy expectations in relation to the government, conditioning Fourth Amendment rights on the terms of internet platforms' user agreements would create a confusing and unstable patchwork of privacy protections. A user's privacy rights could vary depending on which online platform she uses: while one platform's carefully written disclosures might prompt a court to restrict the user's Fourth Amendment rights, another platform's silence might avoid that result. And the user's rights will also be subject to constant (and wholly

[3] The State's bailment analogy does not alter the Fourth Amendment analysis. *See* App. Br. 20–23. The State contends that because use of Snapchat creates a "bailment," a court must "look[] to the contract between the parties"—*i.e.*, the ToS—to determine users' privacy expectations. *Id.* at 22. But even if storing data with a provider established a bailment (a point that is far from settled), that relationship would define only the rights between the user and provider—not the user and the *government*, a non-party to the contract. The State's example of a textbook bailment—a car in a parking lot—illustrates the point: Vehicle owners retain Fourth Amendment rights when they entrust them to parking lot operators, *see, e.g.*, *United States v. Washburn*, 383 F.3d 638, 641–42 (7th Cir. 2004) (analyzing search of vehicle in parking lot under Fourth Amendment automobile exception), and no Fourth Amendment principle would support a different rule if a valet claim ticket reserved the right to inspect a vehicle or report contraband to law enforcement.

unpredictable) change: If ToS dictate the Fourth Amendment's scope, a platform could shift the privacy landscape, often dramatically, any time it updates its ToS. The result would be a tangle of Fourth Amendment protections dictated by the ToS drafting practices of thousands of private corporations. That is confusing and destabilizing for users and would untether the Fourth Amendment from underlying societal expectations of privacy from the government. *See Kyllo v. United States*, 533 U.S. 27, 34 (2001) (emphasizing need to enforce established privacy expectations in new technological contexts). It would also undermine the clarity and administrability that constitutional protections are meant to provide, requiring law enforcement to navigate distinctions embedded in detailed ToS to determine their constitutional obligations. *See Virginia v. Moore*, 553 U.S. 164, 175 (2008) (emphasizing importance of "administrable rules" in Fourth Amendment context).

II. Treating ToS as determinative of privacy expectations would undermine security, transparency, technological innovation, and online expression.

In addition to violating prevailing Fourth Amendment principles, tying constitutional privacy expectations from government intrusion to platforms' ToS would be practically unworkable. Modern digital services depend on user trust that platforms will keep data secure, be transparent about how it is used, and build tools that improve safety and user experience. Interpreting ToS as abrogating users' Fourth Amendment rights would distort that trust-based relationship and produce harmful consequences for society and the digital economy.

First, users will be forced to choose between security and constitutional privacy. Users expect the platforms they use to be safe from malicious actors and cyber threats. To meet that expectation, platforms engage in limited scanning or review—for example, to detect child sexual abuse material, stop account takeovers, block malware, or mitigate spam. *See supra* at 16 n.2. And to preserve user trust, platforms tell their users—via the ToS—that they

will use certain scanning tools and may report bad actors to law enforcement. Users, in turn, consent to those practices because they understand that security is an inherent part of the service provided, and that such interventions are essential to preserving a secure service. In other words, in accepting ToS like *Amici*'s, users accept the tools needed to keep the service safe—*not* a license for the government to intrude on their privacy. If these security tools undermined privacy expectations against the government, it would force users into a binary with no acceptable alternative: either demand robust (and transparent) security or preserve constitutional privacy, but not both. That is a no-win situation. Privacy and security are mutually reinforcing pillars of trustworthy digital services. The Fourth Amendment should not pit them against each other.

Tying Fourth Amendment protections to ToS would also chill the advancement of online security technologies and facilitate problematic uses. As bad internet actors become increasingly sophisticated, the need for innovative, user-protective tools becomes

ever more important. *See, e.g.*, Google, *White Paper: Tackling Scams and Fraud Together* at 8, 19–25 (Dec. 2024), https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Tackling_scams_and_fraud_together.pdf. But if ToS reserving the provider's rights to secure its platform—including by reporting bad actors to law enforcement—were held to vitiate Fourth Amendment rights, companies would hesitate to launch new security tools and law enforcement collaborations for fear that such advances could be later interpreted as inviting government searches. And bad actors will have every incentive to migrate to platforms that have less robust security features and that do not scan for harmful content. This dynamic risks discouraging progress and harming users in the long run. The Fourth Amendment should serve as a limit on government power—not a deterrent to technological innovation by companies.

A Fourth Amendment analysis that turns on ToS will also threaten online expression. Users will be less willing to speak, share, or create online if they believe their communications and

documents fall into a constitutional gray area because of how a platform's ToS describes its operations. The perception that online spaces offer only conditional privacy from government intrusion will deter open engagement and expressive freedom. *See United States v. Jones*, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) ("Awareness that the government may be watching chills associational and expressive freedoms"). Such effects have been well documented. *See, e.g.*, Jonathon Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 Berkeley Tech L.J. 117 (2016). That undermines not only user trust and innovation, but also the democratic and participatory values that the Fourth Amendment was designed to protect. *See Marcus v. Search Warrants of Prop. at 104 E. Tenth St., Kansas City, Mo.*, 367 U.S. 717, 729 (1961) ("[U]nrestricted power of search and seizure could also be an instrument for stifling liberty of expression.").

Digital platforms serve as essential venues for thought, dissent, creativity, and connection. If users feel that, notwithstanding societal privacy expectations, their activity is subject to

government scrutiny simply because of how a platform describes its own practices, they may self-censor or disengage entirely. Such a result would contradict both Fourth Amendment doctrine and its underlying values.

CONCLUSION

The Court should therefore hold that ToS have no bearing on individuals' Fourth Amendment privacy rights in digital searches.

Dated this 1st day of August 2025.

Respectfully submitted,

Electronically signed by Jonathan P. Schneller
Jonathan P. Schneller*
Waseem Salahi*
O'MELVENY & MYERS LLP
400 South Hope Street
Los Angeles, California 90071
Phone: (213) 430-6000
jschneller@omm.com
wsalahi@omm.com

Jeffrey L. Fisher*
O'MELVENY & MYERS LLP
2765 Sand Hill Road
Menlo Park, California 94025
Phone: (650) 473-2600
jfisher@omm.com

Counsel for Google LLC and Snap Inc.

Electronically signed by Andrew T. Dufresne
Andrew T. Dufresne, SBN 1081409
PERKINS COIE LLP
33 E. Main Street, Suite 201
Madison, Wisconsin 53703
Phone: (608) 663-7460
adufresne@perkinscoie.com

Counsel for Google LLC, Snap Inc., and Microsoft Corporation

*admitted *pro hac vice*

FORM AND LENGTH CERTIFICATION

I certify that this brief conforms to the rules contained in Wis. Stats. §§ 809.19(8)(b), (bm), and (c) for a non-party brief produced with a proportional serif font. The length of this brief is 2,992 words.

Dated: August 1, 2025

Electronically signed by Andrew T. Dufresne

Andrew T. Dufresne

CERTIFICATE OF SERVICE

I certify that on this 1st day of August 2025, I caused a copy of this brief to be served upon counsel for each of the parties via the Court's electronic filing system, which will accomplish electronic notice and service for all participants who are registered users.

Electronically signed by
Andrew T. Dufresne
Andrew T. Dufresne