FILED
07-28-2025
CLERK OF WISCONSIN
SUPREME COURT

STATE OF WISCONSIN

SUPREME COURT

Appeal No. 2023AP2319 - CR

STATE OF WISCONISN,

Plaintiff-Appellant,

v.

MICHAEL JOSEPH GASPER,

Defendant-Respondent-Petitioner.

On review of a Court of Appeals decision reversing an order granting suppression entered in the Waukesha County Circuit Court, the Honorable Shelley J. Gaylord, presiding.

NONPARTY BRIEF OF THE WISCONISN ASSOCIATION OF CRIMINAL DEFENSE LAWYERS

Megan Sanders
State Bar No. 1097296

SANDERS LAW OFFICE
411 West Main Street, Suite 204
Madison, WI 53703
megan@sanderslaw.net
(608) 447-8445

Counsel for WACDL

TABLE OF CONTENTS

ARGUMENT 4

Users retain a reasonable expectation of privacy *as to the government* in files they send, receive, or possess via their electronic accounts—even when those files violate their accounts' terms of service. 4

A. Introduction 4

B. A user does not relinquish his reasonable expectation of privacy in an electronic account by agreeing to an ESP's terms of service 7

C. A user does not relinquish his reasonable expectation of privacy in an electronic account by violating the ESP's terms of service. 9

D. *Gasper* departed from Wisconsin precedent by holding that a user can forsake his Fourth Amendment rights by entering into, and then breaching, a private contract with an ESP. 11

CONCLUSION 14

TABLE OF AUTHORITIES

Cases

Byrd v. United States,
584 U.S. 395 (2018) 7, 10

Carpenter v. United States,
585 U.S. 296 (2018) 7

Minnesota v. Olson,
495 U.S. 91 (1990) 10

State v. Baric,
2018 WI App 63, 384 Wis. 2d 359, 919 N.W.2d 221 .....9, 12

State v. Bowers,
2023 WI App 4, 405 Wis. 2d 716, 985 N.W.2d 123 .....9, 13

State v. Gasper,
2024 WI App 72, 414 Wis. 2d 532, 16 N.W.2d 279 .....9, 12

State v. Payano-Roman,
2006 WI 47, 290 Wis. 2d 380, 714 N.W.2d 548 8

State v. Rewolinski,
159 Wis. 2d 1, 464 N.W.2d 401 9

State v. Silverstein,
2017 WI App 64, 378 Wis. 2d 42, 902 N.W.2d 550. .....4, 5

Stoner v. California,
376 U.S. 483 (1964).....10

United States v. Jacobsen,
466 U.S. 109 (1984).....8

United States v. Jones,
565 U.S. 400 (2012).....7

United States v. Washington,
573 F.3d 279 (6th Cir. 2009).....10

Other Authorities

Orin S. Kerr, *Terms of Service and Fourth Amendment Rights*, 172 U. Penn. L. Rev. 287 (2024).....7, 8

The Wisconsin Association of Criminal Defense Lawyers (WACDL) submits this non-party brief regarding users' privacy expectations *as to the government* in files they send, receive, or possess via their electronic accounts in violation of the accounts' terms of service.[1] Because this critical Fourth Amendment issue will be a starting point for the Court's suppression analysis in both *State v. Rauch Sharak*, Appeal No. 2024AP469-CR, and *State v. Gasper*, Appeal No. 2023AP2319, WACDL submits this brief in both cases. WACDL takes no position, in either case, on whether suppression is warranted.

ARGUMENT

Users retain a reasonable expectation of privacy *as to the government* in files they send, receive, or possess via their electronic accounts—even when those files violate their accounts' terms of service.

A. Introduction.

Rauch Sharak and *Gasper* present variations on a recurring fact pattern that often triggers a suppression motion. An individual opens an electronic account, agreeing to terms of service that bar them from using the account for CSAM[2]; the ESP[3] detects suspected CSAM and

---

[1] This brief pertains to users' privacy expectations in digital files associated with their electronic accounts that comprise suspected CSAM and thus violate their accounts' terms of service. Given the applicable word limit, this brief refers at times to a user's expectation of privacy in their "files" or "electronic accounts" as a shorthand for the narrower digital space in question.

[2] CSAM stands for "child sexual abuse material," the umbrella term commonly used for pornographic images and videos involving minors.

[3] ESP stands for "electronic service provider." *State v. Silverstein*, 2017 WI App 64, ¶1, 378 Wis. 2d 42, 902 N.W.2d 550. An ESP is a company offering "any service which provides to users thereof the ability to send or receive ... electronic

tells NCMEC[4]; NCMEC gathers information about the individual and passes it to local law enforcement; and local law enforcement investigates, eventually getting a warrant to search the individual's electronic devices. *See State v. Silverstein*, 2017 WI App 64, 378 Wis. 2d 42, 902 N.W.2d 550. The chart on the following page summarizes the typical sequence of events.

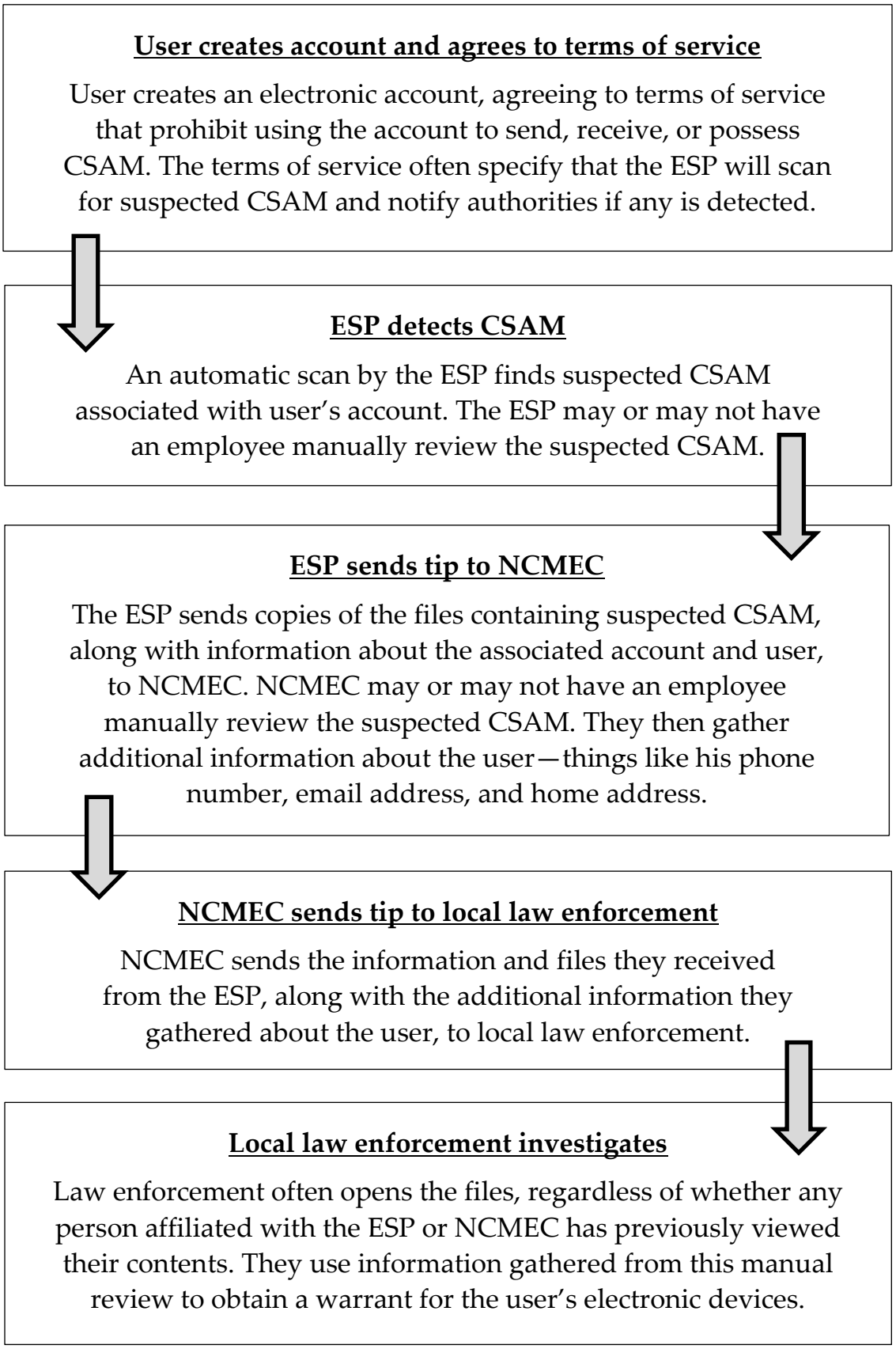
This fact pattern involves an array of actors and steps, but it culminates with police conducting a search pursuant to a warrant. The suppression question these cases present generally revolves around the validity of that warrant: did police secure it by relying on information from a prior, unlawful search—either their own or one by the ESP or NCMEC? But answering that question requires courts to move several steps backward: to the investigative steps police took before securing their warrant, to the information the ESP and NCMEC obtained before police got involved, and to the terms of service the individual agreed to when opening the relevant electronic account.

This brief addresses the first step in the chain: when an individual opens an electronic account and agrees to the ESP's terms of service. Two additional amicus briefs—one filed on behalf of Microsoft, Snap, and Google, the other on behalf of Privacy and Surveillance Accountability, Inc.—likewise focus on this early pivot point. All amici in this case, as well as both defendants and the District 4 Court of Appeals (per its certification of *Rauch Sharak*), appear to agree: the terms of service an individual agrees to when opening an electronic account do not dictate whether he has a reasonable expectation of privacy in that account vis-à-vis the government, even when the individual violates those terms of service by using his account to break the law.

---

communications," including image and video files. 18 U.S.C. § 2510(12), (15); *see also Silverstein*, 378 Wis. 2d 41, ¶5 n.4.

[4] NCMEC stands for "National Center for Missing and Exploited Children." *Id.*, ¶1. NCMEC is "directed by federal law to serve as a clearinghouse for [ESPs'] tips [about suspected CSAM] and as a liaison to law enforcement." *Id.*, ¶5.


User creates account and agrees to terms of service
User creates an electronic account, agreeing to terms of service that prohibit using the account to send, receive, or possess CSAM. The terms of service often specify that the ESP will scan for suspected CSAM and notify authorities if any is detected.
ESP detects CSAM
An automatic scan by the ESP finds suspected CSAM associated with user's account. The ESP may or may not have an employee manually review the suspected CSAM.
ESP sends tip to NCMEC
The ESP sends copies of the files containing suspected CSAM, along with information about the associated account and user, to NCMEC. NCMEC may or may not have an employee manually review the suspected CSAM. They then gather additional information about the user—things like his phone number, email address, and home address.
NCMEC sends tip to local law enforcement
NCMEC sends the information and files they received from the ESP, along with the additional information they gathered about the user, to local law enforcement.
Local law enforcement investigates
Law enforcement often opens the files, regardless of whether any person affiliated with the ESP or NCMEC has previously viewed their contents. They use information gathered from this manual review to obtain a warrant for the user's electronic devices.

B. A user does not relinquish his reasonable expectation of privacy in an electronic account by agreeing to an ESP's terms of service.

The Fourth Amendment protects individuals against unreasonable "official intrusion into [a] private sphere." *See Carpenter v. United States*, 585 U.S. 296, 304 (2018). A sphere is private under the Fourth Amendment when the individual has a reasonable expectation of privacy in it.[5] *Id.* at 304-05. Such an expectation exists when a person believes he can exclude *the governmen*t from either a space or information (e.g., his briefcase, Instagram account, or personal location), and society considers that belief reasonable. *See id.* A person may have a reasonable expectation of privacy despite knowing certain third parties have ready access to the space or information in question—his spouse to his briefcase, say, or his wireless carrier to his location data. *See id.* at 313-16. Whether or not the person can keep a private actor out says little about whether he believes the police can intrude absent a warrant or an exception to the warrant requirement.

The terms of service users accept when opening an electronic account generally clarify that the ESP (the account's true owner) will have ready access to it; users can't keep them out. But those terms comprise a private contract between the user and the ESP, setting ground rules for *their* relationship. Because the government is not a party to terms-of-service contracts, such contracts do not define users' rights *as to the government*. *See generally* Orin S. Kerr, *Terms of Service and Fourth Amendment Rights*, 172 U. Penn. L. Rev. 287, 304-05 (2024).

---

[5] *United States v. Jones*, 565 U.S. 400, 404-05 (2012), articulated a property-based, as opposed to privacy-based, Fourth Amendment theory. The contours of this theory remain murky, but since the *Jones* approach supplemented rather than replaced the privacy-based approach, this Court need not define them to determine whether the Fourth Amendment protects the files at issue here. *See Byrd v. United States*, 584 U.S. 395, 403-04 (2018); *see also* Orin S. Kerr, *Terms of Service and Fourth Amendment Rights,* 172 U. Penn. L. Rev. 287, 306 n.118 (2024).

Granted, terms of service may state that the ESP will give the government information about a user's account under certain circumstances, raising the specter of the private-search doctrine. Under this doctrine, if the ESP is deemed a private actor when it scans accounts for CSAM,[6] then the government may conduct the same search the ESP conducted so long as they intrude into the relevant private sphere no further than the ESP did. *See United States v. Jacobsen*, 466 U.S. 109, 114-22 (1984). But whether this doctrine excepts a particular search from the Fourth Amendment's warrant requirement is a separate question from whether the space or information searched is protected in the first place. The possibility that an exception to the warrant requirement will apply does not preemptively extinguish the requirement itself. That's not how the Fourth Amendment works.

So if terms of service don't dictate whether a user has a reasonable expectation of privacy in an electronic account, what does? The usual considerations:

> (1) whether the defendant had a property interest in the premises; (2) whether he was legitimately (lawfully) on the premises; (3) whether he had complete dominion and control and the right to exclude others; (4) whether he took precautions customarily taken by those seeking privacy; (5) whether he put the property to some private use; and (6) whether the claim of privacy is consistent with historical notions of privacy.

State v. Rewolinski, 159 Wis. 2d 1, 17-18, 464 N.W.2d 401.

---

[6] An ESP may function as a government entity rather than a private actor when it scans users' data for CSAM, or the search may be a joint private-government endeavor under *State v. Payano-Roman*, 2006 WI 47, 290 Wis. 2d 380, 714 N.W.2d 548. These are questions before the Court in *Rauch Sharak.* But if a user lacks a reasonable expectation of privacy in his electronic account, then the kind of entity that searches it is irrelevant; there's no Fourth Amendment violation. The first critical issue, therefore, is whether users have a reasonable expectation of privacy in such accounts.

Wisconsin courts have analyzed these factors as to "digital files" sent, received, or possessed "on electronic platforms" via password-protected accounts—just what's at issue in *Rauch Sharak* and *Gasper*—and have concluded that users have a reasonable expectation of privacy in such files vis-à-vis the government. *See, e.g.*, *State v. Bowers*, 2023 WI App 4, ¶¶18-27, 405 Wis. 2d 716, 985 N.W.2d 123 (quoting *State v. Baric*, 2018 WI App 63, ¶18, 384 Wis. 2d 359, 919 N.W.2d 221). The court of appeals' decision in *State v. Gasper*, of course, went a different way. 2024 WI App 72, ¶28, 414 Wis. 2d 532, 16 N.W.2d 279.

C. A user does not relinquish his reasonable expectation of privacy in an electronic account by violating the ESP's terms of service.

The terms of service that forbid users from sending, receiving, or possessing CSAM via their electronic accounts also specify the actions the ESP will take in the event of a breach. Those actions include transmitting information about the user's account—and any associated suspected CSAM—to the authorities. But just as entering a terms-of-service contract with an ESP doesn't dictate whether a user has a reasonable expectation of privacy in his electronic account, neither does breaching that contract diminish a user's Fourth Amendment rights. As noted above, the fact that the ESP will transmit information to the government means the private-search exception to the warrant requirement may apply; it does *not* eliminate law enforcement's need for a warrant or an exception thereto.

It's helpful, here, to keep the broader Fourth Amendment context in mind: every successful suppression motion has involved a government search of a space or information that turned up evidence of a crime. When a person deals drugs within their home, when a driver's blood contains more alcohol than the law permits, when cell-site data places a defendant at the scene of a crime—in all these scenarios, an individual's expectation of privacy in a given space or in certain information shields his illicit conduct from police unless and

until they obtain a warrant to intrude. Engaging in unlawful activity is no barrier to reasonably expecting privacy.

That remains true when unlawful activity violates a private contract, like the terms of service a user accepts when opening an electronic account. Consider the analogous realm of precedent regarding rental car agreements. In *Byrd v. United States*, 584 U.S. 395, 405-08 (2018), the United States Supreme Court held that a driver could, in theory, have a reasonable expectation of privacy in a rental car for which he wasn't an authorized driver, even though he was using the car to transport drugs.[7] The fact that his driving breached the rental car agreement did not vitiate his reasonable expectation of privacy in the car. *Id.* Or consider cases holding that an apartment occupant retains a reasonable expectation of privacy in his apartment despite a lease breach and criminal conduct within the apartment; neither deprive the occupant of the Fourth Amendment's protection. *See, e.g., United States v. Washington*, 573 F.3d 279, 284-86 (6th Cir. 2009). Finally, courts have repeatedly concluded that a hotel guest has a reasonable expectation of privacy in his room, even if he engages in unlawful activity within it, until his occupancy ends. *See, e.g., United States v. Young*, 573 F.3d 711, 715-16 (9th Cir. 2009). If the guest's commission of a crime violates hotel policy, the hotel can kick him out—but until that point, it can't let police search his room. *See Stoner v. California*, 376 U.S. 483, 486-90 (1964).

The basic point that emerges from these cases is one the District 4 Court of Appeals highlighted in its *Rauch Sharak* certification: privacy expectations are not content-specific. A person's reasonable expectation of privacy in his backpack exists whether the backpack holds heroin or school supplies. A person's reasonable expectation of privacy in his personal location exists whether cell-site data shows he traveled to and from a drug house or to and from the

[7] The *Byrd* Court remanded the matter for an initial determination of whether the driver at issue did, in fact, have such an expectation. 584 U.S. at 410.

grocery store. And a person's reasonable expectation of privacy in his hotel room exists whether he's smoking cigarettes—against hotel policy—or sleeping soundly. Indeed, there would be no exclusionary rule if unlawful conduct, let alone a contract breach, were enough to negate a reasonable expectation of privacy: every time a court grants suppression, it does so because the government unreasonably invaded a private sphere and thereby secured evidence of a crime. The problematic activity within a private sphere doesn't render the government's invasion reasonable; only a warrant—or exception to the warrant requirement—can do that.

D. *Gasper* departed from Wisconsin precedent by holding that a user can forsake his Fourth Amendment rights by entering into, and then breaching, a private contract with an ESP.

Gasper rejects the conclusion set forth here, in the defendants' briefs, in the other amicus briefs filed in these matters, and in the District 4 Court of Appeals' certification of *Rauch Sharak*: that an ESP's terms of service do not control a user's Fourth Amendment rights, even when he violates them by using his electronic account to break the law. *Gasper* takes a new approach to the privacy-expectation test in the context of files sent, received, or possessed via electronic accounts—one that's analytically confused and contrary to Wisconsin precedent. This Court should steer the boat back on course.

In *Gasper*, the court of appeals cited two key reasons why the defendant lacked a reasonable expectation of privacy in a video associated with his Snapchat account: (1) the video violated Snapchat's terms of service, which barred him from using the account for CSAM and said Snapchat would notify the authorities if they detected CSAM; and (2) the video constituted CSAM. *See* 414 Wis. 2d 532, ¶¶21, 24-25, 28. The first component of the court of appeals' rationale overlooks the critical distinction between a user's agreement to let an *ESP* access an otherwise private sphere and that user's consent to a

government search of the sphere. *See supra* Part B. As discussed at length above, sacrificing some degree of privacy as to an ESP, in exchange for access to the ESP's platform, is one thing; waiving a fundamental constitutional right held by individuals against their government is quite another. The second piece of the *Gasper* analysis creates a content-based distinction that finds no support in the Fourth Amendment case law. *See supra* Part C. Individuals legitimately expect privacy within certain spaces and with regard to certain types of information; their expectations aren't conditioned on what they do in those spaces or whether that information suggests their innocence or guilt of some nefarious conduct.

In overlooking these issues, *Gasper* diverged from Wisconsin precedent.

In *Baric*, the court of appeals addressed whether the defendant had a reasonable expectation of privacy in files he "made available on the eDonkey P2P file sharing network." 384 Wis. 2d 359, ¶¶17-18. Such networks are, by definition, *not* private; the files the defendant shared were available to anyone, including law enforcement, with an internet connection and P2P software. *Id.*, ¶¶3, 21. Thus, the privacy-expectation question in *Baric* was an easy "no." But in concluding that the defendant lacked a reasonable expectation of privacy in digital files he *publicly* shared, the court of appeals acknowledged that individuals can keep their digital files private on an electronic platform just as they can keep their personal effects private in physical space. *See id.*, ¶19. And in either case, they can reasonably expect the government to respect that privacy. *See id.*

In *Bowers*, the court of appeals again addressed an issue adjacent to the one presented here. There, the State argued that the defendant had no reasonable expectation of privacy in his Dropbox account. *Bowers*, 405 Wis. 2d 716, ¶17. The court of appeals disagreed. *Id.*, ¶3. Applying the privacy-expectation factors set forth *supra*, pp. 8-9, it held that a Dropbox account is like "a 21st century container used

to hold private papers and effects," and that the defendant used it as such. *Id.*, ¶¶20-26, 43. Thus, *even though he used the account to commit a crime*, he retained a reasonable expectation of privacy in it. *Id.*, ¶45.

Baric recognizes that a user can keep digital files private on an electronic platform. *Bowers* recognizes that using an electronic account to commit a crime does not negate a user's legitimate expectation of privacy in the account. Together, then, the cases stand for the proposition that a user can have a reasonable expectation of privacy in an electronic account that they utilize to commit crimes. While neither case addresses the terms-of-service wrinkle at issue, they *do* make clear that Fourth Amendment rights aren't content-specific, even in the digital realm. Carving out an exception to the Fourth Amendment's protections for files that violate an ESP's terms of service is a content-based distinction, plain and simple. By adopting it, *Gasper* departed from binding precedent. This Court should clarify the appropriate analysis by holding that violating an ESP's terms of service does not negate a user's reasonable expectation of privacy, vis-à-vis the government, in files he sends, receives, or possesses via his electronic account.

CONCLUSION

WACDL respectfully asks this Court hold to that users retain a reasonable expectation of privacy *as to the government* in files they send, receive, or possess via their electronic accounts—regardless of whether those files violate their accounts' terms of service.

Dated this 28th day of July, 2025.

Respectfully submitted,

Electronically signed by Megan Sanders

Megan Sanders
State Bar No. 1097296

SANDERS LAW OFFICE
411 West Main Street, Suite 204
Madison, WI 53703
megan@sanderslaw.net
(608) 447-8445

Counsel for WACDL

CERTIFICATION AS TO FORM AND LENGTH

I hereby certify that this brief conforms to the rules contained in s. 809.19(8)(b), (bm), and (c) for a brief. The length of this brief is 2,991 words.

Dated this 28th day of July, 2025.

Signed:

Electronically signed by Megan Sanders

Megan Sanders
State Bar No. 1097296