

No. 25-1191

In the Supreme Court of the United States

MICHAEL JOSEPH GASPER, *Petitioner*,

v.

STATE OF WISCONSIN

On Petition for Writ of Certiorari
to the Supreme Court of Wisconsin

**BRIEF OF *AMICUS CURIAE*
PROJECT FOR PRIVACY & SURVEILLANCE
ACCOUNTABILITY, INC.
SUPPORTING PETITIONER**

GENE C. SCHAERR

Counsel of Record

ERIK S. JAFFE

JUSTIN A. MILLER

SCHAERR | JAFFE LLP

1717 K Street NW, Suite 900

Washington, DC 20006

Telephone: (202) 787-1060

gschaerr@schaerr-jaffe.com

Counsel for Amicus Curiae

JUNE 8, 2026

TABLE OF CONTENTS

TABLE OF AUTHORITIES.....	ii
INTRODUCTION, SUMMARY, AND INTEREST OF <i>AMICUS CURIAE</i>	1
STATEMENT	3
ADDITIONAL REASONS FOR GRANTING THE PETITION	4
I. This Court Should Grant Review to Correct Widespread Misinterpretations of the Post- <i>Carpenter</i> Third-Party Doctrine.....	5
A. Third-party disclosure is merely one factor in the <i>Carpenter</i> reasonableness inquiry.	6
B. Snapchat’s Warning That It Will Comply with Federal Law Does Not Extinguish Reasonable Expectations of Privacy Over User Data.	8
II. This Court Should Grant Review to Clarify That the Search Here Was Not Private.....	10
A. The government cannot end-run the Fourth Amendment by expanding on or coercing private searches.....	11
B. Lower courts are split on whether warrantless visual examination of computer-matched images violates the Fourth Amendment.....	13
CONCLUSION	16

TABLE OF AUTHORITIES

Cases	Page(s)
<i>Blum v. Yaretsky</i> , 457 U.S. 991 (1982).....	12
<i>Carpenter v. United States</i> , 585 U.S. 296 (2018).....	1, 3, 5-9
<i>Doe #1 v. MG Freesites, LTD</i> , 676 F. Supp. 3d 1136 (N.D. Ala. 2022).....	12
<i>Ex parte Jackson</i> , 96 U.S. 727 (1877).....	7
<i>Ferguson v. City of Charleston</i> , 532 U.S. 67 (2001).....	12
<i>Heidi Grp., Inc. v. Texas Health & Hum. Servs. Comm’n</i> , 138 F.4th 920 (5th Cir. 2025).....	8, 11
<i>Katz v. United States</i> , 389 U.S. 347 (1967).....	6
<i>Koontz v. St. Johns River Water Mgmt. Dist.</i> , 570 U.S. 595 (2013).....	9
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001).....	1, 5
<i>New York State Rifle & Pistol Ass’n, Inc. v. Bruen</i> , 597 U.S. 1 (2022).....	6
<i>Ohio v. Robinette</i> , 519 U.S. 33 (1996).....	6
<i>Packingham v. North Carolina</i> , 582 U.S. 98 (2017).....	10

<i>Skinner v. Railway Lab. Execs.’ Ass’n</i> , 489 U.S. 602 (1989).....	12
<i>Smith v. Maryland</i> , 442 U.S. 735 (1979).....	7
<i>Stanford v. Texas</i> , 379 U.S. 476 (1965).....	10
<i>Students for Fair Admissions, Inc. v.</i> <i>President & Fellows of Harvard Coll.</i> , 600 U.S. 181 (2023).....	9
<i>United States v. Ackerman</i> , 831 F.3d 1292 (10th Cir. 2016).....	14
<i>United States v. Arce</i> , 49 F.4th 382 (4th Cir. 2022)	15
<i>United States v. Bebris</i> , 4 F.4th 551 (7th Cir. 2021)	11
<i>United States v. Jacobsen</i> , 466 U.S. 109 (1984).....	11
<i>United States v. Lowers</i> , 170 F.4th 134 (4th Cir. 2026)	13-15
<i>United States v. Maher</i> , 120 F.4th 297 (2d Cir. 2024).....	14
<i>United States v. Miller</i> , 425 U.S. 435 (1976).....	7, 11
<i>United States v. Miller</i> , 982 F.3d 412 (6th Cir. 2020).....	15, 16
<i>United States v. Reddick</i> , 900 F.3d 636 (5th Cir. 2018).....	15

<i>United States v. Warshak</i> , 631 F.3d 266 (6th Cir. 2010).....	8
<i>United States v. Wilson</i> , 13 F.4th 961 (9th Cir. 2021)	13-15
<i>United States v. Zelaya-Veliz</i> , 94 F.4th 321 (4th Cir. 2024)	8
<i>Willner v. Thornburgh</i> , 928 F.2d 1185 (D.C. Cir. 1991).....	9
Constitutional Provision	
U.S. Const. amend. IV	6
Statutes	
18 U.S.C. §1595	12
18 U.S.C. §2258A.....	9, 12

INTRODUCTION, SUMMARY, AND INTEREST OF *AMICUS CURIAE*¹

This case presents a pair of exceptionally important Fourth Amendment questions: Does a person retain a reasonable expectation of privacy in his data when he uploads it to third-party data storage? And does a government search occur when a government agent visually examines data that the private host had not viewed and where the host's reporting is coerced by government mandate? The governing principles of this Court's Fourth Amendment caselaw strongly suggest that the unwarranted expansions of the third-party doctrine at issue here violate the Constitution: They are incompatible, as this Court put it in *Carpenter v. United States*, 585 U.S. 296 (2018), with "that degree of privacy against government that existed when the Fourth Amendment was adopted." *Id.* at 305 (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)). But federal and state courts continue to treat *Carpenter* as the exception rather than the rule. This Court should grant certiorari to clarify that it meant what it said there.

Carpenter recognized that the Fourth Amendment protects privacy interests that would have been recognized as reasonable at the Founding. Such expectations set the baseline for measuring

¹ This brief was not authored in whole or in part by counsel for any party and no person or entity other than *amicus curiae*, its members, or its counsel has made a monetary contribution toward the brief's preparation or submission. Counsel of record for all parties received timely notice of *amicus*' intent to file this brief.

modern encroachments on privacy, notwithstanding advances in technology that make it easier to invade that privacy. Under such baseline expectations, merely storing information with third parties, under contractual assurances of privacy and security, does not invalidate reasonable expectations of privacy, particularly as against the government.

The Wisconsin courts ignored these basic principles and this Court's guidance. They mistakenly treated the fact that a third party was storing the data and that, as compelled by the government, its terms of service noted its obligation to report certain data to the government, as sufficient to destroy Petitioner's expectation of privacy in his personal data. But, as the petition explains, that is fundamentally wrong. If the government, by fiat, can simply eliminate any reasonable expectations of privacy, the Fourth Amendment would be meaningless.

Because of the serious privacy issues raised by how third-party hosted data is treated, they are of particular concern to *Amicus Curiae* Project for Privacy & Surveillance Accountability, Inc. ("PPSA"), a nonprofit, nonpartisan organization dedicated to protecting privacy rights. PPSA urges this Court to reverse the Supreme Court of Wisconsin's decision and hold that Americans have a reasonable expectation of privacy in their data, even if it is stored by a third party, as an increasing amount of data is these days, or subject to *ipse dixit* government demands for access. The Court can thereby help ensure that Fourth Amendment rights are not left "at the mercy of advancing technology" or the whims of government

abolitions of privacy. *Carpenter*, 585 U.S. at 305 (citation omitted).

STATEMENT

Petitioner Michael Gasper had an account on Snapchat, App.2a ¶2 n.2, a privacy-focused social media app with a distinguishing feature of automatically disappearing messages. To use Snapchat, a user must check a box agreeing to its Terms of Service (“Terms”). App.45a. Had Gasper clicked an extra button during signup to open the Terms and read the 16-page agreement 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”). App.94a ¶6, 99a-101a ¶¶16-19.

After Gasper signed up, 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, App.2a ¶2 & n.3. Neither Snapchat nor NCMEC actually viewed the file. App.2a ¶2. The first human to review the flagged file was a member of law enforcement—without obtaining a warrant. App.2a-3a ¶2. Based on this review, Gasper was arrested and charged with counts related to possession of CSAM. App.2a ¶2.

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. App.3a. The trial court granted the motion, App.3a ¶3, but the Wisconsin 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. App.3a-4a ¶4; App.105a ¶¶28-29. The Wisconsin Supreme Court granted review and vacated the court of appeals’ rationale and the precedential effect of its decision, but the court affirmed the reversal of the suppression order on other grounds, relying on the “private search” exception to the Fourth Amendment’s warrant requirement. App.5a ¶6.

ADDITIONAL REASONS FOR GRANTING THE PETITION

This case presents an enormously important Fourth Amendment question that has divided federal and state courts, generating splits between the Second, Fourth, and Ninth Circuits on the one hand and the Supreme Court of Wisconsin and the Fifth and Sixth Circuits on the other. In contrast to the Supreme Court of Wisconsin’s decision here, the Second, Fourth, and Ninth Circuits correctly held that the government’s warrantless human review of a private automated search remains subject to the Fourth Amendment. These splits should be resolved now.

Moreover, the Wisconsin Supreme Court’s erroneous application of the Fourth Amendment third-party doctrine is but one of many examples of federal and state courts abandoning all semblance of Founding Era privacy and concluding that Americans have no Fourth Amendment protections against a host of intrusive surveillance practices. That conclusion and similar holdings will continue to drastically

undermine Americans' privacy as third-party storage becomes increasingly common and inescapable.

Amicus writes separately to emphasize that, as *Carpenter* clarified, Fourth Amendment protections are not categorically lost when a person shares or stores his data with a third party while maintaining reasonable expectations of privacy. The Court should grant review to prevent a contrary misunderstanding of *Carpenter* from continuing to erode Americans' privacy—especially now, as third-party storage becomes more ubiquitous.

I. This Court Should Grant Review to Correct Widespread Misinterpretations of the Post-*Carpenter* Third-Party Doctrine.

The decision below, as well as those of the Fifth and Sixth Circuits, contravene this Court's repeated holdings that the Fourth Amendment protects "that degree of privacy against government that existed when [it] was adopted." *Carpenter v. United States*, 585 U.S. 296, 305 (2018) (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)). This is true in the context of the third-party doctrine as well, especially regarding the overarching question here—whether users of online storage applications, including Snapchat, have a reasonable expectation of privacy in their account information and files.

Entrusting confidential communications to a third party is a practice that was firmly rooted at the time of the Founding and predates the establishment of the first postal offices. Under a proper understanding of *Carpenter*, those who use third-party data storage do not relinquish any reasonable

expectation of privacy in the contents of those communications.

A. Third-party disclosure is merely one factor in the *Carpenter* reasonableness inquiry.

The Fourth Amendment prohibits “unreasonable searches and seizures.” U.S. Const. amend. IV. It protects people’s actual expectation of privacy so long as that expectation is one that society is prepared to recognize as “reasonable.” *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The scope of the Fourth Amendment’s reach is thus “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,” *New York State Rifle & Pistol Ass’n, Inc. v. Bruen*, 597 U.S. 1, 28 (2022). In this manner, 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 313-314.

In addressing the historically grounded inquiry into reasonable expectations of privacy, *Carpenter* clarified that disclosure to a third party does not automatically invalidate such expectations or the resulting Fourth Amendment protections. 585 U.S. at 314. Although this Court there recognized that disclosing data to a third party can sometimes diminish an expectation of privacy for that data—as any third-party disclosure could—that recognition was

tempered by this Court’s rejection of 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)).

At the Founding, entrusting property to third parties for a limited use, or “bailment,” was common. 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. 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. Even more so here with Snapchat, which uses automatically disappearing messages, thus showing and fostering a clear 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. Texas Health & Hum. Servs. Comm’n*, 138 F.4th

920, 935 (5th Cir. 2025); see *United States v. Zelaya-Veliz*, 94 F.4th 321, 333-334 (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).

This Court should grant certiorari to ensure that the privacy 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).

**B. Snapchat’s Warning That It Will
Comply with Federal Law Does Not
Extinguish Reasonable Expectations of
Privacy Over User Data.**

The warning in Snapchat’s Terms that it scans for CSAM and is required to report what it finds to NCMEC does not extinguish Gasper’s privacy expectations for two reasons. First, the government cannot negate otherwise reasonable privacy expectations by mandating or coercing private actors to notify their users that they will conduct searches on the government’s behalf. Such *ipse dixit* commands would render the Fourth Amendment meaningless. Second, the government cannot, through a third party, condition using digital services essential to modern life on renunciation of Fourth Amendment rights.

1. As to the first point, the government cannot use private disclosure of a government mandate as an end-run around the Fourth Amendment. If Snapchat’s warning of its intent to comply with federal legal obligations eliminated that expectation of privacy, this

would create easy circumvention of the Fourth Amendment. If the State were correct, although the government itself cannot announce it will search an area to eliminate privacy expectations, see *Willner v. Thornburgh*, 928 F.2d 1185, 1189-1190 (D.C. Cir. 1991), 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 is not—and cannot be—the law. The general rule is 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).

2. As to the second point, the government cannot require renunciation of Fourth Amendment rights to participate in essential aspects of modern life. If the State were correct, one could be forced to surrender Fourth Amendment rights in digital data to use any provider subject to 18 U.S.C. §2258A, which penalizes the failure of a provider to report potential CSAM materials. 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, this 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)).

Electronic Service Providers such as Snapchat are both indispensable to modern life and contain vast amounts of intimate information, and 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” essential to First Amendment rights); *Stanford v. Texas*, 379 U.S. 476, 484-485 (1965) (noting First Amendment concerns result in heightened Fourth Amendment concerns). The pervasiveness of third-party hosting of data and the failure to faithfully apply *Carpenter* regarding that data counsel in favor of granting certiorari here.

II. This Court Should Grant Review to Clarify That the Search Here Was Not Private.

Artificial intelligence has made automated searches easier and more pervasive than ever, far beyond the capabilities and budget of any law enforcement agency reliant solely on human agents. Here, the government has effectively mandated automated searches by third-party agents and then meaningfully expanded on the scope of Snapchat and NCMEC’s coerced search by performing the first human review. Indeed, even if the original automated scan was ostensibly private, the government’s own subsequent human review conducted without a warrant was state action. But given the government compulsion to search, even Snapchat’s initial

automated search here was not truly private, but involved Snapchat acting as a government agent.

A. The government cannot end-run the Fourth Amendment by expanding on or coercing private searches.

This Court should grant certiorari to reaffirm that the government remains constrained by the Fourth Amendment when it comes to pervasive, modern data storage practices. Thus, when the government meaningfully expands on a private search of stored data, it must do so in compliance with the Fourth Amendment. And the government cannot coerce searches through onerous government mandates for third parties to conduct searches that the government could not perform itself.

1. When a search is 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). It is undisputed here that law enforcement performed the first human inspection of the files flagged by Snapchat. 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). Here, the government’s human review “exceed[ed] the scope of the” initial scan by the electronic service provider, transforming it into state action. See, e.g., *United States v. Jacobsen*, 466 U.S. 109, 116 (1984).

2. Furthermore, the initial automated search here was not truly private, but rather state action subject to the Fourth Amendment. The Fourth Amendment prohibits unreasonable searches by the government *and* by private parties acting as government agents. *Skinner v. Railway 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. *Blum v. Yaretsky*, 457 U.S. 991, 1004 (1982) (collecting cases).

Coercion to implement automated scans is evident here where 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 such scans. And other laws, state and federal, also *de facto* mandate scanning that would detect CSAM, given the risk of failing to do so where the law remains unsettled. See, e.g., *Doe #1 v. MG Freesites, LTD*, 676 F. Supp. 3d 1136, 1154-1159 (N.D. Ala. 2022) (collecting cases noting it is unsettled if 18 U.S.C. §1595 imposes liability for hosting illegal content if the electronic service provider “should have known” of it.).

Because both the scanning and reporting are compelled by government threat, *Skinner*, 489 U.S. at 614, 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.

Both of these abuses of the third-party doctrine, expanding upon or coercing a purportedly private search, are increasingly problematic in the digital era. This Court should grant certiorari to correct those abuses. But even if the Court declines to revisit the broader contours of the third-party doctrine, certiorari is still warranted because the government search here cannot be justified under the private-search doctrine.

B. Lower courts are split on whether warrantless visual examination of computer-matched images violates the Fourth Amendment.

The confusion over the scope of the third-party doctrine has produced an acknowledged conflict among lower courts regarding warrantless review of computer-matched images. That conflict between the Supreme Court of Wisconsin and the Fifth and Sixth Circuits on one hand and the Second, Fourth, and Ninth Circuits on the other hand also warrants review. See *United States v. Lowers*, 170 F.4th 134, 151 (4th Cir. 2026) (acknowledging circuit split).

The Second and Ninth Circuits hold that a warrantless visual examination is itself a Fourth Amendment search. In *United States v. Wilson*, the Ninth Circuit concluded that although Google's automated systems identified files as matching known CSAM, officers exceeded the scope of the private search when they opened and viewed the images themselves. 13 F.4th 961, 973-974 (9th Cir. 2021). The Ninth Circuit emphasized that hash matching reveals only that a file corresponds to another file; it does not

expose the image's actual contents as does the government's search.

Likewise, in *United States v. Maher*, the Second Circuit held that “the private search doctrine does not authorize a warrantless visual examination of [a] computer-matched image” because the government’s viewing reveals information that no human private actor previously observed. 120 F.4th 297, 314-320 (2d Cir. 2024). Although hash-match reliability may establish probable cause for a warrant, it cannot eliminate the warrant requirement itself. *Id.* at 319-320; see also *Wilson*, 13 F.4th at 973-974.

Thus, the Tenth Circuit correctly noted its “confiden[ce] 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.” *United States v. Ackerman*, 831 F.3d 1292, 1309 (10th Cir. 2016). Based on that understanding, the Tenth Circuit, like the Second and Ninth Circuits, questioned the treatment of automated detection as equivalent to a human private search. *Id.* at 1306-1308.

Most recently among the circuits, the Fourth Circuit recognized that the hash-matching process “carries with it a certain amount of error—both human and computer.” *Lowers*, 170 F.4th at 156. The Fourth Circuit further reasoned that the baseline comparator image used to identify subsequent CSAM may have been misidentified as such: “[E]ven if the hashing algorithm is 100% accurate, there remains the possibility that the human reviewer (who viewed the image previously) misjudged it and erroneously

labeled non-CSAM images (protected by the Fourth Amendment) as CSAM (contraband).” *Ibid.* Because “the determination of whether ‘a given image is [CSAM]’ depends on human judgment * * * the labeling as such for future hashing purposes does as well.” *Ibid.* (quoting *United States v. Arce*, 49 F.4th 382, 393 (4th Cir. 2022)). In other words, the government cannot evade the Fourth Amendment by farming out its searches to artificial intelligence. Any intelligence remains rooted in the judgments of the human intelligence that created it.

The Fifth and Sixth Circuits have reached the opposite conclusion. In *United States v. Reddick*, the Fifth Circuit held that a hash-value match gave investigators “virtual[] certain[ty]” that opening the file would reveal nothing beyond what the private provider had already discovered, bringing the government’s conduct within the private-search doctrine. 900 F.3d 636, 638-640 (5th Cir. 2018). The Sixth Circuit reached the same conclusion, holding that Google’s hash-value search sufficiently frustrated any expectation of privacy to permit officers to view the matched files without a warrant. *United States v. Miller*, 982 F.3d 412, 427-430 (6th Cir. 2020). But even the Sixth Circuit recognized that visual inspection could reveal information beyond the hash match itself: If “the files portrayed something other than [CSAM],” the government agent “would have learned what they showed—whether an embarrassing picture of the sender or an innocuous family photo.” *Id.* at 429. The Sixth Circuit nonetheless upheld the search under the private-search doctrine because it determined that Google’s hash-value matching was sufficiently

reliable, failing to recognize the underlying human element in any AI judgment, as the Fourth Circuit correctly pointed out. See *id.* at 429-430. In this case, the Wisconsin Supreme Court expressly recognized this conflict and erroneously aligned itself with the Fifth and Sixth Circuits.

This split is square, acknowledged, and outcome-determinative. Under the Second, Fourth, and Ninth Circuits' rule, officers must obtain a warrant before visually examining a computer-matched image. Under the Fifth and Sixth Circuits' and Wisconsin Supreme Court's rule, no warrant is required. This acknowledged conflict over an important and recurring question of digital-search law provides yet another compelling reason for this Court's review.

CONCLUSION

The petition should be granted to decide whether Americans retain meaningful privacy rights when using cloud storage. 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 not merely for CSAM, but for anything the government cares to know. Because the holding below removes the Fourth Amendment from the digital realm, certiorari should be granted and that holding should be reversed.

Respectfully submitted,

GENE C. SCHAERR

Counsel of Record

ERIK S. JAFFE

JUSTIN A. MILLER

SCHAERR | JAFFE LLP

1717 K Street NW, Suite 900

Washington, DC 20006

Telephone: (202) 787-1060

gschaerr@schaerr-jaffe.com

Counsel for Amicus Curiae

June 8, 2026