No. 23-893

IN THE

Supreme Court of the United States

JONATHAN WALKER,

Petitioner,

v.

STATE OF ARKANSAS,

Respondent.

On Petition for a Writ of Certiorari
To the Arkansas Court of Appeals

BRIEF IN OPPOSITION OF STATE OF ARKANSAS

TIM GRIFFIN
Arkansas Attorney General
NICHOLAS J. BRONNI
Solicitor General
Counsel of Record
DYLAN L. JACOBS
Deputy Solicitor General
ASHER STEINBERG
Senior Assistant
Solicitor General
JOSEPH KARL LUEBKE
Assistant Attorney General

OFFICE OF THE ARKANSAS
ATTORNEY GENERAL
323 Center Street
Suite 200
Little Rock, AR 72201
(501) 682-6302
nicholas.bronni@
arkansasag.gov

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D.C. 20002

QUESTION PRESENTED

Petitioner uploaded an image file to his Microsoft cloud storage account. Microsoft voluntarily scanned that image and found it was the same image as one its content moderators had previously viewed and classified as child pornography. Without reviewing the image a third time, Microsoft sent it to the National Center for Missing and Exploited Children, which in turn sent it to the police. The question presented is:

Whether police were required to obtain a warrant before they could view the twice privately searched image.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

State v. Lizotte,
197 A.3d 362 (Vt. 2018) 10

United States v. Ackerman,
831 F.3d 1292 (10th Cir. 2016)................. 16, 17

United States v. Artis,
919 F.3d 1123 (9th Cir. 2019)................... 19

United States v. Blouin,
No. CR16-307, 2017 WL 3485736
(W.D. Wash. Aug. 15, 2017)...................... 22

United States v. Bohannon,
506 F. Supp. 3d 907 (N.D. Cal. 2020)....... 1, 16

United States v. Bohannon,
No. 21-12070, 2023 WL 5607541
(9th Cir. Aug. 30, 2023) 13

United States v. Clark,
No. 22-CR-40031, 2023 WL 3543380
(D. Kan. May 18, 2023)............................. 11

United States v. Coyne,
387 F. Supp. 3d 387 (D. Vt. 2018) 19

United States v. Jacobsen,
466 U.S. 109 (1984)........................ 4, 6-9, 12, 15

United States v. Jones,
565 U.S. 400 (2012)........................... 6, 7, 14, 15

United States v. Leon,
468 U.S. 897 (1984).................................. 18

United States v. Lowers,
No. 22-CR-00178, 2024 WL 418626
(E.D.N.C. Feb. 5, 2024)............................. 11, 19

TABLE OF AUTHORITIES—Continued

CONSTITUTION	Page(s)
U.S. Const. amend. IV	6-9, 14, 15, 18-22
STATUTES	
17 U.S.C. 506	23
18 U.S.C. 2258A(a)	1
18 U.S.C. 2258A(f)	1
OTHER AUTHORITIES	
Restatement (First) of Torts (Am. L. Inst. 1934)	16
Ryan D. Balise & Gretchen Lundgren, *The Fourth Amendment's Governmental Action Requirement: The Weapon of Choice in the War Against Child Exploitation*, 41 New Eng. J. on Crim. & Civ. Confinement 303 (2015)	2
"Protecting Our Children Online": Hearing Before the S. Comm. on the Judiciary, 118th Cong. (2023)	21
Hany Farid, *An Overview of Perceptual Hashing*, J. of Online Trust & Safety, Oct. 2021, at 1	1, 2
Ronald J. Hedges et al., *Managing Discovery of Electronic Information* (3d ed. Federal Judicial Center 2017)	2
Kashmir Hill, *A Dad Took Photos of His Naked Toddler. Google Flagged Him as a Criminal*, N.Y. Times (June 21, 2023)	20

Page(s)

CyberTipline 2022 Report, NCMEC, https://perma.cc/XQ5H-B4HGx16........................ 20

Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38 (2005) 1

Marc Stevens et al., *Announcing the first SHA1 collision*, Google Security Blog (Feb. 23, 2017), https://perma.cc/8ARG-T3BQ 2

STATEMENT

Following a jury trial, petitioner Jonathan Walker was convicted on 30 counts of distributing, possessing, or viewing matter depicting sexually explicit conduct involving a child. Pet. App. 5a. The jury sentenced him to 450 years in prison. *Id.* The Arkansas Court of Appeals affirmed. Pet. App. 29a.

1. Since 2009, Microsoft has used "hashing" technology to alert it to the distribution or storage of known images of child pornography on its services. Hany Farid, *An Overview of Perceptual Hashing*, J. of Online Trust & Safety, Oct. 2021, at 1, 12. That technology automatically compares files that Microsoft's users upload or share to "a known catalogue of images that had been previously determined to be sex-abuse material" by a person who viewed the image. Pet. App. 10a. Microsoft scans its services for known child pornography to remove child pornography from its services and prevent it from circulating there. *See United States v. Bohannon*, 506 F. Supp. 3d 907, 911 (N.D. Cal. 2020). Microsoft has no legal duty to monitor user content, *see* 18 U.S.C. 2258A(f), but it is required to report child pornography it becomes aware of on its services to the National Center for Missing and Exploited Children (NCMEC), a nonprofit entity that runs "the nation's centralized reporting system for the online exploitation of children." Pet. App. 3a n.4; *see* 18 U.S.C. 2258A(a).

Hash-matching works by "us[ing] a complex mathematical algorithm to generate" an identifier, the so-called "hash value," that is "unique" to a particular image. Pet. App. 3a n.3 (quoting Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38, 38 (2005)). Because each image's hash value is unique, a false match is virtually impossible. "The most commonly used algorithms" are so accurate that the chance of a false match "is less than one in one billion." Ronald J. Hedges et al., *Managing Discovery of Electronic Information* 52 (3d ed. Federal Judicial Center 2017); *see also* Marc Stevens et al., *Announcing the first SHA1 collision*, Google Security Blog (Feb. 23, 2017), https://perma.cc/8ARG-T3BQ (discussing an experiment on whether a common hash-match algorithm could be deceived into making a false match that only succeeded after nine quintillion failed attempts).

Microsoft's hash-matching algorithm is no different. Unlike "hard-hashing" algorithms, which compare image files' underlying data without viewing the image itself, Farid, *supra*, at 3-4, Microsoft's algorithm, known as PhotoDNA, works by comparing the brightness and color of the pixels in an image to that of the photos in a database, *see id.* at 5-10, 12. According to Microsoft, it returns a false match "about once in every two billion images." Ryan D. Balise & Gretchen Lundgren, *The Fourth Amendment's Governmental Action Requirement: The Weapon of Choice in the War Against Child Exploitation*, 41 New Eng. J. on Crim. & Civ. Confinement 303, 309 (2015). Because of PhotoDNA's reliability it has been adopted by Facebook, Google and X. Farid, *supra*, at 12.

2. Walker is a recidivist child pornography offender. In 2009, he was convicted in Oregon on three first-degree child-pornography possession offenses after he was caught with 120 child-pornographic images on a flash drive. Pet. App. 18a, 20a.

On April 28, 2020, Walker uploaded an image file from his computer to his Microsoft OneDrive cloud storage account. Pet. App. 2a. Microsoft's PhotoDNA scanned that image and found it was an identical match to a child-pornographic image previously "reviewed by Microsoft content moderators." Pet. App. 93a. Microsoft sent a report with that information, the image itself, and Walker's IP address to NCMEC. Pet. App. 3a. NCMEC, which didn't open the image, Pet. App. 98a, forwarded the report to Arkansas State Police two weeks later, Pet. App. 99a.

When Arkansas State Police received the report, a special agent who specializes in investigating Internet crimes against children reviewed the report, viewed the image it contained, and confirmed it constituted child pornography. Pet. App. 3a. Arkansas State Police's investigation revealed that the IP address in the report was Walker's. Pet. App. 3a-4a. Based on these facts, police applied for and obtained a warrant to search Walker's apartment and computers. Pet. App. 4a.

Upon searching Walker's apartment, police seized several laptop computers. Pet. App. 4a. One contained a custom hard drive with seven discrete partitions. *Id.* In the seventh, police found hundreds of images and videos of child pornography. *Id.* Walker was charged with 30 counts of possessing child pornography. Pet. App. 1a.

At trial, Walker moved to suppress the evidence found in the search. Pet. App. 8a. He theorized that although Microsoft's hash-matching software viewed his file—and Microsoft content moderators had previously reviewed the image it contained—no person at Microsoft ever opened his copy of that image. *Id.* Therefore, he reasoned, police exceeded Microsoft's search by viewing Walker's copy. *Id.*

At the suppression hearing, the State Police agents who handled Walker's investigation and obtained the search warrant testified that hash-matching's accuracy was akin to DNA testing's, and that it assigned photos unique hash values that couldn't be shared by other photos. Pet. App. 10a. Thus, the State argued, the image in Walker's file "actually had been viewed" by a Microsoft employee before police saw it. Pet. App. 76a. Walker didn't introduce any contrary evidence, Pet. App. 32a-77a, or otherwise challenge the accuracy of Microsoft's algorithm, Pet. App. 2a n.2.

The trial court denied Walker's suppression motion. Pet. App. 30a. Walker was convicted on all 30 counts of possession of child pornography that he was charged with, and he was sentenced as a habitual offender to 30 consecutive 15-year terms. Pet. App. 1a.

3. Walker appealed his convictions, raising a panoply of issues, including the denial of his suppression motion. Pet. App. 2a. A unanimous panel of the Arkansas Court of Appeals affirmed. Pet. App. 29a.

The court of appeals explained that the private-search doctrine permits the government to search items previously searched by a private party, to the same extent as the private party searched them. Pet. App. 12a. In so doing, the court of appeals noted, this Court has held that the government can "confirm[] information" it received from the private party and avoid "the risk of misdescription by the private party." *Id.* (citing *United States v. Jacobsen*, 466 U.S. 109 (1984)).

Applying that rule here, the court of appeals concluded that by viewing Walker's image, police "merely confirmed what had already been learned in the private search." Pet. App. 13a. Following the Fifth and Sixth Circuits—which had both upheld searches on materially identical facts—the court of appeals explained that Microsoft's hashing search allowed it to identify Walker's image "with almost absolute certainty." Pet. App. 16a. And that identification, in turn, meant that Walker's image was "known child pornography" that private parties had previously reviewed. Pet. App. 18a. Thus, when police viewed the image for themselves, they "learned no more than had already been learned from . . . the private search." *Id.*

Walker then petitioned for review by the Arkansas Supreme Court. That court denied his petition; no justice dissented. Pet. App. 31a.

REASONS FOR DENYING THE PETITION

I. The shallow conflict on the question presented does not merit review.

Walker asserts this Court should grant certiorari to resolve a conflict between the decision below and the many decisions consistent with it, and a decision of one court: the Ninth Circuit in *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021). This Court has seen that conflict before and declined to review it. In *Wilson v. California*, 142 S. Ct. 751 (2022) (No. 20-1737), the same defendant who prevailed in *Wilson* challenged his *state* conviction, which was based on evidence obtained from the same search the Ninth Circuit held unlawful. In response, California predicted the Ninth Circuit's outlier decision wouldn't persuade other courts, Br. in Opp. 23, and this Court denied review.

Three years later, California's prediction has held true, making review even less warranted today than it was then—and for good reason. The Ninth Circuit held that viewing a hash-matched image flagged as child pornography exceeds a provider's private search because by viewing the image, police learn whether it's "in fact child pornography." *Wilson*, 13 F.4th at 973. That rationale would condemn every application of the private-search doctrine. Whenever police search something a private party previously searched, they avoid "the risk of misdescription" and learn whether it's truly the contraband the private party said it was—and the private-search doctrine permits them to do so. *United States v. Jacobsen*, 466 U.S. 109, 119 (1984).

Accordingly, every appellate court but the Ninth Circuit to address the question has held that police may view hash-matched images because those images have already been privately searched twice before: once when a hashing algorithm scanned them and determined they were a match to a known child-pornographic image, and once when content moderators originally viewed that image and classified it as child pornography. The Ninth Circuit's lone divergent view, to which the United States has acquiesced in that circuit, does not warrant review.

A. The most important statement of the private-search doctrine is this Court's opinion in *Jacobsen*. But the doctrine dates back over a century, to a time when this Court's "Fourth Amendment jurisprudence was tied to common-law trespass." *United States v. Jones*, 565 U.S. 400, 405 (2012). In *Burdeau v. McDowell*, 256 U.S. 465 (1921), a suspect's safes were "blown open" by private detectives, who turned over the private papers they contained to the government. *Id.* at 473-74. This Court granted that the suspect had "an unquestionable right of redress against those who illegally and wrongfully took his private property"—i.e., a trespass claim. *Id.* at 475. Yet it held that the government's retention and examination of the papers was not an "unreasonable search or seizure, as whatever wrong was done was the act of individuals in taking the property of another." *Id.* A government search of privately trespassed property was not a second trespass.

Half a century later, this Court departed from its former "exclusively property-based approach" to Fourth Amendment law, *Jones*, 565 U.S. at 405, holding that the government violates the Fourth Amendment when it "violate[s] a person's 'reasonable expectation of privacy,'" even when there is no trespass. *Id.* at 406 (quoting *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)). The question then arose whether the private-search doctrine survived this shift. This Court held that it did, ultimately concluding that because private searches defeat any expectation of privacy in the items searched, the government may search to the same extent the private party did.

The Court first announced that rule in *Walter v. United States*, 447 U.S. 649 (1980), a case where private parties received and opened a misdirected shipment of obscene films before turning them over to police. *Id.* at 651-52. In the Court's lead opinion, which the Court subsequently adopted in *Jacobsen*, Justice Stevens wrote that "there was nothing wrongful about the Government's . . . examination of [the packages'] contents to the extent that they had already been examined by third parties." *Id.* at 656. He explained that their search "frustrated th[e] expectation" of privacy in the packages "in part." *Id.* at 659. But because the third parties did not examine or screen the films, an "unfrustrated portion of that expectation" in the films themselves "remain[ed]." *Id.*

So absent a warrant, the government could not screen the films. *Id.*

In *Jacobsen*, the Court adopted Justice Stevens's rule and held that once a private search has occurred, a subsequent government search is allowed so long as it does not "exceed[] the scope of the private search." 466 U.S. at 115. In that case, Federal Express employees opened a damaged box in transit and found a suspicious tube; opening the tube, they found a series of nested zip-lock bags, the innermost of which contained a white powder. *Id.* at 111. After they saw the powder, they notified federal law enforcement and repackaged the box. *Id.* Federal agents then removed the tube and bags, opened the bags, and performed a field test on the powder, which identified the substance as cocaine. *Id.* at 111-12.

The Court held the field test, though it "exceeded the scope of the private search," *id.* at 122, "was not a 'search' within the meaning of the Fourth Amendment" at all, *id.* at 123, because it could only detect whether the powder was cocaine, a fact in which there was no legitimate privacy interest. But the Court held that the private search authorized the government's initial search of the box. The Court explained that defendants "could have no privacy interest in the contents of the package . . . since the Federal Express employees had just examined the package." *Id.* at 119. Because "private parties had compromised the integrity of th[e] container," it "could no longer support any expectation of privacy." *Id.* at 120 n.17.

Critically, the Court acknowledged that the government learned more from its search than it learned from the FedEx employees' description of the package—namely, whether that description was accurate. But that did not matter. The Fourth Amendment did not protect "the risk of a flaw in the employees' recollection," or even "the "risk of misdescription." *Id.* at 119. Because the employees had already searched the package—however accurately or inaccurately they may have described its contents—the government was free to "avoid[] the risk" of inaccuracy and search the package itself. *Id.*

B. As every appellate court besides the Ninth Circuit to address the question has held, under *Jacobsen* government inspection of privately hash-matched images does not violate the Fourth Amendment. Pet. 10-13. The question under *Jacobsen* is whether, "by the time [the government] viewed the suspect image files, [the defendant's] expectation of privacy in his computer files had already been thwarted by a private third party." *United States v. Reddick*, 900 F.3d 636, 638 (5th Cir. 2018). When a service provider scans a user's image file and finds it contains an image that the provider has previously viewed and classified as child pornography, the answer to that question is yes.

To start, when a service provider uses hash-matching software to scan a user's image file for possible matches to child pornography, that alone is a search of the image. *See United States v. Miller*, 982 F.3d 412, 430-31 (6th Cir. 2020); *Reddick*, 900 F.3d at 639. And that search "compromise[s] the integrity" of the file, *Jacobsen*, 466 U.S. at 120 n.17, even more than a person's inspection of the image would. "Most people who view images do not use a magnifying glass to undertake a pixel-by-pixel inspection. Common hash algorithms, by contrast, catalogue every pixel," *Miller*, 982 F.3d at 430, as did the one in this case. If "a private party gets only a quick view of a picture before concluding that it is child pornography," every court would agree that would "trigger the private-search doctrine." *Id.* at 430-31; *see United States v. Wilson*, 13 F.4th 961, 974 (9th Cir. 2021) (requiring a warrant because "no Google *employee* viewed *Wilson's* files") (first emphasis added). It wouldn't make "sense . . . to treat a more accurate search of a file differently." *Miller*, 982 F.3d at 431.

Yet even before a hash-matched image is scanned, it has been searched once before. When a service provider's hash-matching software reports that a user's image file contains an image the provider classified as child pornography, that means the provider's employees have previously viewed the image in the user's file. The chances a hash-matching algorithm, including Microsoft's, returns a false match are virtually zero. Police testified as much below, Pet. App. 12a, 59a, and Walker didn't challenge the accuracy of Microsoft's algorithm, Pet. App. 2a n.2. So when police opened Walker's file, there was "a virtual certainty that [their] viewing of the file[] would disclose the same image[] that [Microsoft's] employees had already viewed." *Miller*, 982 F.3d at 429 (internal quotation marks omitted); *see also State v. Lizotte*, 197 A.3d 362, 375 (Vt. 2018) (explaining that a hash match "established that an AOL employee had previously viewed the [matched] image").

In sum, the image that police viewed here had already been inspected by Microsoft twice: once by Microsoft's hash-matching software, and once by the Microsoft employee who originally classified that image as child pornography.

C. In spite of that double inspection, a single court has held that police need a warrant to open a hash-matched image: the Ninth Circuit. It reasoned that because police only learn for certain whether a hash-matched image is child pornography when they open it, they need a warrant to open the image. *Wilson*, 13 F.4th at 973. As California predicted when the same defendant in *Wilson* unsuccessfully sought cert from his state conviction, Br. in Opp. 23, *Wilson v. California*, 142 S. Ct. 751 (2022) (No. 20-1737), that rationale hasn't persuaded other courts. Indeed, three years later, no court has followed *Wilson* and every court to address its reasoning has rejected it.[1]

Moreover, the only party affected by the slight disuniformity *Wilson* created, the United States, declined to seek certiorari in *Wilson* and had already begun seeking warrants to open hash-matched images in the Ninth Circuit before *Wilson* was even decided. *See Wilson*, 13 F.4th at 965 n.3. Were the government to change its mind and seek review of the Ninth Circuit's rule, that might warrant certiorari and indeed summary reversal. But review isn't warranted here to correct the Ninth Circuit's error.

As Walker explains, Pet. 13, the Ninth Circuit held that viewing a hash-matched image exceeds the scope of the private search because by viewing the image, "[t]he government learn[s] . . . [information] above and beyond the information conveyed" to it by the service provider. *Wilson*, 13 F.4th at 973. In particular, the

[1] In addition to the decision below, Pet. App. 17a n.8, several district courts have expressly rejected *Wilson*, *see United States v. Lowers*, No. 22-CR-00178, 2024 WL 418626, at *9-10 (E.D.N.C. Feb. 5, 2024); *United States v. Montijo*, No. 21-CR-75, 2022 WL 93535, at *6 (M.D. Fla. Jan. 10, 2022), and other courts since *Wilson* have followed the Fifth and Sixth Circuits, *see United States v. Clark*, No. 22-CR-40031, 2023 WL 3543380, at *6 (D. Kan. May 18, 2023).

Ninth Circuit reasoned, the government learns "what the image show[s]" and whether the image is "in fact child pornography," *id.*, whereas before viewing, the government only knows that the service provider said it was child pornography. Echoing that reasoning, Walker argues that the police exceeded the scope of Microsoft's search because viewing his file confirmed Microsoft's classification wasn't "mistaken." Pet. 19.

That rationale fundamentally misunderstands the private-search doctrine, which is why no court has been persuaded by it. The private-search doctrine doesn't turn on how much the private party tells police; as the Ninth Circuit itself held after *Wilson*, it doesn't even require "subjective knowledge of what was learned during the private search." *United States v. Phillips*, 32 F.4th 865, 870 (9th Cir. 2022), *cert. denied*, 143 S. Ct. 467 (2022).[2] Nor does it require police to learn nothing from their own search; if that were the law, there would be no reason to do one.

Instead, the rationale for the private-search doctrine is that the private search itself—not the information relayed about it—frustrates any expectation of privacy and permits the government to search what was searched privately. When the government does, it may "avoid[] . . . the risk of misdescription," as it did in *Jacobsen*, and verify that the private party's description was accurate. *Jacobsen*, 466 U.S. at 119.

[2] Conversely, the private-search doctrine isn't satisfied by merely receiving information from a private party. *See Jacobsen*, 466 U.S. at 120 n.17 (stating a warrant would be required if "the police simply learn from a private party that a container contains contraband" and the private party's knowledge didn't arise from a private search).

Indeed, that's the whole point of such searches. As the California Court of Appeal explained in rejecting a challenge to the same search at issue in *Wilson*, the "possibility of error exists in all cases under the private search doctrine—there is [always] some chance that the private party is conveying inaccurate information." *People v. Wilson*, 270 Cal. Rptr. 3d 200, 223 (Cal. Ct. App. 2020), *cert. denied*, 142 S. Ct. 751 (2022). If verifying whether reported contraband was "in fact" contraband meant a government search exceeded the private-search doctrine, as the Ninth Circuit held in *Wilson*, 13 F.4th at 973, no search would ever satisfy the doctrine.

D. Attempting to shore up that aberrant rationale, Walker offers a slightly different gloss on it. He claims that when police open a hash-matched file, they learn something the provider didn't: "exactly what the image shows." Pet. 18. But that's not right.

To the contrary, a file is only flagged as a match if it contains an image that the provider's employees previously viewed and determined was child pornography. Because providers usually don't keep detailed descriptions of the pornographic images they view and flag, *see Wilson*, 13 F.4th at 972, the provider may not be able to give one to police at the time it finds a match. But that's true even when providers manually review a matched file before sending it to NCMEC; the only additional information they record or convey in such cases is that they opened the file. *See, e.g.*, *United States v. Bohannon*, No. 21-12070, 2023 WL 5607541, at *1 (9th Cir. Aug. 30, 2023) (discussing a Microsoft CyberTip that answered "Yes" to "the form question, 'Did Reporting ESP view entire contents of uploaded file?'"). Yet under the Ninth Circuit's rule, and Walker's, that's enough, *see id.*—

showing that nothing turns on whether the provider recalls the details of what it saw in a child-pornographic image.

Because providers *have* viewed the images that hash-matched files contain, Walker's further analogy between hash-matching and *Walter*, Pet. 20-21, where the private party only viewed an obscene film's labeling but not the film itself, is inapt. As even the Ninth Circuit acknowledged, hash-matching is more like a variation on *Walter*'s facts where "the misdirected package c[a]me into the hands of someone who had previously viewed the same film." *Wilson*, 13 F.4th at 975. To such a recipient, the package would be as good as searched; it wouldn't "support any reasonable expectation of privacy because [its] contents [could] be inferred from [its] outward appearance." *Arkansas v. Sanders*, 442 U.S. 753, 764 n.13 (1979), *overruled on other grounds by California v. Acevedo*, 500 U.S. 565 (1991). That the Ninth Circuit "would still [require] a warrant" in that case, *Wilson*, 13 F.4th at 975, proves the error of its rule.

And this case is even easier than that one. When an image is hash-matched, a provider hasn't just seen an image's "label," Pet. 20, but has searched it pixel by pixel and knows that it's the same image its moderators previously reviewed and deemed child pornography.

E. Finally, Walker suggests the Ninth Circuit's rule could be adopted as a narrowing construction of the private-search doctrine in light of its supposed inconsistency with the trespass approach to Fourth Amendment law, as reinvigorated by *Jones*. Pet. 22. But that argument—which was never raised at any level below and which the Court has denied certiorari to address five times since *Jones*[3]—is no more availing than Walker's other defenses of the Ninth Circuit's rule.

Walker boldly claims that the return to trespass in *Jones* "makes clear that *Jacobsen* reached the wrong result." Pet. 23. But the private-search doctrine didn't begin with *Jacobsen*; it dates to the trespass era. As the Court understood trespass then, "whatever wrong was done" in private-search cases was the private trespass, not the government's subsequent search. *Burdeau*, 256 U.S. at 475; *see also Miller*, 982 F.3d at 433 (suggesting that under *Burdeau*, the provider, if anyone, is "the one that engaged in the trespass"). Moreover, in the trespass era, electronic communications weren't deemed protected by the Fourth Amendment, because they weren't a physical "effect" like a letter, *Olmstead v. United States*, 277 U.S. 438, 464 (1928), and traveled through "wires beyond [one's] house," *id.* at 466. Under that rule, a virtual image saved to the cloud would likewise be beyond trespass's protections.

Yet even if trespass law could be applied without regard to trespass-era precedent, there is no trespass in cases like this one. To start, trespass on a child-pornographic image file is an oxymoron. Trespass requires lawful possession, but no one can lawfully

[3] *See Phillips v. United States*, 143 S. Ct. 467 (2022) (No. 22-5898); *Wilson v. California*, 142 S. Ct. 751 (2022) (No. 20-1737); *Ringland v. United States*, 141 S. Ct. 2797 (2021) (No. 20-1204); *Miller v. United States*, 141 S. Ct. 2797 (2021) (No. 20-1202); *Reddick v. United States*, 139 S. Ct. 1617 (2019) (No. 18-6734) (all denying cert on whether *Jones* supplanted the private-search doctrine).

possess child pornography.[4] Consequently, there is no trespass when police open a child-pornographic image, just as there is no trespass when police search and seize drugs in plain view. And even if that weren't true, no trespass occurred here. Microsoft's service agreement with its users, like that of most service providers, requires users to consent to the disclosure of data that Microsoft reasonably believes contains child pornography.[5] *See United States v. Bohannon*, 506 F. Supp. 3d 907, 915 (N.D. Cal. 2020). When the government then opens consensually disclosed files, it doesn't trespass on them. *See United States v. Weber*, No. 22-30191, 2024 WL 722558, at *1 (9th Cir. Feb. 22, 2024); Restatement (First) of Torts sec. 253 (Am. L. Inst. 1934) (no trespass if third party in control of property has authority to consent).

Walker also claims then-Judge Gorsuch's opinion in *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), which Walker concedes didn't decide the question presented, Pet. 14, supports his trespass argument. But *Ackerman* involved a critically different fact pattern. There, a provider forwarded to NCMEC a user's email that contained one hash-matched image and three non-hash-matched images. 831 F.3d at 1294. The government viewed the email and all four images. *Id.* The Tenth Circuit reached the obvious conclusion that the government "exceeded rather than repeated [the] private search" by reviewing materials "the content of which [the provider] . . .

[4] Of course, if police unlawfully enter a space, like a house or car, and discover contraband, there is still a trespass. But here, police only inspected Walker's pornographic image file itself.

[5] That agreement is not in the record here because Walker never made a trespass argument below, to which it would have been relevant.

knew nothing about" in addition to the single hash-matched image. *Id.* at 1306. In dicta, it suggested the government also committed a trespass "when it opened and examined Mr. Ackerman's email," *id.* at 1308, which "could have contained much besides potential contraband for all anyone knew," *id.* at 1307.

Nothing in that discussion suggests a trespass occurred here. Here the police solely opened a contraband image, not an email containing it. And the file police opened was consensually disclosed under Walker's agreement with Microsoft, while the disclosure of Ackerman's entire email and multiple non-hash-matched images may have exceeded the scope of any consent he gave to disclosure.

II. The question presented doesn't otherwise merit review.

Walker claims his seemingly narrow question presented has profound ramifications. According to him, if the decision of the intermediate appeals court below stands, police will be allowed to open any cloud-stored data that an algorithm flags as "potentially relevant to law enforcement," not just hash-matched child-pornographic images. Pet. 27. In truth, the question presented wouldn't even have profound ramifications in this context.

To the contrary, answering the question presented in Walker's favor wouldn't result in suppression in his or any other pending case; the good-faith exception would protect police's reasonable reliance on the all-but-unanimous view that what they did was legal. And prospectively, it wouldn't alter police conduct. Walker concedes that hash-matching will virtually always suffice for a warrant, so his rule wouldn't lead to fewer searches. And it wouldn't even force police to get a warrant to open images; because hash-matching is so reliable, police could avoid the delay Walker's rule would otherwise impose and simply seek a warrant to search a user's computer based on the hash match.

A. Walker says the question presented "may well be outcome-determinative in this case." Pet. 17. That "may well" is used advisably. Were Walker to prevail, the good-faith exception would inevitably preclude suppression in his case—and in any other pending case presenting this question.

Walker correctly points out that the evidence used to convict him was the fruit of police's opening his hash-matched image. Pet. 17. But of course, that isn't the end of the suppression analysis. Even if opening the image were unlawful, "evidence obtained from a search should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment." *United States v. Leon*, 468 U.S. 897, 919 (1984). After all, suppression "cannot be expected . . . to deter objectively reasonable law enforcement activity." *Id.*

Here, the police's conduct was more than reasonable. They obtained a warrant after informing the court they had opened Walker's image, and reasonably relied on the court's determination that the image supporting the warrant was lawfully viewed. And at the time the warrant issued, every appellate court in the country to address the question had held opening a hash-matched image was lawful, with just one case in the interim reaching a contrary conclusion. Accordingly, many courts have held that even if opening a hash-matched image requires a warrant, the good-faith exception would bar suppression.[6]

Indeed, the circuit split on opening hash-matched images only arose because of an outlier approach to the good-faith exception that the Ninth Circuit has since rejected. In *Wilson*, the district court held that the good-faith exception didn't apply under Ninth Circuit precedent that carved out searches *preceding* a warrant's issuance from the good-faith exception. *United States v. Wilson*, No. 15-cr-02838, 2017 WL 2733879, at *13 (S.D. Cal. June 26, 2017). The government didn't challenge that ruling on appeal, forcing the Ninth Circuit to confront the Fourth Amendment question. *Wilson*, 13 F.4th at 966 n.4. Yet before it even decided *Wilson*, the Ninth Circuit had already recognized that this Court's decision in *Herring v. United States*, 555 U.S. 135 (2009), had abrogated its precedent excepting pre-warrant searches from the good-faith rule. *See United States v. Artis*, 919 F.3d 1123, 1133 (9th Cir. 2019). Consequently, the Ninth Circuit has since held that the good-faith exception shields pre-*Wilson* searches that may have violated the rule announced in *Wilson*. *See Weber*, 2024 WL 722558, at *1-2. Thus, even the Ninth Circuit agrees the good-faith exception would apply to violations of its supposed rule.

B. Of course, this Court sometimes grants certiorari to decide Fourth Amendment questions even though the good-faith exception will likely preclude suppression on remand. But answering the question

[6] *See, e.g.*, *Lowers*, 2024 WL 418626, at *10; *United States v. Tennant*, No. 23-CR-79, 2023 WL 6978405, at *17 (N.D.N.Y. Oct. 10, 2023); *Montijo*, 2022 WL 93535, at *8; *United States v. Coyne*, 387 F. Supp. 3d 387, 402-03 (D. Vt. 2018).

presented in the Petition would also have very little prospective effect on police conduct.

Usually when this Court grants certiorari on the Fourth Amendment's warrant requirement, requiring a warrant has the potential to deter a significant number of unreasonable searches. *See, e.g.*, *Carpenter v. United States*, 585 U.S. 296, 316-17 (2018) (requiring probable cause to obtain cell-site records); *Riley v. California*, 573 U.S. 373 (2014) (requiring a warrant to search arrestees' cell phones). This case is strikingly different. Here, Walker concedes that in the cases the question presented concerns, "law enforcement should have no difficulty procuring a warrant" to open a hash-matched image. Pet. 24.

That concession is correct. When police receive a hash-matched image, it means an employee "trained on th[e] . . . definition" of child pornography determined the image was contraband. *Miller*, 982 F.3d at 431. That assessment might occasionally err,[7] but it is more than enough for probable cause, and a

[7] Walker cites one reported example, an instance where Google flagged photos of a child's swollen genitalia—including one in which an adult's hand was visible—that his parents took to send to their doctor. Pet. 3, 20 (citing Kashmir Hill, *A Dad Took Photos of His Naked Toddler. Google Flagged Him as a Criminal*, N.Y. Times (June 21, 2023)). Content moderators cannot be blamed for failing to divine the purposes for taking an explicit photograph. But more importantly, when a photo is taken for benign purposes like that one, it won't be circulated and appear in hash-match scans of other users' data. Walker also misleadingly suggests that only half of the images providers send to NCMEC are really child pornography. Pet. 29 (citing *CyberTipline 2022 Report*, NCMEC, https://perma.cc/XQ5H-B4HGx1). In reality, NCMEC classifies half of the reports it receives as non-actionable because they are missing key information, like an image or an IP address. *See CyberTipline 2022 Report*.

magistrate will have no way of knowing if a tip is a rare error until the image is opened. As for the possibility of an errant hash-match, it is virtually zero. So requiring warrants here would not "ensure[] that there is, in fact, probable cause" in cases where that's actually in question. Pet. 24. Instead, it would merely delay police's opening the pornographic images they are sent while they apply and wait for warrants that are certain to issue.

And while that delay wouldn't protect anyone's Fourth Amendment rights, it would have harmful consequences for victims and law enforcement. In 2022, NCMEC sent 3.25 million reports to domestic law enforcement, 57% of which, or about 1.85 million, contained sufficient information to be actionable. *"Protecting Our Children Online": Hearing Before the S. Comm. on the Judiciary*, 118th Cong. 4 (2023) (statement of Michelle DeLaune, President and CEO, NCMEC), https://perma.cc/9YWD-B3KW. Forcing police to inundate busy state courts with millions of warrant applications just to view the images those reports contain before seeking another warrant to search the suspect's devices would make an already backlogged investigatory system sclerotic. And it would endanger here-and-now victims. Over a quarter of the material NCMEC receives is material it's never seen before. *Id.* at 13. Some of that material "has just been produced." *Id.* at 4. If police had to seek a warrant just to find out if that's the case, and go through two layers of warrant applications to search a possible victim's residence, victims' abuse would be prolonged.

Further, it is very unlikely that a decision in Walker's favor would actually require police get a warrant to open images. Instead, the likely consequence is that police would often skip the step of reviewing a suspect's image and simply get a warrant to search his devices. After all, Walker concedes that a tip from a provider that a user's file contains child pornography is probable cause to believe it does. Pet. 24. Yet if that's true, the tip is also probable cause to believe there's child pornography on the user's devices where the file is stored.

Accordingly, "many courts have held that a hash value match from a reliable source can constitute probable cause for a search warrant." *Lynch v. United States*, No. 20-CR-0223, 2023 WL 3741646, at *5 (S.D. Tex. Apr. 3, 2023); *see, e.g.*, *United States v. Blouin*, No. CR16-307, 2017 WL 3485736, at *4 (W.D. Wash. Aug. 15, 2017) ("Because hash values . . . provide high confidence that the contents of files associated with such hash values are known, the images or videos need not themselves be downloaded . . . in advance of the issuance or execution of a search warrant."). So Walker's rule would hardly safeguard Fourth Amendment interests. Instead, it would encourage police to jump to the far more intrusive step of searching a suspect's home without making certain a provider's report was accurate first.

C. Lastly, recognizing that a decision in this case wouldn't actually affect his or other child-pornography cases, Walker conjures a series of hypothetical consequences in cases that don't exist. Under the logic of the decision below, he claims, police could warrantlessly search emails, text messages and photos that algorithms flag as "terrorist content," copyright infringement, or even "potential hate speech" or "COVID misinformation." Pet. 26, 28.

Setting aside the dearth of criminal investigations into copyright infringement,[8] hate speech or misstatements about COVID, there's a reason that Walker doesn't cite a single case where the private-search doctrine has been applied to authorize searches in his hypotheticals. *See* Pet. 25-27 (only discussing algorithms scanning for such content, not any law enforcement search relying on them). The examples he gives involve content that's flagged in the first instance by a program, like "[k]eyword search programs [that] flag potential hate speech," or software that compares user content to copyrighted material. Pet. 26. Decisions like the one below, by contrast, authorize searches where hash-matching is used to "identify *known* child pornography" that someone has previously seen and flagged. Pet. App. 18a (emphasis added).

None of the decisions Walker criticizes say that—or decide if—a program's flagging a file as child pornography in the first instance would be enough of a private search to allow police to open it. So whether the private-search doctrine is satisfied by a purely virtual search is a question for a future case. And judging by Walker's inability to cite any case where that question has arisen, the wait for that case might be a while.

[8] There are rarely enforced criminal copyright infringement statutes, *see, e.g.*, 17 U.S.C. 506, but it is doubtful that a criminal copyright infringement investigation has ever begun with a tip from Google that its copyright-infringement content filter has caught someone uploading an infringing text file to his cloud storage, as Walker suggests could occur, Pet. 26.

CONCLUSION

The petition for a writ of certiorari should be denied.

Respectfully submitted,

TIM GRIFFIN
Arkansas Attorney General
NICHOLAS J. BRONNI
Solicitor General
Counsel of Record
DYLAN L. JACOBS
Deputy Solicitor General
ASHER STEINBERG
Senior Assistant
Solicitor General
JOSEPH KARL LUEBKE
Assistant Attorney General

OFFICE OF THE ARKANSAS
ATTORNEY GENERAL
323 Center Street
Suite 200
Little Rock, AR 72201
(501) 682-6302
nicholas.bronni@arkansasag.gov

March 22, 2024