No. 23-___

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

PETITION FOR A WRIT OF CERTIORARI

Michael Kiel Kaiser
LASSITER & CASSINELLI
1218 W. 6th Street
Little Rock, AR 72201

Easha Anand
Counsel of Record
Jeffrey L. Fisher
STANFORD LAW SCHOOL
SUPREME COURT
LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305
(650) 724-3345
eanand@stanford.edu

QUESTION PRESENTED

Technology companies automatically scan trillions of digital files that are uploaded onto their servers, including emails and photographs. Their algorithms can scan for anything, from faces in photographs to the content of digital files stored in online file storage systems.

The question presented is: Does the Fourth Amendment require police to get a warrant before they open a digital file that was flagged by a private technology company's computer program as potentially containing illegal content but that no human being has previously opened?

RELATED PROCEEDINGS

Walker v. State, No. CR-22-572 (Ark. Ct. App. May 17, 2023)

State v. Walker, No. 10CR-20-107 (Ark. Cir. Ct. Clark Cnty. Apr. 1, 2022)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Constitutional Provisions

Statutes

Legislative Materials

Other Authorities

PETITION FOR A WRIT OF CERTIORARI

Petitioner Jonathan Walker respectfully petitions for a writ of certiorari to review the judgment of the Court of Appeals of Arkansas, Division III.

OPINIONS BELOW

The decision of the court of appeals is available at 2023 Ark. App. 295 and reprinted in the Appendix to the Petition ("Pet. App.") at 1a-29a. The Arkansas Supreme Court's order denying review is reprinted at Pet. App. 31a. The district court's order denying petitioner's motion to suppress evidence (Pet. App. 30a) is unpublished.

JURISDICTION

The decision of the court of appeals was issued on May 17, 2023. Pet. App. 1a. On September 21, 2023, the Arkansas Supreme Court denied en banc review. *Id.* 31a. This Court has jurisdiction under 28 U.S.C. § 1257(a).

RELEVANT CONSTITUTIONAL PROVISION

The Fourth Amendment of the United States Constitution provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

INTRODUCTION

Warrantless searches are generally prohibited under the Fourth Amendment. But this Court has carved out a narrow exception: Where a private actor has previously conducted a search, the government may repeat that search, so long as it does not go beyond what the private actor has done. *United States v. Jacobsen*, 466 U.S. 109, 115 (1984). Purporting to apply that exception, the Arkansas Court of Appeals held that a police officer does not violate the Fourth Amendment by opening a file that had been flagged as potential contraband by a private actor's algorithm, even though no human being ever opened the file.

The opinion below is in direct conflict with an opinion from the Ninth Circuit, which finds a Fourth Amendment violation on materially identical facts. *See United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021). It's also wrong. Opening the file—seeing the actual image in question—went beyond the scope of the private actor's search, which was limited to flagging the image as potential contraband. And, as then-Judge Gorsuch put the point in a similar case, there's "reason to wonder" whether the private search doctrine is even good law in the wake of this Court's recent Fourth Amendment decisions. *See United States v. Ackerman*, 831 F.3d 1292, 1307 (10th Cir. 2016).

When a private actor's algorithm flags potential contraband, the solution for police is simple: Get a warrant. Many police departments have a policy of doing just that. The signoff of a neutral magistrate is particularly critical in cases like this one, which involve images suspected of being child sexual abuse material (CSAM). Companies understandably face

immense public pressure to clear their platforms of CSAM, and police officers are understandably eager to identify potential criminals.

And those understandable pressures may lead to overlooking the privacy interests on the other side of the ledger. Although we know little about the content of the algorithms that large technology companies use to flag potential contraband, we know that these algorithms can be wildly overinclusive, flagging, for instance, a photograph of a rash on a toddler, sent to a pediatrician, as potential CSAM. *See* Kashmir Hill, *A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal.*, N.Y. Times (June 21, 2023), https://perma.cc/7VPV-G8WA. Before a police officer opens a file that may contain a perfectly legal—and deeply personal—image, a neutral party should confirm that doing so strikes the appropriate balance between privacy and law enforcement.

The implications of the question presented also extend far beyond this case. If the opinion below is correct, law enforcement and technology companies can collaborate to allow police officers virtually unfettered access to private emails, documents, and photographs. This Court has been vigilant about safeguarding Fourth Amendment rights in the face of new technologies. It should grant certiorari in this case to make clear that, before opening a file that no private actor had previously opened, police officers must obtain a warrant.

STATEMENT OF THE CASE

A. Factual background

1. On April 28, 2020, a Microsoft algorithm called PhotoDNA flagged a file uploaded to a private Microsoft OneDrive account as potential CSAM. Pet. App. 2a-3a.

Very little about PhotoDNA is publicly known. The algorithm is based around a technology known as "hash matching," which converts the photograph into a string of characters that are unique to that photograph. Pet. App. 14a-15a. If any two photographs have the same "hash value," they're virtually certain to be identical. *Id.* "Hash matching" is extremely reliable at identifying identical photographs. *Id.*

But PhotoDNA doesn't just match identical photographs. It also purports to be able also to detect similar photographs (for instance, photographs that have been rotated, cropped, or otherwise altered). *See* Ofcom, *Overview of Perceptual Hashing Technology* 3 (2022), *available at* https://perma.cc/2R54-C2S8. There is no public data about the reliability of the algorithm.

PhotoDNA attempts to match users' files to databases of suspected CSAM. *See PhotoDNA*, Microsoft, https://perma.cc/9N9T-8XVT (last accessed Feb. 14, 2024). There are many such databases, including ones maintained by Microsoft and the National Center for Missing and Exploited Children (NCMEC).[1] Those databases may contain a range of

[1] At the suppression hearing, one officer testified that PhotoDNA flagged Mr. Walker's file as a potential match with

files, from CSAM confirmed as such by law enforcement to more innocent content, such as a home video recorded by a seven-year-old. *See* Kashmir Hill, *How Your Child's Online Mistake Can Ruin Your Digital Life*, N.Y. Times (Nov. 29, 2023), https://perma.cc/ED9Q-HVY3.

2. Once PhotoDNA flagged the image as potential CSAM, federal law required Microsoft to report the image to NCMEC. *See* 18 U.S.C. §§ 2258A(a), 2258E(6). Microsoft accordingly sent along a "CyberTip" to NCMEC that contained the file, the hash value, the file name, and the IP address associated with the file. Pet. App. 3a.

NCMEC classified the file as "Apparent Child Pornography (Unconfirmed)" and assigned it NCMEC's lowest priority level. Pet. App. 88a. NCMEC added the following note to the CyberTip: "Please be advised that NCMEC staff have not opened or viewed any uploaded files submitted with this report at this time." *Id.* 98a. It then forwarded the CyberTip to Arkansas state police, based on the location of the IP address. *Id.* 3a.

4. Upon receipt, an Arkansas State Police officer opened the file and reviewed the image. Pet. App. 3a. He then swore out an affidavit for a warrant to search the physical address associated with the IP address from the CyberTip. *Id.* 9a. Specifically, he stated:

Microsoft's CSAM database, while another testified that it was a potential match with NCMEC's database. *Compare* Pet. App. 61a *with id.* 41a. The record suggests the former. *Id.* 93a. Which database was used in this case was not relevant to the decision below and is not relevant to the question presented.

> Microsoft OneDrive made the report to NCMEC on April 28, 2020. The cyber tip reported that one (1) image of apparent child pornography (unconfirmed) was uploaded to a Microsoft OneDrive Account. Microsoft OneDrive provided the image to NCMEC and I was eventually provided the image that was uploaded. The image is of a prepubescent minor male depicting nudity in a sexually suggestive pose.

Id. Nowhere in the affidavit did the officer explain why Microsoft believed that the image might contain "apparent child pornography."

Based on the affidavit, a search warrant was issued. Pet. App. 4a. Law enforcement searched Mr. Walker's apartment and seized several computers, some of which contained CSAM. *Id.*

B. Procedural history

1. The State charged Mr. Walker with multiple child pornography related offenses. Pet. App. 1a. Mr. Walker filed a motion to suppress the evidence resulting from the search of his apartment and computers. *Id.* 4a n.5. He argued that Arkansas police violated the Fourth Amendment by opening the file forwarded by Microsoft and NCMEC without first obtaining a warrant. *Id.* 86a.

The trial court held a hearing on the motion to suppress. Two Arkansas police officers testified. Pet. App. 34a-68a. Neither provided information about how PhotoDNA worked or about the database of suspected CSAM. *Id.* Both acknowledged that neither Microsoft nor NCMEC had opened the file in question. *Id.* 53a.

The trial court denied the motion to suppress without providing any reasoning. Pet. App. 30a. Mr. Walker was then convicted of multiple counts of distributing, possessing, or viewing matter depicting sexually explicit conduct involving a child and sentenced to 450 years in prison. *Id.* 5a.

2. Mr. Walker appealed his conviction to the Arkansas Court of Appeals and renewed his argument that law enforcement's warrantless inspection of the file flagged by Microsoft violated his Fourth Amendment rights.[2] Pet. App. 8a.

In response, the State argued that opening Mr. Walker's file without a warrant was permitted under the private search doctrine. Pet. App. 11a. It relied on *United States v. Jacobsen*, 466 U.S. 109 (1984). In *Jacobsen*, employees of a private freight company opened a damaged package and observed sealed bags of unknown white powder within. *Id.* at 111. The company employees alerted law enforcement, who—without a warrant—opened the bags and performed a chemical test that identified the white powder as cocaine. *Id.* at 111-12.

Jacobsen held that law enforcement's inspection of the package did not violate the Fourth Amendment. This Court explained that when law enforcement officers merely repeat the same search a private actor has conducted, they do not need a warrant. *Jacobsen*, 466 U.S. at 115. But any "additional intrusion" must be separately justified. *Id.* at 122. Because the company employees had examined the package, the

---

[2] Mr. Walker also raised other challenges to his conviction and sentence. Pet. App. 2a. Those claims are not relevant to this petition.

officers were free to inspect the same package themselves. *Id* at 119-120. In so doing, the officers "learn[ed] nothing that had not previously been learned during the private search." *Id*. at 120.

Additionally, this Court held that the officers' chemical test did not constitute a "search" under the Fourth Amendment. The Court acknowledged that such a test had not been previously conducted by private actors, and police "therefore exceeded the scope of the private search." *Jacobsen*, 466 U.S. at 122. However, the majority reasoned that the chemical test, which was limited to determining whether or not the substance was cocaine was not a search under the Fourth Amendment *Id.* at 123 (citing *United States v. Place*, 462 U.S. 696 (1983)). The field test could "disclose only one fact"—"whether or not a suspicious white powder was cocaine." *Jacobsen*, 466 U.S. at 122. If it wasn't cocaine, the field test "could tell [police] nothing more, not even whether the substance was sugar or talcum powder." *Id.*

3. Mr. Walker responded that *Jacobsen* did not apply to the law enforcement conduct here. Brief of Appellant Jonathan Walker at 19-23, *Walker v. State*, 2023 Ark. App. 295 (Ark. Ct. App. 2023) (No. CR-22-572). Arkansas police didn't merely repeat the same search that employees at Microsoft had conducted. Microsoft employees saw only that the PhotoDNA algorithm had flagged the file as potential CSAM; Arkansas police actually opened the file. Pet. App. 11a. In support of this argument, Mr. Walker cited the Ninth Circuit's decision in *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021). Pet. App. 17a n.8. In *Wilson*, the Ninth Circuit held that, absent a warrant, the Fourth Amendment forbids law enforcement from

opening a file that had been flagged by a private actor's algorithm as suspected CSAM if no private actor had previously opened the file. 13 F.4th at 972-79.

4. The Arkansas Court of Appeals affirmed Mr. Walker's conviction. Pet. App. 2a. The Arkansas court reasoned that because Mr. Walker's file had already been labeled as suspected CSAM, the government's inspection of the file "merely confirmed what had already been learned in the private search." *Id.* 13a.

The Arkansas court declared itself "strongly persuaded" by the Fifth Circuit's holding in *United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018), which had found that no Fourth Amendment violation occurred when law enforcement opened a file in equivalent circumstances. Pet. App. 13a. Citing *Reddick*, the Arkansas court described the high reliability of hash-value technology, and therefore held that the officers "learned no more than had already been learned from the hash-value analysis of the private search" by opening and viewing the file. *Id.* 18a. The Arkansas court also found "instructive" the Sixth Circuit's holding in *United States v. Miller*, 982 F.3d 412 (6th Cir. 2020), which similarly permitted law enforcement to inspect files without a warrant under the private search doctrine even when no human being had previously opened the files. Pet. App. 16a-17a. The Arkansas court acknowledged that *Wilson* "reached a different result . . . on similar facts," but nonetheless declared itself "persuaded by the analysis in *Reddick* and *Miller*." *Id.* 17a n.8.

5. The Arkansas Supreme Court declined to review the decision of the Arkansas Court of Appeals. Pet. App. 31a.

REASONS FOR GRANTING THE WRIT

I. There is a square split on the question presented.

In ruling that law enforcement did not violate Mr. Walker's Fourth Amendment rights, the Arkansas Court of Appeals was "persuaded by the analysis" of the Fifth and Sixth Circuits. Pet. App. 17a n.8. At the same time, it recognized that the Ninth Circuit "reached a different result . . . on similar facts." *Id.*

The Arkansas court was correct. If anything, it understated the extent of the split. Though the Fifth and Sixth Circuits both agree that the Fourth Amendment permits law enforcement to open files in cases like this one, they disagree on why. Appellate courts in both California and Florida have also aligned themselves with the Fifth and Sixth Circuits. And though the Ninth Circuit is the only federal court of appeals to squarely hold that the Fourth Amendment requires a warrant before law enforcement opens a file that a private actor's algorithm has flagged as potential contraband, the Tenth Circuit—in an opinion by then-Judge Gorsuch—has endorsed the Ninth Circuit's underlying logic.

1. *No warrant required*. Consistent with the Arkansas rule, both the Fifth and Sixth Circuits, as well as other state courts, would have permitted the warrantless search of Mr. Walker's file. As in Mr. Walker's case, in each of these courts, a private actor's software marked the files in question as potential contraband, but neither the private actor nor NCMEC actually opened the files.

a. In *United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018), law enforcement opened and reviewed files

that Microsoft's algorithm had flagged as potential CSAM without obtaining a warrant. *Id.* at 638. Even though nobody at Microsoft or NCMEC had previously viewed the files, the Fifth Circuit held that this search "did not effect an intrusion on Mr. Reddick's privacy that he did not already experience as a result of the private search." *Id.* at 637.

The Fifth Circuit reasoned that the visual review of those files "was akin to the government agents' decision to conduct chemical tests" in *United States v. Jacobsen*, 466 U.S. 109 (1984). *Reddick*, 900 F.3d at 639. According to the Fifth Circuit, visual inspection of the images "merely confirmed that the flagged file was indeed child pornography," just as the chemical test in *Jacobsen* merely confirmed whether the powder was cocaine. *Id.*

b. In *United States v. Miller*, 982 F.3d 412 (6th Cir. 2020), the Sixth Circuit rejected the reasoning of the Fifth Circuit but arrived at the same outcome.

The Sixth Circuit dismissed *Reddick*'s suggestion that a detective's visual inspection of algorithmically flagged files was the equivalent of the chemical test in *Jacobsen*. *Miller*, 982 F.3d at 429. However, the Sixth Circuit nevertheless agreed with the Fifth Circuit's conclusion that the Fourth Amendment did not require a warrant when a private actor's algorithm had flagged potential contraband. Citing the reported reliability of hash-matching technology, the Sixth Circuit held there was a "virtual certainty" that law enforcement review of the images would disclose that they were CSAM, and thus the review did not exceed the scope of the private search. *Id.* at 429-31.

The Sixth Circuit hastened to add that, were it not for *Jacobsen*, there would be "legitimate" objections to

its holding. *Miller*, 982 F.3d at 418. The court acknowledged the force of the argument that opening the file should qualify as a search: The Fourth Amendment protects "papers" from government trespass; opening a file is a trespass on digital "papers"; and this Court requires a warrant before police can open a sealed letter entrusted to a third party, the analog equivalent of opening a file like the one at issue *Id.* at 418, 432-33 (first citing *United States v. Jones*, 565 U.S. 400, 404-08 (2012); and then citing *Ex parte Jackson,* 96 U.S. 727, 732-33 (1877)). However, the Sixth Circuit believed *Jacobsen* foreclosed any consideration of that argument and so nonetheless ruled against the defendant. *Miller*, 982 F.3d at 433.

c. Three state appellate courts have also endorsed the position of the Fifth and Sixth Circuits. As detailed *supra*, the Arkansas Court of Appeals held that because law enforcement "merely confirmed what had already been learned in the private search," the Fourth Amendment did not require a warrant. Pet. App. 13a. The California Court of Appeals reached the same conclusion in a similar case: Because "the government did not further infringe on" the defendant's privacy, "but rather guarded against the risk that" the private actor's "report was wrong," no warrant was required. *People v. Wilson*, 270 Cal. Rptr. 3d 200, 219 (Cal. Ct. App. 2020), *review denied*, 2021 Cal. LEXIS 485 (Cal. 2021). And the Florida District Court of Appeal, block quoting *Reddick*'s analysis, has also reasoned that police officers do not need a warrant to open a file that a private party's algorithm has flagged as potential contraband, because they "merely confirm[] what the hash value match already had

established." *Morales v. State*, 274 So. 3d 1213, 1218 (Fla. Dist. Ct. App. 2019).

2. *Warrant required.*

a. On functionally identical facts to this case, the Ninth Circuit has held that the Fourth Amendment requires a warrant before law enforcement opens a file flagged as potential contraband by a private actor's software.

In *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021), the Ninth Circuit held that opening such a file fell outside the private search doctrine and thus violated the Fourth Amendment. It offered two reasons for this holding. First, police "learned exactly what the image showed." *Id.* at 973. Until the file was opened, police "had no *image* at hand at all; the entire composition was hidden." *Id.* at 974 (emphasis in original). But once police opened the file, they learned information about who was in the image, where the image was taken, and so on. *Id.* Second, police "learned the image was in fact" CSAM, not just *potential* CSAM—information that was "clearly necessary" for the prosecution. *Id.* at 973.

The Ninth Circuit's conclusion followed directly from this Court's decision in *Walter v. United States*, 447 U.S. 649 (1980). In *Walter*, a private party opened a package and found boxes of film, labeled with "suggestive drawings" and "explicit descriptions" that made clear they depicted illegal obscene content. *Id.* at 652. Police officers then viewed the films without obtaining a warrant. *Id.* Because the private party had not viewed the films, this Court held that the police officers' viewing violated the Fourth Amendment. Viewing the films was a "significant expansion of the [private] search" even if the "descriptive labels" had

already been exposed. *Id.* at 657-58. As the Ninth Circuit explained, a flag by an algorithm as potential contraband "function[s] as a label for the images in the same way that the boxes describing the films in *Walter* suggested that the images on the films were obscene." *Wilson*, 13 F.4th at 973. And opening the files—"like viewing the movie in *Walter*—substantively expanded the information available to law enforcement far beyond what the label alone conveyed." *Id.*

The Ninth Circuit also acknowledged that it was "contribut[ing] to a growing tension in the circuits," recognizing that both the Fifth and Sixth Circuits "recently decided the issue before us and came to a contrary conclusion." *Wilson*, 13 F.4th at 976, 978.

b. Although the Tenth Circuit has yet to rule directly on the question presented, the Ninth Circuit has correctly explained that the "underlying analysis" in then-Judge Gorsuch's opinion in *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), is "entirely consistent with" the Ninth Circuit's opinion and at odds with the opinions of the Fifth and Sixth circuits and various state courts. *Wilson*, 13 F.4th at 977.

Ackerman held that a private actor's "search that suggested a hash value match" between the defendant's email attachment and a database of potential CSAM did not entitle a government actor to open the email without a warrant. *Ackerman*, 831 F.3d at 1305, 1308-09. By opening the email, the government actor "could have learned any number of private and protected facts." *Id.* at 1306. To be sure, in *Ackerman*, the government opened not only the image flagged as potential CSAM but also three additional attachments. *Id.* But as the Ninth Circuit explained, Ackerman's central holding—that warrantless

government review of hash-matched images "risked exposing new and protected information"—should apply even in cases like this one, where the only image in question was the one flagged by a private actor's algorithm. *Wilson*, 14 F.4th at 976-77 (quoting *Ackerman*, 831 F.3d at 1306 (Gorsuch, J.)).

Then-Judge Gorsuch additionally observed for the Tenth Circuit that the status of the private search doctrine more broadly was at best "uncertain" in light of this court's decision in *United States v. Jones*, 565 U.S. 400 (2012). *Ackerman*, 831 F.3d at 1307. *Jacobsen* held only that the government did not infringe on the defendant's reasonable expectation of privacy by repeating a private search. But *Jones* made clear that even if the government does not infringe on a reasonable expectation of privacy, it can still effect a Fourth Amendment search if it commits a physical trespass. *Jones*, 565 U.S. at 409. The government's conduct in *Jacobsen* would have constituted a trespass to chattels at common law, but *Jacobsen* did not address that possibility. *Ackerman*, 831 F.3d at 1307 (citing *Jones*, 565 U.S. at 419 n.2 (Alito, J., concurring in the judgment)). In fact, the Tenth Circuit found the impact of *Jones* was "even clearer" in the digital file context than in *Jacobsen*, because the government sought to justify "the warrantless opening and examination of (presumptively) private correspondence." *Ackerman*, 831 F.3d at 1307.

3. The time is now ripe for this Court to resolve the question presented. Most previous petitions on this question were denied before the Ninth Circuit's opinion in *Wilson* created a clean split. *See United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018), *cert. denied*, 139 S. Ct. 1617 (2019) (No. 18-6734); *United*

States v. Miller, 982 F.3d 412 (6th Cir. 2020), *cert. denied*, 141 S. Ct. 2797 (2021) (No. 21-8017). In the one case denied since the Ninth Circuit's decision, respondents claimed that "the issues are of limited and diminishing importance" because the law enforcement unit in that case "had already changed its practices" to secure a warrant. Brief in Opposition at 28-29, *Wilson v. California*, 142 S. Ct. 751 (2022) (No. 20-1737). In this case, there has been no such change of practice; as far as the record discloses, Arkansas police continue to open files in cases like this one without securing a warrant.

This Court's intervention is sorely needed. There is now a square 2-1 split among the federal courts, with three state appellate courts weighing in as well. Indeed, the Ninth Circuit has split from California courts—and the two courts reached different conclusions in the *same* case, involving the *same* challenged conduct as to the *same* defendant. *Compare United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021), *with People v. Wilson*, 270 Cal. Rptr. 3d 200 (Cal. Ct. App. 2020); *see* Petition for Writ of Certiorari at 12, *St. James School v. Biel*, 140 S. Ct. 2049 (2020) (No. 19-348) (certiorari granted, 140 S. Ct. 680, and consolidated under the name *Our Lady of Guadalupe School v. Morrissey-Berru*, 140 S. Ct. 2049 (2020) (No. 19-267)) (granting certiorari where state court split from federal circuit in which state was located).

II. This case is an ideal vehicle for resolving the question presented.

The issue whether the government exceeded the scope of the private search was pressed and passed upon below. Pet. App. 8a-18a, 70a-76a; Brief of Appellant Jonathan Walker at 19-23, *Walker v. State*,

2023 Ark. App. 295 (Ark. Ct. App. 2023) (No. CR-22-572).

The question presented may well be outcome-determinative in this case. Police officers used the information they learned from opening the disputed file to secure a warrant, and all the evidence used to convict Mr. Walker was found pursuant to that warrant. *See* Pet. App. 9a. If the Fourth Amendment forbade opening the disputed file, the evidence in question was all fruit of the poisonous tree.

Finally, it's clear that the Ninth Circuit would have decided this case differently than the court below. Critical to the Ninth Circuit's holding was the fact that neither the private actor nor NCMEC had opened the file in question. The record here makes clear the same was true in this case. By contrast, in many cases, there is a factual dispute about whether the private actor or NCMEC opened the file before law enforcement did, such that it is unclear how the case would come out in the Ninth Circuit. *See, e.g.*, *State v. Osgood*, No. 1 CA-CR 22-0302, 2023 WL 6628636 (Ariz. Ct. App. Oct. 12, 2023) (record unclear about whether private companies had viewed images); *United States v. Ringland*, 966 F.3d 731, 733 (8th Cir. 2020) (NCMEC possibly reviewing some images that the private entity had not reviewed).

III. The lower court's opinion is wrong.

"[T]he most basic constitutional rule" of the Fourth Amendment is that warrantless searches are per se unreasonable, subject to few exceptions that are "jealously and carefully drawn." *Coolidge v. New Hampshire*, 403 U.S. 443, 454-55 (1971) (quotation omitted). Accordingly, in this case, the State bears the

burden of proving that its agents' warrantless search was justified by the private search exception to the Fourth Amendment's warrant requirement. *Id.* at 455 (quoting *United States v. Jeffers*, 342 U.S. 48, 51 (1951)). Under the private search doctrine, the government may repeat a private search to learn what had "previously been learned during [that] search." *United States v. Jacobsen*, 466 U.S. 109, 120 (1984). But the government "may not exceed the scope of the private search unless it has the right to make an independent search." *Walter v. United States*, 447 U.S. 649, 657 (1980).

The government has not met its burden of showing that the private search exception applies here. By opening and inspecting the photograph when no private party had previously done so, the government exceeded the scope of the private search. It learned crucial information—above and beyond what any employee at Microsoft had learned—about what was depicted in the photograph and whether it constituted CSAM.

1. A police officer exceeds the scope of a private search when he opens and visually inspects files that were never opened by a private actor. That is so because he obtains information that had not "previously been learned" by the private party: He learns what the image actually depicts and thereby confirms that it is contraband.

The police officer—and only the police officer—learns exactly what the image shows. As the Ninth Circuit put the point, "[o]nly the image itself could reveal, for example, the number of minors depicted, their identity, the number of adults depicted alongside the minors, the setting, and the actual sexual acts

depicted." *United States v. Wilson*, 13 F.4th 961, 974 (9th Cir. 2021). The image might also contain details about a person's home or objects he owns. The private actor knows only that an algorithm has flagged the file as potential contraband; he does not know what the image looks like.

As a result, the police officer—and only the police officer—is able to confirm that the image is contraband. To be sure, the private actor knows, because of the algorithm's flag, that the image is *potential* contraband. But as then-Judge Gorsuch explained, that's a far cry from confirming that the image actually was contraband. *United States v. Ackerman*, 831 F.3d 1292, 1306 (10th Cir. 2016). In cases like this one, for instance, "the hash value match could have proven mistaken" or the person "who identified the original image as child pornography [could have been] mistaken in his assessment." *Id.*

Start with the first possibility—that "the hash value match could have proven mistaken." Courts are right to note that hash value matching, standing alone, is extremely reliable. *See, e.g.*, *United States v. Miller*, 982 F.3d 412, 430 (6th Cir. 2020). But PhotoDNA doesn't just flag images that are a "hash match" to images in Microsoft's database of actual CSAM. It also flags images that are variants of the images in its database. Microsoft doesn't release details on how it finds those variants, or exactly how much variance is permitted, but independent researchers have concluded that PhotoDNA has a

"non-negligible inaccuracy" rate and can easily "generate false-positive results."[3]

Now consider the second possibility mentioned by then-Judge Gorsuch—that the person "who identified the original image as child pornography was mistaken in his assessment." Again, neither Microsoft nor NCMEC releases details on how its content moderators identify images as prohibited CSAM. But *The New York Times* has documented how tech companies routinely classify entirely innocent images—a photograph of a rash on a toddler sent to a pediatrician, or an intimate moment between a mother and child captured by the sentimental father—as CSAM.[4]

Because police learn additional information by opening the file, this case is squarely governed by *Walter*. Recall that in *Walter*, a private party saw film boxes that were labeled (via "suggestive drawings" and "explicit descriptions of the contents") as obscenity. 447 U.S. at 652. But police still exceeded the scope of the search by viewing the films themselves. Viewing the film gave more information to police than even the most detailed label could. *Id.* at 657. And doing so confirmed that the films were, in fact, obscenity. *Id.* A majority of the Justices on this Court held that the Fourth Amendment had been violated. So too, here. The private hash-match may *label* the disputed file as

---

[3] *See* Ofcom, *Overview of Perceptual Hashing Technology* 3 (2022), *available at* https://perma.cc/2R54-C2S8; Neal Krawetz, *PhotoDNA and Limitations*, Hacker Factor Blog (Aug. 27, 2021), https://perma.cc/DUW5-25QZ.

[4] *See* Kashmir Hill, *A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal*, N.Y. Times (June 21, 2023), https://perma.cc/7VPV-G8WA.

potential contraband, but only viewing the file provides the needed information to confirm its illegal nature.

2. Courts that have reached a contrary conclusion have relied on two rationales, both mistaken.

First, the court below and the Sixth Circuit believed that the key question was how reliable the PhotoDNA technology is at flagging CSAM. *See, e.g.*, Pet. App. 18a; *Miller*, 982 F.3d at 417-18. The Sixth Circuit, for instance, held that the Fourth Amendment permitted opening a defendant's file because the "hash-value match's near-perfect accuracy" creates a "virtual certainty that the files" were CSAM. *Miller*, 982 F.3d at 418. But the question is not whether opening the file is "virtually certain" to reveal CSAM. It's whether there is a "'virtual certainty' that its search *will disclose nothing more than what a private party's earlier search has revealed*." *See id.* (emphasis added). Here, the opposite is true: The private actor knew only that PhotoDNA flagged the material as potential CSAM, but nothing else; opening the file not only confirmed that it was CSAM but inevitably revealed other information (how many people were in the image, where it was taken, and so on). As the Ninth Circuit explained, reliability "is pertinent to whether probable cause could be shown to obtain a warrant, not to whether the private search doctrine precludes the need for a warrant." *Wilson*, 13 F.4th at 979.

Second, the Fifth Circuit believed that opening a file flagged by a private actor was the equivalent of the chemical test in *Jacobsen*, because it "merely confirmed that the flagged file was indeed child pornography." *United States v. Reddick*, 900 F.3d 636,

639 (5th Cir. 2018). But that reasoning "conflates" two "entirely different" parts of the Court's holding in *Jacobsen*. *Wilson*, 13 F.4th at 978. *Jacobsen* did not excuse the warrantless chemical test "via the private search exception but for an entirely different reason"—namely, that a chemical test is not a search at all for Fourth Amendment purposes. *Id.* No party in this case, by contrast, has argued that opening a digital file is not a search.

Even on the Fifth Circuit's reading of *Jacobsen*, the analogy is flawed. The Fifth Circuit claimed that opening the image file was akin to the chemical tests of *Jacobsen* because it "merely confirmed that the flagged file was indeed child pornography." *Reddick*, 900 F.3d at 639. But in *Jacobsen*, the drug test was binary; it could reveal only whether or not the substance was cocaine and "no other arguably 'private' fact," not even "whether the substance was sugar or talcum powder." 466 U.S. at 122-23. By contrast, if the photographs flagged in this case were not CSAM, an officer would learn far more than whether a package contained "sugar or talcum powder"; he would have access to deeply personal photographs that could reveal intimate details about a person's life. As the Sixth Circuit put the point: "If the files portrayed something other than child pornography, [the government] would have learned what they showed—whether an embarrassing picture of the sender or an innocuous family photo." *Miller*, 982 F.3d at 429.

3. To the extent there's any doubt, *Jacobsen*'s private search rule should be construed narrowly, because recent precedents of this Court put *Jacobsen* on shaky footing.

a. First, as explained *supra*, this Court's decision in *United States v. Jones*, 565 U.S. 400 (2012), makes clear that *Jacobsen* reached the wrong result. As then-Judge Gorsuch observed, "the warrantless opening and examination of (presumptively) private correspondence . . . seems pretty clearly to qualify as exactly the type of trespass to chattels that the framers sought to prevent when they adopted the Fourth Amendment." *Ackerman*, 831 F.3d at 1307.

Considering whether there has been a trespass makes good sense in private search cases. Otherwise, *Jacobsen*'s rule that a government actor can repeat a search conducted by a private actor would allow law enforcement to storm into your bedroom without a warrant because a private party previously broke in and told the police what she saw.

b. Second, consider *Carpenter v. United States*, 138 S. Ct. 2206 (2018). That case cautioned against "mechanically applying the third-party doctrine" to new contexts. *Id.* at 2219. Justice Gorsuch took an even stronger stand against the third-party doctrine, pointing out that "our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers," a result "functionally compelled by the demands of modern life." *Id.* at 2262, 2270 (Gorsuch, J., dissenting).

Jacobsen derives the private search doctrine from the very third-party doctrine that this Court cautioned in *Carpenter* should be limited. *Jacobsen*, 466 U.S. at 117; *see also Wilson*, 13 F.4th at 971 n.9. Uncertainty about the third-party doctrine thus should cast doubt on the continued vitality of the private search doctrine.

4. Finding a Fourth Amendment violation in cases like this one will not preclude the detection or prosecution of CSAM. It would mean only that police officers get a warrant before opening a file that no private actor has previously opened. Indeed, many jurisdictions already require or otherwise routinely obtain warrants before opening a file flagged by a private company as potential CSAM. *See Wilson*, 13 F.4th at 965 n.3. There is no evidence that police in those jurisdictions are unable to adequately investigate CSAM-related crimes. Moreover, because the file in question is already in law enforcement's possession, there's no risk that evidence will be lost, and no other exigency that would counsel against obtaining a warrant. And police are already required to get a warrant before they search a person's home or hard drive. An additional warrant requirement for opening an image flagged as contraband merely changes when, not whether, police must seek a warrant.

Based on what we know today, law enforcement should have no difficulty procuring a warrant when a program flags an image as potential CSAM; it must simply explain the process by which the image was flagged. *See, e.g.*, *Ackerman*, 831 F.3d at 1309 (acknowledging that "NCMEC's law enforcement partners will struggle not at all to obtain warrants to open emails" with the right "facts in hand"). But we have limited insight into how the technology works, and it evolves quickly. Involving a "neutral and detached magistrate" ensures that there is, in fact, probable cause before law enforcement goes rummaging through private photographs and emails. *See Riley v. California*, 573 U.S. 373, 382 (2014) (quotation omitted).

IV. The question presented is important.

1. If the decision below stands, OneDrive files hash-value matched as CSAM are not the only files that law enforcement may open up without a warrant. Police could open photographs from your iPhone that facial recognition technology thinks contain known criminals; emails from your Outlook account that a word search flags as containing terrorist content; or documents you've backed up on Google Drive that a piece of software identifies as infringing a copyright. After all, the decision below turned only on "the reliability of hash-value matching to identify known child pornography." Pet. App. 18a.

To start, big tech surveillance isn't limited to Microsoft OneDrive. Private actors are scanning *everything* uploaded to "the cloud"—that is, the private servers that host emails, store photographs, and back up documents. *See* Michael Tabb et al., *What is "The Cloud" and How Does It Pervade Our Lives?*, Sci. Am. (Dec. 1, 2021), https://perma.cc/2X9L-ND3F. The average person stores 500GB on "the cloud"—the equivalent of 300,000 photographs or 37.5 million pieces of paper—and in many cases, files are uploaded to the cloud automatically, even if the user hasn't chosen to do so. Ivan Dimitrov, *Stacks of Storage: How Much Space Does Your Data Take Up?*, pCloud (Dec. 2, 2020), https://perma.cc/G6RP-74Y5. Google scans your emails and attachments; Apple the photographs on your phone; and Meta your private Facebook messages.[5]

---

[5] *See* Janko Roettgers, *Google Will Keep Reading Your Emails, Just Not for Ads*, Variety (Jun. 23, 2017, 12:43 PM),

Big tech companies aren't just scanning for CSAM, either. Consider two other hash-matching applications: scanning for "terrorist content" and scanning for copyright infringement. Like the CSAM databases at issue in this case, the databases used for those hash-matching applications are shrouded in secrecy. But even from what little we know, those databases, too, may be vastly overinclusive. The Global Internet Forum for Counter Terrorism (GIFCT), for instance—the primary database used by big tech for hash matching terrorist content—has publicly acknowledged false positives in its database, such as a music video that "was not violent, graphic, or explicit." *See* GIFCT, 2022 GIFCT Transparency Report 34-35 (2022), *available at* https://perma.cc/2H42-PJSR. And users have roundly criticized Google Drive's copyright infringement database; at one point, the database categorized all text files containing the number "1" as copyright infringement. *See* Matthew Humphries, *Google Drive Flags Text Files Containing "1" as a Copyright Infringement*, PCMag (Jan. 25, 2022), https://perma.cc/F5X3-L2YT.

And nothing about the opinion below is limited to hash-matching. Keyword search programs flag potential hate speech, *see, e.g.*, Michelle Hampson, *Combating Hate Speech Online With AI*, IEEE Spectrum (Feb. 21, 2023), https://perma.cc/F5X3-

---

https://perma.cc/725S-LK4M; James Outram, *Top 10 Photo Manager Software with Facial Recognition: A Comprehensive Guide*, Daminion (Jan. 27, 2024, 2:46 PM), https://perma.cc/SX2Q-UR89; Sarah Frier, *Facebook Scans the Photos and Links You Send on Messenger*, Bloomberg (Apr. 4, 2018, 11:06 AM), https://perma.cc/5GVJ-XHR5.

L2YT; facial recognition algorithms could be used to scan for fugitives, *see* William Crumpler, *How Accurate are Facial Recognition Systems – and Why Does It Matter?*, Ctr. for Strategic & Int'l Stud. (Apr. 14, 2020), https://perma.cc/4X32-XWP2 (surveying literature); and so on. The opinion below takes the position that if a company's algorithm flags an email, message, image, or video as potentially relevant to law enforcement, police have the right to open it up, even if no human at the company ever did.

2. To make matters worse, the purportedly private actors doing the scanning are intertwined with the government in ways that the private actors in *Jacobsen* and *Walter* were not. Technology companies are required by law to report suspected CSAM and face severe fines for failing to do so. 18 U.S.C. §§ 2258A(a), (e). They are also under intense governmental pressure to proactively monitor for CSAM. *See* Cecilia Kang & David McCabe, *'Your Product Is Killing People': Tech Leaders Denounced Over Child Safety*, N.Y. Times (Jan. 31, 2024), https://perma.cc/WKA7-Y4FF.

Moreover, the tools they use to detect potential CSAM are developed hand in hand with the government. PhotoDNA, for instance, is available for all intents and purposes only to law enforcement and their partners. *PhotoDNA*, Microsoft, https://perma.cc/9N9T-8XVT (last accessed Feb. 14, 2024). It was developed by Microsoft but is now owned by NCMEC. NCMEC was created by federal law to collaborate with federal, state, and local law enforcement to, among other things, operate a tipline for private actors who uncover suspected CSAM on their platforms. *See* 34 U.S.C. § 11293(b). Every court

to squarely consider the question has held NCMEC is a state actor. *See United States v. Ackerman*, 831 F.3d 1292, 1297-1300 (10th Cir. 2016) (Gorsuch, J.); *United States v. Keith*, 980 F. Supp. 2d 33, 41-42 (D. Mass. 2013).

The private search doctrine thus allows the government to use private actors to make an end run around the strictures of the Fourth Amendment. The government could coerce private actors (by statute or using subtler forms of pressure) into scanning for and sharing private emails or files containing disfavored content—COVID misinformation, for instance, or slogans used by political dissidents. *Cf. Missouri v. Biden*, 83 F.4th 350, 359-66 (5th Cir. 2023) (detailing various forms of direct and indirect pressure by government on social media companies to remove content on "divisive topics" such as COVID-19 vaccine side effects and election fraud).

3. To require a warrant before police rummage through private files flagged as potential contraband is not to say that those flags have no role to play in the law enforcement process. In the mine run of cases, such a flag may well be sufficient to obtain a warrant. But that's no small thing: Warrants are "'an important working part of our machinery of government,' not merely 'an inconvenience to be somehow "weighed" against the claims of police efficiency.'" *Riley v. California*, 573 U.S. 373, 401 (2014) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 481 (1971)).

A warrant interposes a neutral magistrate in a process where no other actor has an incentive to value privacy. Technology companies, concerned about public scrutiny and government sanctions, flag anything that remotely resembles CSAM: Of the 32

million reports of suspected CSAM that technology companies sent to NCMEC in 2022, the majority were not "actionable," because, among other reasons, they lack any "apparent child sexual exploitation nexus." *See CyberTipline 2022 Report*, NCMEC, https://perma.cc/XQ5H-B4H6 (last accessed Feb. 14, 2024); *"Protecting Our Children Online": Hearing Before the S. Comm. on the Judiciary*, 118th Cong. 4 (2023) (statement of Michelle DeLaune, President and CEO, NCMEC), *available at* https://perma.cc/C27B-T8HZ. And police officers, engaged in the "often competitive enterprise of ferreting out crime," are not the ideal arbiters to decide when "the right of privacy must reasonably yield" to the needs of law enforcement. *Johnson v. United States*, 333 U.S. 10, 14 (1948).

In cases like this one, the balance between privacy and law enforcement interests is particularly sensitive. The law enforcement interests at play are, of course, weighty. But the privacy interests are, too. If a flag turns out to be mistaken, police officers have opened and viewed a private file—often, an intimate private photograph. *See Miller*, 982 F.3d at 429.

This Court has an "obligat[ion]—as '[s]ubtler and more far-reaching means of invading privacy have become available to the [g]overnment'—to ensure that the 'progress of science' does not erode Fourth Amendment protections." *Carpenter v. United States*, 138 S. Ct. 2206, 2223 (2018) (quoting *Olmstead v. United States*, 277 U.S. 438, 473-74 (1927) (Brandeis, J., dissenting)). It should grant certiorari and resolve the question presented.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be granted.

Respectfully submitted,

Michael Kiel Kaiser
LASSITER & CASSINELLI
1218 W. 6th Street
Little Rock, AR 72201

Easha Anand
Counsel of Record
Jeffrey L. Fisher
STANFORD LAW SCHOOL
SUPREME COURT
LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305
(650) 724-3345
eanand@stanford.edu

February 16, 2024