No. _____

IN THE

SUPREME COURT OF THE UNITED STATES

RICHARD EDWARD BRILLHART,
Petitioner,

v.

UNITED STATES OF AMERICA,
Respondent.

On Petition for a Writ of Certiorari to the
United States Court of Appeals
for the Eleventh Circuit

PETITION FOR A WRIT OF CERTIORARI

ROGER G. AZCONA
Counsel of Record
LAW OFFICE OF ROGER AZCONA
403 N.W. 3rd Street
Okeechobee, Florida 34972
(863) 763-4166
azconalaw@gmail.com

Counsel for Petitioner

QUESTION PRESENTED

Whether the private-search doctrine permits law enforcement, without a warrant, to open and visually inspect a digital file in Petitioner's account when no private party opened or viewed that copy, solely because its hash value matches a different copy previously viewed by a private provider.

PARTIES TO THE PROCEEDING

Petitioner Richard Edward Brillhart was the defendant-appellant below. Respondent United States of America was the plaintiff-appellee below.

RELATED PROCEEDINGS

United States v. Brillhart, No. 2:22-cr-00053-SPC-NPM-1 (M.D. Fla.) (judgment entered Oct. 1, 2024).

United States v. Brillhart, No. 2:03-cr-00121-JES-KCD-1 (M.D. Fla.) (revocation sentence imposed with the sentence in No. 2:22-cr-00053 on Oct. 1, 2024).

United States v. Brillhart, Nos. 24-13226 & 24-13232 (11th Cir.) (judgment entered July 9, 2026; rehearing denied Sept. 1, 2026).

CORPORATE DISCLOSURE STATEMENT

Petitioner is an individual. No corporate disclosure statement is required.

TABLE OF CONTENTS

Question Presented i
Parties to the Proceeding ii
Related Proceedings ii
Corporate Disclosure Statement ii
Table of Authorities iv–v
Petition for a Writ of Certiorari 1
Opinions Below 1
Jurisdiction 1
Constitutional and Statutory Provisions Involved 1
Statement of the Case 1
A. Google's automated hash match and the government's warrantless review 1
B. Proceedings below 3
Reasons for Granting the Petition 5
I. The decision below deepens an acknowledged three-to-three circuit conflict 6
A. The Fifth, Sixth, and Eleventh Circuits permit warrantless viewing after a hash match 6
B. The Second, Fourth, and Ninth Circuits require an actual private viewing of the defendant's file 7
C. The conflict is square and mature 8
II. The decision below conflicts with Walter and Jacobsen 9
A. No private actor frustrated Brillhart's privacy in his copy 9
B. Matching content does not establish a prior search of the same file 12
C. Visual review reveals materially more than a binary match 13
III. The question is exceptionally important and recurring 14
IV. This federal case is an appropriate vehicle for the Fourth Amendment question 16
Conclusion 19

TABLE OF AUTHORITIES

CASES

Carpenter v. United States, 585 U.S. 296 (2018) 15
Chatrie v. United States, No. 25-112 (June 29, 2026) 18
Gasper v. Wisconsin, No. 25-1191 (cert. denied Oct. 5, 2026), and Brief in Opposition (filed June 1, 2026) 16–17
Hamilton-Brown Shoe Co. v. Wolf Bros. & Co., 240 U.S. 251 (1916) 17
Murray v. United States, 487 U.S. 533 (1988) 17–18
Rakas v. Illinois, 439 U.S. 128 (1978) 11
Riley v. California, 573 U.S. 373 (2014) 15
United States v. Braun, No. 25-2740 (7th Cir. Aug. 20, 2026) 18
United States v. Brillhart, Nos. 24-13226 & 24-13232 (11th Cir. July 9, 2026) 1
United States v. Jacobsen, 466 U.S. 109 (1984) 4–6, 9–13
United States v. Lowers, 170 F.4th 134 (4th Cir. 2026) 4, 8–9
United States v. Maher, 120 F.4th 297 (2d Cir. 2024) 4, 7–9
United States v. Miller, 982 F.3d 412 (6th Cir. 2020) 4, 6, 9
United States v. Reddick, 900 F.3d 636 (5th Cir. 2018) 4, 6, 9
United States v. Sparks, 806 F.3d 1323 (11th Cir. 2015), overruled on other grounds by United States v. Ross, 963 F.3d 1056 (11th Cir. 2020) (en banc) 14
United States v. Wilson, 13 F.4th 961 (9th Cir. 2021) 4, 7–9, 13
Walter v. United States, 447 U.S. 649 (1980) 5, 9–10, 12–13
Williamson v. United States, No. 26-5743, Petition for a Writ of Certiorari (filed Sept. 28, 2026) 16

CONSTITUTIONAL PROVISION

U.S. Const. amend. IV 1, 5, 8, 11–12

STATUTES

18 U.S.C. § 2252 3
18 U.S.C. § 2258A 15
18 U.S.C. § 3231 1
28 U.S.C. § 1254(1) 1, 17
28 U.S.C. § 1257(a) 1, 17
28 U.S.C. § 1291 1

RULES

Supreme Court Rules 13.1 and 13.3 1

PETITION FOR A WRIT OF CERTIORARI

Richard Edward Brillhart respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Eleventh Circuit.

OPINIONS BELOW

The published opinion of the court of appeals is United States v. Brillhart, Nos. 24-13226 & 24-13232 (11th Cir. July 9, 2026), and is reproduced at Pet. App. 1a–37a. The unpublished order denying panel rehearing and rehearing en banc is reproduced at Pet. App. 38a–39a. The district court's opinion denying suppression is reported at 2023 WL 3304278 and is reproduced at Pet. App. 40a–61a.

JURISDICTION

The district court had jurisdiction under 18 U.S.C. § 3231. The court of appeals had jurisdiction under 28 U.S.C. § 1291. The court of appeals entered judgment on July 9, 2026, and denied a timely petition for panel rehearing and rehearing en banc on September 1, 2026. This petition is timely under Rules 13.1 and 13.3 of this Court. This Court has jurisdiction under 28 U.S.C. § 1254(1).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The Fourth Amendment to the United States Constitution is reproduced at Pet. App. 62a. The pertinent jurisdictional provisions of 28 U.S.C. §§ 1254(1) and 1257(a) are reproduced at Pet. App. 63a.

STATEMENT OF THE CASE

A. Google's automated hash match and the government's warrantless review

This case arises from one digital file that no private person opened or viewed in Brillhart's account before the government did. Google maintains a repository of

hash values and classifications derived from files its human reviewers previously determined to depict child sexual abuse material. The original review involved an image in another user's file. Google's later process compared a mathematically generated identifier for Brillhart's copy against that repository and relied on the earlier classification to report the matched copy, without a contemporaneous human viewing. The original human review and the later automated comparison were separate events involving separate copies. Pet. App. 4a–7a, 17a–20a.

Google identified four files associated with Brillhart's accounts. Three received contemporaneous private visual review. The remaining file was one of two attachments to CyberTip 90034851 (Exhibit 3A). Google's witness explained that one attachment was reviewed contemporaneously, while the other was reported through a match to a previously reviewed repository image. Pet. App. 6a–7a, 64a–67a (Suppression Hr'g Tr. 105–107, 124, Dkt. No. 192). The report confirms that distinction. Dkt. No. 70-8, at 8–9. Even assuming the match was accurate, Brillhart challenges the government's first visual inspection of his reported copy.

Officer Katrina Lee, formerly known as O'Brien, recognized that Google had not contemporaneously viewed the second attachment in Exhibit 3A. NCMEC had viewed neither attachment. Dkt. No. 70-8, at 15. Lee nevertheless opened both: she relied on the private viewing of one and the hash match for the other. Pet. App. 68a–72a (Suppression Hr'g Tr. 169–173). She supplied visual descriptions to Special Agent Soleil Randall and confirmed that descriptions were incorporated into multiple warrant affidavits. Pet. App. 73a–75a (Suppression Hr'g Tr. 179–181).

The September 1, 2021 applications for Google accounts, Brillhart's residence, and his vehicle incorporated descriptions of both attachments to CyberTip

90034851. Dkt. Nos. 70-12, at 11–12, ¶¶20–21; 70-13 and 70-14, at 22–24, ¶¶35–36. The Yahoo affidavit recited Yahoo reports and identifying evidence, without the challenged Google-file description. Dkt. No. 70-11, ¶¶21–61. The affidavits also contained other reported material and identifying evidence. The ensuing searches yielded evidence introduced at trial. Pet. App. 7a–8a. A grand jury charged distribution and possession under 18 U.S.C. § 2252. Pet. App. 8a. The challenged viewing's consequences for particular warrants and trial evidence remain distinct from the constitutional question decided below.

The issue is the governmental act that followed Google's automated comparison and report: opening and visually inspecting Brillhart's copy without a warrant even though no private actor had opened or viewed that copy. Even assuming the match accurately identified identical visual content, knowledge about an earlier copy does not answer whether Google's later process exposed the contents of Brillhart's own file. The constitutional argument therefore does not require this Court to decide the technical reliability of the match.

B. Proceedings below

Brillhart moved to suppress the evidence derived from the warrantless governmental review. The district court denied the motion on three grounds. First, it held that Brillhart lacked a reasonable expectation of privacy because he had used providers whose terms prohibited illegal content and warned of scanning and reporting. Second, it held that the private-search doctrine authorized law enforcement to view the files. Third, it held that the good-faith exception independently foreclosed suppression. Pet. App. 40a–61a.

A jury convicted Brillhart of distribution and possession. The district court entered judgment on October 1, 2024, imposing concurrent prison terms of 480 months and 240 months. Pet. App. 10a–11a. The court of appeals affirmed the convictions, vacated the sentences, remanded for resentencing, and dismissed the related revocation appeal as moot. Pet. App. 37a.

The Eleventh Circuit affirmed the convictions in a published opinion. It described the expectation-of-privacy question as 'close' but declined to decide it. Pet. App. 13a. It likewise declined to address good faith. Ibid. The court instead rested its suppression ruling solely on the private-search doctrine.

The court began with the settled rule that a government search following a private search is permissible only if it does not exceed the scope of the private search. Pet. App. 14a (citing United States v. Jacobsen, 466 U.S. 109, 115 (1984)). It recognized that Google's process was different from the traditional private-search cases: no human reviewed Brillhart's copy, and Google's conclusion arose from comparing its hash to a repository entry created after a person reviewed a different copy. Pet. App. 16a–19a.

The court then expressly acknowledged that the circuits are divided. The Fifth and Sixth Circuits hold that a hash match supplies the virtual certainty necessary to permit a subsequent warrantless police viewing. United States v. Reddick, 900 F.3d 636 (5th Cir. 2018); United States v. Miller, 982 F.3d 412 (6th Cir. 2020). The Second, Fourth, and Ninth Circuits hold that it does not. United States v. Maher, 120 F.4th 297 (2d Cir. 2024); United States v. Lowers, 170 F.4th 134 (4th Cir. 2026); United States v. Wilson, 13 F.4th 961 (9th Cir. 2021). Pet. App. 17a–18a.

The Eleventh Circuit joined the Fifth and Sixth. It reasoned that a hash match makes it virtually certain that a government inspection will find the same visual content a private reviewer saw in the earlier copy. Pet. App. 18a–21a. It rejected the analogy between a hash and the descriptive labels in Walter v. United States, 447 U.S. 649 (1980), reasoning that a hash is produced from the file's underlying binary data and, in that sense, 'is the content.' Pet. App. 22a–24a. And it rejected the opposing circuits' reliance on the personal nature of Fourth Amendment rights, reasoning that an earlier review of an identical copy 'dissipate[s]' a suspect's privacy interest in his own copy. Pet. App. 26a–27a.

Brillhart timely sought panel rehearing and rehearing en banc. The court denied both on September 1, 2026. Pet. App. 38a–39a.

REASONS FOR GRANTING THE PETITION

The Court should grant review because the decision below deepens a square and acknowledged conflict over an important question of federal constitutional law. Three circuits permit police to open a person's private digital file without a warrant when an algorithm reports that its hash matches a previously reviewed copy. Three circuits hold that the government may not do so unless a private actor first opened the defendant's own file. The same federal search has opposite constitutional consequences depending only on geography.

The Eleventh Circuit's rule also conflicts with Walter and Jacobsen. Those cases ask what the private party actually exposed before the government acted. Here, no private party exposed any visual content from Brillhart's copy. A hash match may establish that two copies are identical, but it cannot transform a search of one person's effect into a search of another person's effect. And opening the file revealed

its complete visual content, not merely the binary fact that its hash matched a database entry.

The question recurs when providers use automated matching to report digital material and officers subsequently inspect the reported files. The published decision below identifies the constitutional conflict and chooses a side. The unresolved privacy and remedial issues should be distinguished from the legal rule the panel expressly decided.

I. THE DECISION BELOW DEEPENS AN ACKNOWLEDGED THREE-TO-THREE CIRCUIT CONFLICT

A. The Fifth, Sixth, and Eleventh Circuits permit warrantless viewing after a hash match.

Reddick held that Microsoft's PhotoDNA matching process supplied virtual certainty permitting government viewing. 900 F.3d at 637–640. Its technology should not be assumed identical in every respect to the matching process here. The Fifth Circuit analogized the inspection to Jacobsen's contraband-identification test; Miller rejected that particular analogy while reaching the same constitutional result.

Miller permitted government viewing of files Google had identified through hash matching, emphasizing reliability established on that record. 982 F.3d at 415–416, 429–431. It expressly distinguished visual inspection from a binary chemical test. Id. at 429. Its rationale instead treated reliable knowledge of previously reviewed content as sufficient virtual certainty to permit inspection of the defendant's matched copies.

The decision below expressly 'agree[d] with the Fifth and Sixth Circuits.' Pet. App. 18a. It held that Google's automated process 'qualifies as a valid private search' because it spared a later employee from repeating what an earlier reviewer

had done to an identical copy. Ibid. In the court's view, the 'controlling question' was whether law enforcement was virtually certain it would find nothing materially different when it opened Brillhart's copy. Pet. App. 19a. Relying on its assessment of hash reliability, the court held that standard satisfied. Pet. App. 19a–21a.

Those three circuits thus treat the private-search doctrine as an information-certainty rule. If an automated identifier makes the content of a private digital file sufficiently predictable, the government may open the file without a warrant even though no private person has opened that copy.

B. The Second, Fourth, and Ninth Circuits require an actual private viewing of the defendant's file.

Three other circuits reject that approach. In Wilson, Google's automated system identified email attachments through hash matching, but no Google employee viewed the defendant's attachments. 13 F.4th at 965–966. The Ninth Circuit held that the government exceeded the private search when it opened them. Id. at 971–979. Hash information could provide probable cause, the court explained, but it did not reveal the attachments' contents and did not itself frustrate the defendant's privacy in those unopened files. Id. at 973–978. The court vacated the conviction and reversed the suppression ruling; the government had waived any alternative basis for avoiding exclusion. United States v. Wilson, No. 18-50440, slip op. at 38–39 & n.14 (9th Cir. Sept. 21, 2021).

The Second Circuit followed Wilson in Maher. Google's system matched a file in Maher's account to a previously reviewed file, but no private actor visually examined Maher's copy. 120 F.4th at 302–304. The court held that a hash match could support probable cause but did not authorize warrantless visual inspection

under the private-search doctrine. United States v. Maher, No. 23-6181, slip op. at 39–40 (2d Cir. Oct. 30, 2024). It emphasized that the earlier viewing of a file in another account could not frustrate Maher's personal expectation of privacy in his own unopened file. 120 F.4th at 317–319. The court ultimately affirmed on good-faith grounds. Id. at 320–323.

Most recently, the Fourth Circuit adopted the same rule in Lowers. It held that an automated hash match did not itself expose the contents of a file and that law enforcement performed a new search when it opened the defendant's copy. 170 F.4th at 149–156. The court stressed that Fourth Amendment rights are personal: if the defendant could not challenge the government's search of somebody else's copy, then a private search of somebody else's copy could not extinguish his rights in his own. Id. at 153–154. The court affirmed on attenuation grounds, not because the governmental viewing was lawful. United States v. Lowers, No. 24-4546, slip op. at 41–46 (4th Cir. Mar. 10, 2026).

These circuits treat the doctrine as an exposure rule faithful to its rationale: a government agent may repeat what a private actor actually did to the defendant's property, but may not replace the missing private search with an inference—however accurate—about what a new search will reveal. The split concerns whether the governmental viewing violates the Fourth Amendment. Whether that violation requires exclusion remains a separate inquiry, as the differing dispositions in Wilson, Maher, and Lowers demonstrate.

C. The conflict is square and mature.

The decision below catalogued both sides of the conflict and chose one. Pet. App. 17a–18a. Each line of cases involves an automated hash match, no

contemporaneous human review of the defendant's copy, and a later warrantless governmental viewing. The Eleventh Circuit distinguished Lowers's lack of record evidence establishing hash reliability. Pet. App. 20a n.5. But Lowers also relied independently on the personal nature of Fourth Amendment rights and the additional information revealed by visual inspection. 170 F.4th at 153–156. Maher and Wilson likewise reject reliance on a prior viewing of another person's copy. The conflict therefore persists even assuming the match here was accurate.

The division is now even and entrenched. Reddick and Miller supplied one rule. Wilson and Maher supplied the opposite rule. Lowers addressed the disagreement at length, and the published decision below responded point by point before joining Reddick and Miller. Further percolation is unlikely to dissolve a conflict that turns on competing understandings of this Court's precedents.

The conflict also changes day-to-day police procedure. In the Fifth, Sixth, and Eleventh Circuits, a hash report allows an officer to open the reported file before applying for a warrant. In the Second, Fourth, and Ninth Circuits, the report may establish probable cause, but, absent another applicable exception, the officer must obtain a warrant before visually inspecting the file. Only this Court can supply a uniform national rule.

II. THE DECISION BELOW CONFLICTS WITH WALTER AND JACOBSEN

A. No private actor frustrated Brillhart's privacy in his copy.

The private-search doctrine rests on a straightforward premise. The Fourth Amendment does not regulate a search by a private person acting independently of government. Jacobsen, 466 U.S. at 113. Once that private person has exposed particular information belonging to the defendant, a government agent does not

perform a new Fourth Amendment search merely by repeating the same examination and learning nothing more. Id. at 115–120. The permissible government search is therefore measured by the private search that actually occurred.

Walter illustrates the limit. Private employees opened a misdelivered package and saw suggestive drawings and explicit descriptions on film boxes, but did not project the films. 447 U.S. at 651–652. Federal agents later projected them without a warrant. The Court reversed. Justice Stevens's plurality opinion concluded that the projection exceeded the private examination; Justice White, joined by Justice Brennan, agreed that the warrantless projection infringed the petitioners' Fourth Amendment interests, and Justice Marshall concurred in the judgment. Id. at 654–657 (plurality opinion); id. at 660–662 (White, J., concurring in part and in the judgment); id. at 660 (Marshall, J., concurring in the judgment). Strong evidence about what the films would show did not authorize the government to look.

Jacobsen involved the opposite sequence. Federal Express employees opened the defendant's damaged package, cut open a tube inside, removed plastic bags, and exposed white powder before summoning federal agents. 466 U.S. at 111. The agents then reopened the same package and examined the same exposed material. Id. at 111–112. Because the private search had already frustrated the defendant's privacy in that package and the government's inspection revealed nothing more, the Court found no additional invasion. Id. at 119–121.

Jacobsen expressly distinguished receiving a private report of contraband in a container from lawful reinspection after private parties had compromised that container's integrity. 466 U.S. at 120 n.17. Information sufficient for probable cause

does not itself authorize opening a container that still supports a reasonable expectation of privacy. The issue here is whether hash-based processing, without private visual inspection of Brillhart's copy, supplies the necessary prior exposure.

Here, the original private reviewer viewed an image in another user's file and supplied the basis for a repository hash and classification. Google's later process compared Brillhart's file against that stored information; it did not repeat the original visual review on his copy. Officer Lee then performed the first visual inspection of Brillhart's reported copy. Unlike the agents in Jacobsen, she was not reopening the same container whose contents private employees had already exposed. Pet. App. 4a–7a, 16a–19a.

The contrary rule loses sight of the personal nature of Fourth Amendment rights. See Rakas v. Illinois, 439 U.S. 128, 133–134 (1978). A person ordinarily cannot object to a search of someone else's property because that search did not invade his own protected privacy. The necessary corollary is that a private search of someone else's property does not eliminate his privacy in his own. Identical contents do not merge two separately possessed effects into one constitutional object. The physical analogue is a private search of one sealed container followed by a governmental search of a different, still-sealed container believed to contain an identical item. Certainty about the second container's contents would not make it the container already searched. The same distinction applies to copies stored in different users' accounts: repetition of content is not repetition of a search of the same effect.

B. Matching content does not establish a prior search of the same file.

Assume that the hash match accurately established identical data. That assumption would explain what Officer Lee expected to see; it would not establish that a private person had already opened Brillhart's file. The copies were associated with different users' accounts. Content identity does not make those distinct copies the same effect for purposes of measuring the scope of an antecedent private search. Pet. App. 7a, 26a–27a.

The Eleventh Circuit reasoned that a hash is not merely a label because it is mathematically produced from the file's underlying data. Pet. App. 22a–24a. That premise does not collapse two different acts: the original human viewing of an image, which produced the repository classification, and the later automated reliance on the stored hash and classification. Brillhart does not contend that the original reviewer saw only a label. He contends that no private reviewer saw his copy. The later comparison supplied information about that copy without displaying its visual contents to a private reviewer.

Walter shows why confidence is not exposure. The labels there described the films in explicit terms. 447 U.S. at 652. Even if those descriptions made the unlawful character of the films virtually certain, the agents still needed a warrant to project them because no private party had done so. Id. at 654–657. Greater accuracy may strengthen probable cause. It does not expand the scope of an antecedent private search.

Nor does Jacobsen's 'virtual certainty' language establish a free-standing certainty exception to the warrant requirement. The Court used that language after private employees had already opened the defendant's own package and exposed the

innermost bag. 466 U.S. at 118–120. Virtual certainty helped establish that the agents' handling of the same package would reveal nothing beyond the completed private search. It did not substitute for a private search that never happened.

The decision below reverses that order of operations. Under its rule, sufficiently reliable information about private material allows the government to expose the material without a warrant. The Fourth Amendment ordinarily works the other way: reliable information supplies probable cause, and probable cause supplies the basis to seek a warrant from a neutral magistrate.

C. Visual review reveals materially more than a binary match.

The government search also exceeded Google's automated process in depth. The hash match answered one binary question: whether Brillhart's file had the same hash as a repository entry classified as child pornography. Officer Lee's visual review exposed every detail of the image. As Walter recognizes, viewing expressive material discloses information qualitatively different from reading even a detailed external description. 447 U.S. at 654–657.

Jacobsen's treatment of the field test confirms the distinction. After the private employees and agents had exposed the powder, the agents chemically tested a trace amount. The Court held that the test was not a search because it could disclose only whether the substance was cocaine—'nothing of special interest' beyond contraband status. 466 U.S. at 122–123. Opening a digital image is not comparably binary. It reveals private visual facts about the people, acts, context, and composition depicted. Wilson, 13 F.4th at 976–978.

The Eleventh Circuit's breadth-versus-depth distinction does not save the search. Pet. App. 24a–26a. The relevant breadth question is whether the private

search extended to Brillhart's copy at all. It did not. And the depth of the government's examination matters because the government transformed a nonvisual mathematical match into a complete visual inspection.

The court of appeals relied on its decision in Sparks, but that precedent points the other way. Sparks permitted an agent to rewatch a video that a private party had watched and prohibited the agent from watching a separate video that the private party had not. 806 F.3d at 1335–1336, overruled on other grounds by United States v. Ross, 963 F.3d 1056 (11th Cir. 2020) (en banc). Brillhart's copy, stored in his account and never opened by a private person, is the digital analogue of the separate, unviewed video.

Requiring a warrant would not force officers to 'avert their eyes' from information already revealed. Google may transmit the report, hash, classification, subscriber information, and file. Officers may use that evidence to establish probable cause. Absent another applicable exception, the warrant requirement prevents the government from opening the file until a neutral judicial officer authorizes the search.

III. THE QUESTION IS EXCEPTIONALLY IMPORTANT AND RECURRING

Automated scanning is now an ordinary feature of cloud storage, email, messaging, and other digital services. Providers may compare enormous volumes of private data against databases of known material without a person reviewing each matched file. The constitutional line between a provider's automated process and the government's later inspection therefore affects a vast and growing category of searches.

Congress requires providers that obtain actual knowledge of facts or circumstances evidencing specified apparent violations involving child sexual abuse material to report them to NCMEC. 18 U.S.C. § 2258A(a). It does not require providers to monitor users or affirmatively search, screen, or scan communications. Id. § 2258A(f). The reporting framework does not itself authorize a warrantless governmental visual inspection. A clear constitutional rule would allow providers to meet their obligations and officers to investigate serious crimes while preserving the neutral-warrant safeguard.

The issue is not confined to child-pornography investigations. The doctrine announced below turns on automated identification, not the substantive offense. Providers can use hashes or other digital signatures to flag copyrighted works, malware, extremist material, stolen data, or any category added to a private database. If certainty about a match substitutes for a prior private exposure, the exception will expand with the reach of automated classification.

Digital storage also magnifies the privacy interests at stake. Modern accounts can hold years of communications and expressive material. This Court has repeatedly cautioned against mechanical application of physical-world doctrines when new technology enables access to qualitatively different stores of private information. See Riley v. California, 573 U.S. 373, 393–397 (2014); Carpenter v. United States, 585 U.S. 296, 310–313 (2018). The same caution is warranted before converting a limited doctrine that permits repetition of an actual private search into authority for a first governmental viewing.

The answer need not impede urgent investigations. A hash match, provider classification, account information, and statutory report may together establish

probable cause. Officers can preserve the file while seeking a warrant, and exigent circumstances remain available when their requirements are satisfied. The disagreement concerns who decides whether the government may open the file—the investigating officer or a neutral magistrate.

The question has also reached state courts. The Court denied certiorari in Gasper v. Wisconsin, No. 25-1191, on October 5, 2026. That disposition leaves the acknowledged circuit conflict unresolved. This petition presents the issue through a published federal appellate decision that expressly surveys the conflict and adopts one side. Another petition presents the overlapping private-search question alongside government-action and warrant/good-faith questions. Petition for a Writ of Certiorari at ii, Williamson v. United States, No. 26-5743 (filed Sept. 28, 2026). Brillhart presents the private-search question alone, through a published decision expressly addressing the split.

IV. THIS FEDERAL CASE IS AN APPROPRIATE VEHICLE FOR THE FOURTH AMENDMENT QUESTION

The constitutional question was developed at an evidentiary hearing and expressly resolved in the published decision below. The testimony distinguishes the contemporaneously reviewed attachment from the hash-only attachment and confirms Lee's subsequent inspection. Pet. App. 64a–72a. Even assuming an accurate match, the remaining legal dispute is whether prior review of a distinct copy associated with another user's account supplies the private exposure necessary to permit visual inspection of Brillhart's reported copy.

The panel assumed a protected privacy interest and expressly chose a side of the private-search conflict. Pet. App. 13a–27a. It did not decide reasonable

expectation of privacy or good faith. Those alternative grounds may be considered on remand; this petition seeks review of the private-search holding rather than a ruling on those unresolved questions.

The court of appeals affirmed Brillhart's convictions but vacated his sentences and remanded for resentencing. Pet. App. 37a. That posture does not defeat jurisdiction: Section 1254(1) authorizes certiorari "before or after rendition of judgment or decree." 28 U.S.C. § 1254(1). Unlike the state-court final-judgment requirement in 28 U.S.C. § 1257(a), invoked by Wisconsin in opposing review in Gasper, this statute permits review of the federal appellate judgment here. See Brief in Opposition at 9–15, Gasper, No. 25-1191 (filed June 1, 2026). The denial in Gasper did not identify a reason, and Brillhart does not attribute it to that objection. Although this Court ordinarily awaits final judgment, see Hamilton-Brown Shoe Co. v. Wolf Bros. & Co., 240 U.S. 251, 258 (1916), the practice is prudential. The question presented concerns the affirmed convictions and will not be revisited during resentencing. The acknowledged conflict supplies a compelling reason to review it now.

The challenged file's description entered the Google, residence, and vehicle applications. Dkt. No. 70-12, ¶21(b); Dkt. Nos. 70-13 and 70-14, ¶36(b). The Yahoo affidavit did not include that description. Dkt. No. 70-11, ¶¶21–61. Those facts do not alone establish which trial evidence resulted from the challenged viewing. Any claim of derivative suppression requires tracing that viewing through the relevant warrant and seizure to the evidence introduced at trial. Under Murray v. United States, 487 U.S. 533, 542–543 (1988), an independent source requires that the unlawful search neither prompt the decision to seek the warrant nor supply

information affecting its issuance. Whether untainted information supported each warrant and whether officers would have sought it without the challenged viewing remain questions for remand. The omission from the Yahoo affidavit does not, by itself, resolve the latter inquiry. United States v. Braun, No. 25-2740, slip op. at 9–17 (7th Cir. Aug. 20, 2026), illustrates these issues: the majority reversed suppression based on untainted probable cause and an independent decision to seek the warrant, without deciding the constitutional question. The concurrence adds no circuit holding. Brillhart seeks the correct constitutional rule and remand to resolve the remaining suppression issues, not automatic exclusion or reversal of his convictions.

Chatrie v. United States, No. 25-112, slip op. at 10 n.4 (June 29, 2026), confirms that unresolved exclusionary-rule issues need not prevent review of the constitutional question. There, this Court decided that a Fourth Amendment search occurred while leaving good faith for reconsideration below. It rejected the contention that its decision was advisory because the lower court could still provide relief. Brillhart likewise seeks resolution of the constitutional holding, leaving remaining suppression grounds to the lower courts. Chatrie does not resolve those grounds here; it supports that sequence of review.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted,

ROGER G. AZCONA
Counsel of Record
LAW OFFICE OF ROGER AZCONA
403 N.W. 3rd Street
Okeechobee, Florida 34972
(863) 763-4166
azconalaw@gmail.com

Counsel for Petitioner

November 3, 2026