No. 18-6734

IN THE SUPREME COURT OF THE UNITED STATES

HENRY FRANKLIN REDDICK, PETITIONER

v.

UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

BRIEF FOR THE UNITED STATES IN OPPOSITION

NOEL J. FRANCISCO
Solicitor General
Counsel of Record

BRIAN A. BENCZKOWSKI
Assistant Attorney General

SONJA M. RALSTON
JOHN P. TADDEI
Attorneys

Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

QUESTION PRESENTED

Whether a police officer violated petitioner's Fourth Amendment rights, and triggered application of the exclusionary rule, when he opened and viewed digital child-pornography files that petitioner had uploaded to a file-hosting service, where the private file-hosting company had already scanned the files, determined that they were images previously identified as child pornography, and sent them to the National Center for Missing and Exploited Children, which in turn sent the files to the police officer.

IN THE SUPREME COURT OF THE UNITED STATES

No. 18-6734

HENRY FRANKLIN REDDICK, PETITIONER

v.

UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

BRIEF FOR THE UNITED STATES IN OPPOSITION

OPINIONS BELOW

The opinion of the court of appeals (Pet. App. A1-A5) is reported at 900 F.3d 636. The order of the district court (Pet. App. B1-B6) is not published in the Federal Supplement but is available at 2017 WL 1353803.

JURISDICTION

The judgment of the court of appeals was entered on August 17, 2018. The petition for a writ of certiorari was filed on November 14, 2018. The jurisdiction of this Court is invoked under 28 U.S.C. 1254(1).

STATEMENT

Following a guilty plea in the United States District Court for the Southern District of Texas, petitioner was convicted of possession of child pornography, in violation of 18 U.S.C. 2252A(a)(5)(B) and (b)(2). Judgment 1. He was sentenced to 36 months of imprisonment, to be followed by ten years of supervised release. Judgment 2-3. The court of appeals affirmed. Pet. App. A4.

1. Petitioner uploaded digital child-pornography files to Microsoft SkyDrive, a cloud file-hosting service. Pet. App. A3. Microsoft automatically scanned the files and generated a "hash value" for each of them. Id. at A2-A3. "[A] hash value is a string of characters obtained by processing the contents of a given computer file and assigning a sequence of numbers and letters that correspond to the file's contents." Id. at A2. "The hash value has been described as an electronic equivalent of a fingerprint in that two iterations of the same image will, to an over 99% level of accuracy, produce the same hash value." Id. at B1 (footnote omitted). "Conversely, the chance[] of two different images generating the same hash value is nearly non-existent." Ibid. Hash values "are regularly used to compare the contents of two files against each other." Id. at A2.

In this case, Microsoft compared the hash values of petitioner's uploaded files against a National Center for Missing and Exploited Children (NCMEC) database of "known child

pornography hash values." Pet. App. A4; see id. at B1. Each hash value in the NCMEC database corresponds to a file that someone has opened, viewed, and determined to be child pornography. D. Ct. Doc. 87, at 57 (Dec. 12, 2017) (Tr.). "[L]aw enforcement regularly relies on a hash value match with the NCMEC database results to successfully identify images that are, indeed, images of child pornography." Pet. App. B2. In addition, in a voluntary effort to fight the online distribution of child pornography, many internet-service providers compare the hash values of their users' files with the hash values in the NCMEC database. Ibid. Upon detecting a match between the hash value of a user-uploaded file and a hash value in the NCMEC database, an internet-service provider will send a "CyberTip" containing the file, along with the uploader's IP address information, to NCMEC. Id. at A3; see 18 U.S.C. 2258A(2) (requiring report of any "apparent violation" of federal child-pornography law).

Here, Microsoft determined that some of petitioner's uploaded files had hash values that matched hash values in the NCMEC database. Pet. App. A2-A3, B2. Without opening or viewing the files, Microsoft created three CyberTips containing the matched files and petitioner's subscriber information and sent the CyberTips to NCMEC. Id. at A3, B2. Also without opening or viewing the files, NCMEC confirmed the hash-value matches and forwarded the CyberTips to the Corpus Christi Police Department. Ibid. The CyberTips listed some of the names of the matched files,

which included "sucking mandick.jpg," "very yb and dad.jpg," "boy sucking boydick.jpg," "boydick and mancock.jpg," and "boy.kiddy.pedo.[](gay preteen kidsex) 9.06.mpg." Id. at B5 n.5; Gov't C.A. Br. 7.

Upon receiving the CyperTips, Police Detective Michael Ilse opened each matched file and confirmed that it was child pornography. Pet. App. A3, B2. Detective Ilse subsequently applied for a warrant to search petitioner's home, including several digital devices. Ibid. In his affidavit in support of the warrant application, Detective Ilse described the CyberTips and the hash-value matches, listed some of the names of the matched files, recounted his opening of the matched files, and explained why the files appeared to be images of child pornography. Id. at B2. A state judge issued the requested warrant. Ibid.

When law-enforcement officers arrived at petitioner's home to execute the warrant, they informed petitioner that they were searching for evidence of child-pornography possession. Tr. 28. After denying that he possessed child pornography, petitioner told the officers that the search "must be related to a letter he received from Microsoft stating that he had violated the terms of service" and informing him that Microsoft had "blocked him" from its system. Tr. 28-29. The ensuing search of petitioner's home yielded hundreds of still images of child pornography and more than a dozen child-pornography videos. Pet. App. B2. Some of the images depicted prepubescent children performing oral sex on adult

men, and at least one image depicted a prepubescent child in bondage. Presentence Investigation Report (PSR) ¶¶ 10-11.

2. A federal grand jury in the Southern District of Texas returned an indictment charging petitioner with four counts of possession of child pornography, in violation of 18 U.S.C. 2252A(a)(5)(B), based on petitioner's possession of certain child-pornography images that agents found on digital devices in petitioner's home. Indictment 2-4; D. Ct. Doc. 51, at 2 n.1 (Apr. 28, 2017); PSR ¶¶ 1, 9-10. Thereafter, petitioner moved to suppress the child-pornography files that Microsoft had forwarded to NCMEC and the evidence discovered during the search of his home. Pet. App. B1. As relevant here, petitioner argued that, by opening and viewing the matched files, Detective Ilse exceeded the scope of Microsoft's prior search and thus violated petitioner's Fourth Amendment rights.[1] D. Ct. Doc. 34, at 3 (Feb. 7, 2017). Petitioner also contended that the NCMEC database "may contain images that are not actually child pornography" because "[t]he element of human judgment in selecting which images qualify as illegal necessarily implies the possibility of error." D. Ct. Doc. 40, at 2 n.1 (Mar. 8, 2017). Petitioner did not argue that he had a property interest in the matched files, or assert that United States v. Jacobsen, 466 U.S. 109 (1984), could not support the constitutionality of

[1] Although petitioner initially asserted that NCMEC is a "government agent[]" that also violated his Fourth Amendment rights, D. Ct. Doc. 34, at 3 (Feb. 7, 2017), petitioner abandoned that argument as "moot" after learning that NCMEC neither opened nor viewed the matched files. D. Ct. Doc. 40, at 4 (Mar. 8, 2017).

Detective Ilse's actions on the theory that United States v. Jones, 565 U.S. 400 (2012), had overruled it. See D. Ct. Doc. 34, at 3-5; D. Ct. Doc. 40, at 4-6; D. Ct. Doc. 42, at 2-3 (Mar. 17, 2017); Tr. 58-60, 66-67.

The district court convened a suppression hearing at which Detective Ilse and a computer-forensics specialist testified. Tr. 7-57. During his testimony, Detective Ilse stated that he opened and viewed petitioner's matched files to verify that they were child pornography, which is his practice in child-pornography investigations. Tr. 36. Detective Ilse testified that he does not apply for a warrant to search a suspect's "personal effects and house" based solely on hash-value matches. Tr. 36-37. Detective Ilse further stated that the law-enforcement officers he knows who investigate child-pornography offenses will look at each image "to verify that what they're investigating is child pornography." Tr. 46; see Tr. 45-46. In addition, the computer-forensic specialist testified that NCMEC populates its database with the hash values of files depicting "known children" after "somebody has looked at the files and made a judgment that these are child pornography." Tr. 57.

Following the hearing, the district court denied petitioner's suppression motion. Pet. App. B1-B6. The court found "no evidence" to support petitioner's contention that the NCMEC database might contain hash values for adult pornography or other non-child-pornography files. Id. at B2. The court further found

that the record "reflects the near certainty" that the matched files "were each single images that qualified as child pornography: contraband and nothing more." Id. at B5. The court also reasoned that "the NCMEC match and file names, without viewing the images, might establish sufficient probable cause to support the validity of the warrant" to search petitioner's house. Ibid. And it determined that, regardless, even if it "assume[d] without deciding" that Detective Ilse's viewing of the matched files violated the Fourth Amendment, suppression was unwarranted because the good-faith exception to the exclusionary rule applied. Id. at B4-B5.

After the district court denied his motion to suppress, petitioner pleaded guilty to one of the child-pornography possession counts, reserving the right to appeal the denial of his suppression motion. Pet. App. A3; see D. Ct. Doc. 48, at 1 (Apr. 28, 2017). The district court sentenced petitioner to 36 months of imprisonment, to be followed by ten years of supervised release. Judgment 2-3.

3. The court of appeals affirmed. Pet. App. A1-A5.

a. In his opening appellate brief, petitioner principally contended that the district court erred in applying the good-faith exception. Pet. C.A. Br. 2, 10-41. Petitioner also briefly argued that Detective Ilse violated his Fourth Amendment rights by opening and viewing the matched files. Id. at 14-15. In making that argument, petitioner relied in part on Jacobsen, supra, explaining

that Jacobsen recognizes that "when a private individual conducts a search of something that is private to another individual, a subsequent search by a government agent violates the Fourth Amendment when it exceeds the scope of the private individual's search." Pet. C.A. Br. 14. Petitioner did not argue that this Court's decision in Jones, supra, had abrogated Jacobsen, nor did he claim a property interest in the matched files. See Pet. C.A. Br. at 3-41. Petitioner also did not renew his contention that the NCMEC database might contain hash values for files that were not child pornography, and he did not challenge the district court's finding that "no evidence" supported that claim. Pet. App. B2; see Pet. C.A. Br. 3-41.

Petitioner instead took issue with the provenance of the images in the NCMEC database only in his reply brief. In that brief, petitioner contended that the district court had "doubts" about the legality of Detective Ilse's conduct, in part because petitioner's counsel had "provided the district court with examples in which federal agents and police officers had made a mistake by charging or accusing people with possessing child pornography, where the images did not qualify as such." Pet. C.A. Reply Br. 10. Petitioner also faulted the government for "present[ing] no witness from NCMEC on the process by which it is determined that database images are child pornography or the reliability or any other statistics concerning that determination." Id. at 11. Citing those circumstances, petitioner

contended that "the record in this case belies the government's claim that the hash values of the digital files are the equivalent of child pornography. Id. at 16; see id. at 16-17. In addition, petitioner mentioned the "property-rights prong of the Fourth Amendment" in a footnote, id. at 13 n.2, but he did not argue that the Court should apply that "prong" here, nor did he contend that Jones, supra, has abrogated Jacobsen. See Pet. C.A. Reply Br. 2-19.

b. The court of appeals upheld the district court's denial of petitioner's motion to suppress based on the private-search doctrine. The court of appeals explained that the "critical" Fourth Amendment inquiry as set forth in this Court's decision in Jacobsen "is whether the authorities obtained information with respect to which the defendant's expectation of privacy has not already been frustrated." Pet. App. A3 (quoting United States v. Runyan, 275 F.3d 449, 461 (5th Cir. 2001)). The court of appeals observed that, under Jacobsen, if a search by a private party "'frustrat[es] * * * the original expectation of privacy,'" the Fourth Amendment "'does not prohibit governmental use of' the now-nonprivate 'information.'" Ibid. (quoting Jacobsen, 466 U.S. at 117). Here, the court found that Microsoft conducted a private search when it automatically scanned petitioner's files, generated hash values for them, and matched those hash values to hash values in the NCMEC database, id. at A2-A3, and "whatever expectation of privacy [petitioner] might have had in the hash values of his files

was frustrated by Microsoft's private search," id. at A4; see id. at A4 n.1 ("assum[ing] without deciding" that petitioner had a legitimate expectation of privacy in the matched files).

The court of appeals observed that, "[w]hen Detective Ilse first received [petitioner]'s files, he already knew that their hash values matched the hash values of child pornography images known to NCMEC." Pet. App. A4. Explaining that "hash value comparison allows law enforcement to identify child pornography with almost absolute certainty," ibid. (citation and internal quotation marks omitted), the court determined that Detective Ilse's opening of the files "was no 'significant expansion of the search that had been conducted previously by a private party' sufficient to constitute 'a separate search,'" ibid. (quoting Walter v. United States, 447 U.S. 649, 657 (1980) (opinion of Stevens, J.)). The court explained that "opening the file merely confirmed that the flagged file was indeed child pornography, as suspected," in circumstances where it was "'virtually certain'" that the files were images of child pornography. Ibid. (citation omitted)

ARGUMENT

Petitioner contends (Pet. 11-23) that the exclusionary rule should be applied on the theory that Detective Ilse violated his Fourth Amendment rights by opening and viewing child-pornography files that petitioner had uploaded to Microsoft SkyDrive, where Microsoft had already scanned the files, determined that they were

images previously identified as child pornography, and sent them to NCMEC, which in turn sent the files to Detective Ilse. In making that Fourth Amendment claim, petitioner now argues (Pet. 21-23) that this Court's decision in United States v. Jones, 565 U.S. 400 (2012), abrogated United States v. Jacobsen, 466 U.S. 109 (1984), and bolsters his suppression claim, but he did not make that argument below, and the court of appeals did not address it. In any event, the court of appeals correctly determined that no Fourth Amendment violation occurred, and that factbound determination accords with this Court's precedent and does not conflict with any decision of another court of appeals. Moreover, the applicability of the good-faith exception to the exclusionary rule -- as recognized by the district court -- makes this an unsuitable vehicle for addressing petitioner's Fourth Amendment arguments. Further review is unwarranted.

1. The court of appeals correctly determined that Detective Ilse did not violate petitioner's Fourth Amendment rights by opening and viewing the matched files.

The Fourth Amendment's protection against unreasonable searches and seizures applies only to intrusions by government actors, not to searches conducted by private parties. See Burdeau v. McDowell, 256 U.S. 465, 475 (1921). In Jacobsen, the Court held that a government search that follows a private search of the same effects comports with the Fourth Amendment so long as it does not exceed the scope of the private search. 466 U.S. at 115-118.

In Jacobsen, Federal Express employees opened a damaged cardboard box and found crumpled newspaper covering a tube containing "a series of four zip-lock plastic bags, the outermost enclosing the other three and the innermost containing about six and a half ounces of white powder." 466 U.S. at 111. After notifying federal agents of their discovery, the employees put the plastic bags back inside the tube and placed the tube and newspapers back into the box. Ibid. When the first federal agent arrived, he removed the bags from the tube and saw the white power. Ibid. The agent then opened each of the plastic bags and removed a trace of the white powder, which a field test confirmed was cocaine. Id. at 111-112.

In holding that the agent's actions and the field test were constitutionally permissible, the Court began with the proposition that the "initial invasions of [the] package were occasioned by private action" and therefore did not implicate the Fourth Amendment. Jacobsen, 466 U.S. at 115. And once the private search had occurred, the Court reasoned, "[t]he additional invasions of respondents' privacy by the Government agent must be tested by the degree to which they exceeded the scope of the private search." Ibid. That rule, the Court explained, rests on the principle that "[o]nce frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information." Id. at 117. Rather, the "Fourth Amendment is implicated only if the authorities use information

with respect to which the expectation of privacy has not already been frustrated." Ibid.

Applying that standard in Jacobsen, the Court concluded that the agent's "viewing of what a private party had freely made available for his inspection did not violate the Fourth Amendment." 466 U.S. at 119-120. The Court found that, "[e]ven if the white powder was not itself in 'plain view' because it was still enclosed in so many containers and covered with papers, there was a virtual certainty that nothing else of significance was in the package and that a manual inspection of the tube and its contents would not tell him anything more than he already had been told." Id. at 118-119. The "advantage" the government gained from reexamining the contents of the box, the Court explained, "was merely avoiding the risk of a flaw in the employees' recollection, rather than in further infringing respondents' privacy." Id. at 119. The Court similarly found that "the removal of the plastic bags from the tube and the agent's visual inspection of their contents" was not a Fourth Amendment search because those actions "enabled the agent to learn nothing that had not previously been learned during the private search." Id. at 120. The Court reasoned that "the package could no longer support any expectation of privacy," in part because "[t]he agents had already learned a great deal about the contents of the package from the Federal Express employees, all of which was consistent with what they could see." Id. at 121.

The Court also concluded that the field test of the white powder did not constitute a Fourth Amendment search. Jacobsen, 466 U.S. at 122-126. The Court explained that "[t]he field test at issue could disclose only one fact previously unknown to the agent -- whether or not a suspicious white powder was cocaine." Id. at 122. Relying in part on its reasoning in United States v. Place, 462 U.S. 696 (1983), the Court explained that "[a] chemical test that merely discloses whether or not a particular substance is cocaine does not compromise any legitimate interest in privacy" because "Congress has decided * * * to treat the interest in 'privately' possessing cocaine as illegitimate." Jacobsen, 466 U.S. at 123; see id. at 123-125 (discussing Place). The Court thus reasoned that "the likelihood that official conduct of the kind disclosed by the record will actually compromise any legitimate interest in privacy seems much too remote to characterize the testing as a search subject to the Fourth Amendment." Id. at 124.

As the court of appeals determined, this Court's analysis in Jacobsen resolves this case. Pet. App. A3. Microsoft, a private actor, scanned petitioner's uploaded files, compared them to NCMEC's database of child-pornography hash values, and identified specific files with hash values that matched those in NCMEC's database. See id. at A2-A3, B2. Those hash-value matches indicated "with almost absolute certainty" that petitioner's matched files were images of child pornography, id. at A4 (citation

omitted), and Microsoft then sent only the matched files to NCMEC, which in turn sent the files to Detective Ilse. Because Microsoft's actions had already revealed that the files matched images previously identified as child pornography, Detective Ilse's viewing of the files "was no 'significant expansion'" of those prior searches "sufficient to constitute 'a separate search.'" Ibid. (quoting Walter v. United States, 447 U.S. 649, 657 (1980) (opinion of Stevens, J.)). At most, Detective Ilse's "visual review of the suspect images -- a step which merely dispelled any residual doubt about the contents of the files -- was akin to the government agents' decision to conduct chemical tests on the white powder in Jacobsen." Ibid. And petitioner identifies no court of appeals that has reached a different result on analogous facts. See Pet. App. A4 (noting consistency with United States v. Ackerman, 831 F.3d 1292, 1306-1307 (10th Cir. 2016) (Gorsuch, J.)).

2. a. Petitioner errs in contending that suppression is warranted under "this Court's opinion in Walter v. United States, 447 U.S. 649 (1980)." Pet. 16. As an initial matter, "there was no single opinion of the Court" in Walter. Jacobsen, 466 U.S. at 115. Although petitioner treats Justice Stevens's opinion in Walter as the opinion of the Court, see Pet. 16-18, only one other Justice joined that opinion. See Walter, 447 U.S. at 651. In any event, no conflict exists between Walter and the decision below.

In Walter, employees of a private company opened a misdirected carton, found rolls of motion picture films whose boxes included "explicit descriptions of the contents," and turned the carton over to federal agents, who later viewed the films without obtaining a warrant. 447 U.S. at 651-652 (opinion of Stevens, J.); see Jacobsen, 466 U.S. at 115. In considering those facts, six Justices -- two in the majority and four in dissent -- took the view that "the legality of the governmental search must be tested by the scope of the antecedent private search." Jacobsen, 466 U.S. at 116; see id. at 115-117. The four dissenting justices, however, found that the private employees had "so fully ascertained the nature of the films before contacting the authorities" that "the FBI's subsequent viewing of the movies on a projector did not 'change the nature of the search.'" Walter, 447 U.S. at 663 (Blackmun, J., dissenting, joined by Burger, C.J., Powell and Rehnquist, J.J.) (citation omitted). Justice Marshall concurred in the judgment without authoring or joining an opinion, id. at 660, and the two other Justices who agreed with the result took the view that the government's projection of the films would have infringed the Fourth Amendment even if the private employees had watched the films before turning them over to the government, see id. at 660-662 (White, J., concurring in part and concurring in the judgment, joined by Brennan, J.).

The fractured decision in Walter does not suggest that Detective Ilse violated the Fourth Amendment in this case. The

result in that case depended both on Justice Marshall's unexplained vote and on the votes of two other Justices whose approach was later superseded by the Court's adoption of the private-search doctrine in Jacobsen. In addition, the circumstances that the Court considered in Walter are significantly different from the facts here. In Walter, the FBI agents knew only that the rolls of film bore suspicious labels, but here, Detective Ilse knew both that some file names were indicative of child pornography and that Microsoft had already scanned the matched files and determined that they were images previously identified as child pornography. The facts of this case are thus analogous to Jacobsen, not Walter. In any event, that case-specific question does not warrant this Court's review.

b. Petitioner also argues (Pet. 12-20) that Detective Ilse's review of the matched files exceeded the scope of Microsoft's hash-value match because, petitioner claims, Detective Ilse did not "know" that the files were child-pornography images until he opened and viewed the files. Pet. 20. The premise of petitioner's argument is that the NCMEC database might contain hash values for files that are not child pornography and that a hash-value match to the NCMEC database thus does not establish that the file in question is child pornography. See Pet. 16, 18-20. The argument is unsound.

To begin with, the application of the private-search doctrine turns on "the degree to which" a government search "exceeded the

scope of the private search," Jacobsen, 466 U.S. at 115 (emphasis added), not on the nature of the evidence the private party uncovered. When Detective Ilse reviewed files that matched images that another person had already viewed, he did not exceed the scope of that earlier review, whether or not the images in question were actually child pornography. Petitioner does not dispute that the hash matching uniquely identified the files as containing images whose contents were already known, Pet. App. A3, and Detective Ilse did not infringe any privacy interest by looking at those previously viewed images. Furthermore, even if the precise contents of the image did matter, the Court held in Jacobsen that "[p]rotecting the risk of misdescription hardly enhances any legitimate privacy interest, and is not protected by the Fourth Amendment." 466 U.S. at 119.

In addition, the district court found "no evidence" to support petitioner's contention that the NCMEC database might contain hash values for files that are not child pornography. Pet. App. B2. Petitioner did not challenge that factual finding in his opening court of appeals' brief, see Pet. C.A. Br. 3-41, and the arguments in his reply brief came too late to preserve the issue. See United States v. Jackson, 426 F.3d 301, 304 n.2 (5th Cir. 2005) (per curiam) ("Arguments raised for the first time in a reply brief * * * are waived."). The court of appeals' opinion accordingly did not mention petitioner's challenge to the district court's factual findings regarding the NCMEC database. See Pet. App. A2-

A4. Petitioner identifies no reason for this Court to depart from its usual practice of declining to review claims that were "not pressed or passed upon" in the court of appeals below. United States v. Williams, 504 U.S. 36, 41 (1992) (citation omitted).

In any event, the district court did not err, much less clearly err, in rejecting petitioner's contention that NCMEC's database may include hash values of files that are not child pornography. Pet. App. B2. At the suppression hearing, one of the government's witnesses testified that NCMEC populates its database with the hash values of files depicting "known children" after "somebody has looked at the files and made a judgment that these are child pornography." Tr. 57. Although petitioner asserted during the district court proceedings that "NCMEC's database may contain images that are not actually child pornography," D. Ct. Doc. 40, at 2 n.1, he supported that assertion only with two news articles that described instances "where federal agents and police officers had made a mistake by charging or accusing people with possessing child pornography," Pet. 13. See D. Ct. Doc. 40, at 2 n.1. Those articles did not discuss the NCMEC database, see ibid., and petitioner introduced no evidence that the NCMEC database includes hash values for files that are not child pornography.

Finally, no court of appeals has adopted petitioner's view that the NCMEC database may include hash values of files that are not child pornography, and several courts of appeals have

recognized that the NCMEC database is limited to known child pornography. See United States v. Morrissey, 895 F.3d 541, 547 n.1 (8th Cir. 2018) ("NCMEC maintains a database of known child pornography that law enforcement can compare images to in order to determine if an image is confirmed child pornography -- meaning NCMEC has identified the subject in the image as a minor."); United States v. Woods, 684 F.3d 1045, 1051 (11th Cir. 2012) (per curiam) (recognizing that the NCMEC database catalogues "images of known child pornography"); United States v. Lacey, 569 F.3d 319, 322 n.2 (7th Cir.) ("NCMEC maintains a database of known victims of child pornography."), cert. denied, 558 U.S. 948 (2009); United States v. Sheldon, 223 Fed. Appx. 478, 480 (6th Cir. 2007) (referring to "the known-victim database maintained by * * * [NCMEC]"). The district court decision in United States v. Keith, 980 F. Supp. 2d 33 (D. Mass. 2013) (cited by Pet. 11, 14-15), also does not cast doubt on the provenance of the images in the NCMEC database because that case involved a hash-value match to a different database -- specifically, a database maintained by America Online (AOL) containing "hash values of files that AOL has at some time concluded contain child pornography." Id. at 37.

3. Petitioner additionally contends (Pet. 21-23) that the Court should grant a writ of certiorari to consider whether this Court's decision in Jones, supra, has abrogated Jacobsen. Petitioner raises this argument for the first time in this Court and did not press it below. See Pet. C.A. Br. 3-41; Pet. C.A.

Reply Br. 1-20. To the extent that petitioner now asserts (Pet. 21) that a footnote in his court of appeals' reply brief was sufficient to preserve a claim that Jones abrogated Jacobsen, that assertion is incorrect. In that footnote, petitioner observed that, after Florida v. Jardines, 569 U.S. 1, 10-11 (2013), "[o]ne might wonder about the viability of the portion of * * * Jacobsen" that relied on Place, supra. Pet. C.A. Reply Br. 13 n.2. But petitioner then acknowledged that Jardines had not, in fact, abrogated Jacobsen, see ibid.; the court of appeals did not address any abrogation argument; and no reason exists for the Court to consider it in the first instance, see, e.g., Department of Transp. v. Association of Am. R.Rs., 135 S. Ct. 1225, 1234 (2015).

In any event, Jones does not cast doubt on the decision below. Jones recognizes that a Fourth Amendment search occurs when the government "obtains information by physically intruding on a constitutionally protected area," in a manner that would constitute a "common-law trespass." 565 U.S. at 405, 406 n.3. Although petitioner contends that the court of appeals should have "considered" whether Detective Ilse "violated [petitioner]'s property rights under the Fourth Amendment," Pet. 23, petitioner does not provide any basis for concluding that he had a cognizable property interest in the matched files when Detective Ilse opened and viewed them. He does not dispute Microsoft's authority to send the files to NCMEC; Microsoft's authority to block him from its system when it discovered the files; or NCMEC's authority to

send the files to Detective Ilse. See Pet. App. A3-A5, B1-B2; Tr. 28-29. He thus cannot show the control or authority over the files that would be a prerequisite to any claim of common-law trespass. See, e.g., Oliver v. United States, 466 U.S. 170, 183 n.15 ("The law of trespass recognizes the interest in possession and control of one's property."); Restatement (Second) of Torts § 217, at 417 ("A trespass to a chattel may be committed by intentionally (a) dispossessing another of the chattel, or (b) using or intermeddling with a chattel in the possession of another.").

Petitioner notes (Pet. 22-23) that the Tenth Circuit has observed that, after Jones, "it seems at least possible" that this Court would now conclude that the drug test in Jacobsen, which required the officers to "exceed[] the scope of the search previously performed by the private party and remove[] and destroy[] a small amount of powder," constituted a Fourth Amendment search. Ackerman, 831 F.3d at 1307. But Ackerman did not suggest that Jones has undercut Jacobsen's determination that the Fourth Amendment allows a federal agent to replicate a private search without exceeding its scope. See id. at 1307-1308. In Ackerman, a government agent opened an email containing four attachments and viewed all four attachments, only one of which a private party (AOL) had determined had a hash value that matched child pornography. Id. at 1306. In light of its determination that "opening the email and viewing the [other] three attachments * * * was enough to risk exposing private, noncontraband information

that AOL had not previously examined," the Tenth Circuit expressly declined to resolve the question at issue in petitioner's case, i.e., whether a government agent conducts a Fourth Amendment search by opening a single file after a private party determines that the file's hash value matches the hash value of a child-pornography image. Id. at 1306-1307. Accordingly, as the opinion below recognizes, no conflict exists between Ackerman and the court of appeals' decision in petitioner's case. See Pet. App. A4.

4. Finally, this case would be a poor vehicle for addressing the questions presented in the petition because the district court correctly denied petitioner's suppression motion based on the good-faith exception to the exclusionary rule.

The exclusionary rule is a "'judicially created remedy'" that is "designed to deter police misconduct." United States v. Leon, 468 U.S. 897, 906, 916 (1984) (citation omitted). The rule does not apply "where [an] officer's conduct is objectively reasonable" because suppression "cannot be expected, and should not be applied, to deter objectively reasonable law enforcement activity." Id. at 919. Instead, to justify suppression, "police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system" for the exclusion of probative evidence. Herring v. United States, 555 U.S. 135, 144 (2009). "[E]vidence 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." Leon, 468 U.S. at 919 (citation omitted).

As the district court correctly determined, Pet. App. B5, even if Detective Ilse's review of the matched files constituted a search that violated the Fourth Amendment, the good-faith exception to the exclusionary rule would apply. This Court has held that suppression is inappropriate "when the police conduct a search in objectively reasonable reliance on binding judicial precedent," because such searches do not involve the type of culpable conduct that warrants an exclusionary sanction. Davis v. United States, 564 U.S. 229, 239 (2011); see id. at 249. In this case, a reasonable officer would believe that the court of appeals' decision in United States v. Runyan, 275 F.3d 449 (5th Cir. 2001), allowed Detective Ilse to open and view the matched files after a private party had already determined that the files' hash values matched hash values in the NCMEC database.

In Runyan, the defendant's ex-wife and friends discovered a cache of child pornography on CDs, floppy disks, and ZIP drives in the defendant's home. 275 F.3d at 453. After viewing some of the child-pornography files, the private searchers gave the materials to the police, who allegedly examined files that the private searchers had not reviewed. Id. at 453-454, 464. The Fifth Circuit determined that, "under Jacobsen, confirmation of prior knowledge does not constitute exceeding the scope of a private

search," which in turn "suggests that opening a container that was not opened by private searchers would not necessarily be problematic if the police knew with substantial certainty, based on the statements of the private searchers, their replication of the private search, and their expertise, what they would find inside." Id. at 463. The court further stated that "the police do not exceed the scope of a prior private search when they examine the same materials that were examined by the private searchers, but they examine these materials more thoroughly than did the private parties." Id. at 464. The court thus determined that the police "did not exceed the scope of the private search if they examined more files on the privately-searched disks than [the private searchers] had." Id. at 465.

Given this backdrop, it was objectively reasonable for Detective Ilse to believe that his review of the matched files complied with the Fourth Amendment. In addition, when Detective Ilse applied for the warrant to search petitioner's home, he "fully recited the circumstances by which he came into possession of the [matched] files and the fact that he opened them and viewed them." Pet. App. B5. Because the state judge issued a warrant for petitioner's home after being apprised of that history, a reasonable officer would rely on the judge's determination that the Fourth Amendment permitted the warrant. See Leon, 468 U.S. at 918-921.

The district court was thus correct in determining that "nothing in the warrant or otherwise known by [Detective Ilse] * * * would have made an objectively reasonable officer doubt the warrant's validity." Pet. App. B5. And because suppression is not appropriate "when the police act with an objectively 'reasonable good-faith belief' that their conduct is lawful," Davis, 564 U.S. at 238 (quoting Leon, 468 U.S. at 909), the matched files that Detective Ilse viewed and the evidence subsequently seized pursuant to the warrant in petitioner's case were properly admitted into evidence. Accordingly, a decision in petitioner's favor on the questions presented in the petition would not change the ultimate outcome here.

CONCLUSION

The petition for a writ of certiorari should be denied.

Respectfully submitted.

NOEL J. FRANCISCO
Solicitor General

BRIAN A. BENCZKOWSKI
Assistant Attorney General

SONJA M. RALSTON
JOHN P. TADDEI
Attorneys

MARCH 2019