No. 20-1204

In the Supreme Court of the United States

MARK RINGLAND, PETITIONER

v.

UNITED STATES OF AMERICA

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

BRIEF FOR THE UNITED STATES IN OPPOSITION

ELIZABETH B. PRELOGAR
Acting Solicitor General
Counsel of Record
NICHOLAS L. MCQUAID
Acting Assistant Attorney General
ANN O'CONNELL ADAMS
Attorney
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 she opened and viewed digital child pornography files that petitioner had attached to an email, where Google 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 them to the police.

ADDITIONAL RELATED PROCEEDINGS

United States District Court (D. Neb.):

United States v. *Ringland*, No. 17-cr-289 (June 11, 2019)

United States Court of Appeals (8th Cir.):

United States v. *Ringland*, No. 19-2331 (July 16, 2020)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases:

Cases—Continued: Page

Constitution and statutes:

Miscellaneous:

In the Supreme Court of the United States

No. 20-1204

MARK RINGLAND, PETITIONER

v.

UNITED STATES OF AMERICA

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

BRIEF FOR THE UNITED STATES IN OPPOSITION

OPINIONS BELOW

The opinion of the court of appeals (Pet. App. 3a-14a) is reported at 966 F.3d 731. The order of the district court (Pet. App. 15a-30a) is not published in the Federal Supplement but is available at 2019 WL 77276.

JURISDICTION

The judgment of the court of appeals was entered on July 16, 2020. A petition for rehearing was denied on October 6, 2020 (Pet. App. 1a-2a). On March 19, 2020, this Court extended the time within which to file any petition for a writ of certiorari due on or after that date to 150 days from the date of the lower-court judgment, order denying discretionary review, or order denying a timely petition for rehearing. The petition for a writ of certiorari was filed on February 25, 2021. The jurisdiction of this Court is invoked under 28 U.S.C. 1254(1).

STATEMENT

Following a jury trial in the United States District Court for the District of Nebraska, petitioner was convicted on one count of receiving child pornography, in violation of 18 U.S.C. 2252(a)(2). Judgment 1. He was sentenced to 168 months of imprisonment, to be followed by ten years of supervised release. Judgment 2-3. The court of appeals affirmed. Pet. App. 3a-14a.

1. Google uses proprietary "hashing" technology to detect confirmed images of child sexual abuse on its servers. D. Ct. Doc. 73-2, at 2 (Aug. 30, 2018); see Pet. App. 5a. After an image is viewed by at least one Google employee and confirmed to be apparent child pornography, it is given a digital fingerprint called a "hash" that is added to Google's repository of hashes. D. Ct. Doc. 73-2, at 2; see Pet. App. 4a-5a. Comparing the hash values of content uploaded to Google's services against the repository of child pornography hash values allows Google to identify duplicate images of child pornography and prevent them from circulating on Google's products. *Ibid.* Federal law does not require Google to undertake those efforts, see 18 U.S.C. 2258A(f); but it does require Google and other "electronic communication service provider[s]" who become aware of child pornography on their services to report it to the National Center for Missing and Exploited Children (NCMEC), a nonprofit entity. 18 U.S.C. 2258E(6); see Pet. App. 5a; 18 U.S.C. 2258A(a).

Between March 20, 2017, and April 19, 2017, Google sent reports to NCMEC's CyberTipline containing 1216 files from petitioner's email account mringland69@gmail.com that had been flagged as apparent child pornography, some of which were discovered through

Google's hashing technology. Pet. App. 5a. Google affirmed that it had reviewed 502 of the files but gave no information on whether it had reviewed the others. *Ibid.* Using the Internet Protocol (IP) addresses contained in Google's report, NCMEC identified the internet service provider as Sprint PCS in Omaha, Nebraska. *Id.* at 16a; NCMEC forwarded all of the reports to the Nebraska State Police. *Id.* at 5a, 16a-17a.

On June 20, 2017, Google discovered that the address mringland65@gmail.com was linked to petitioner's mringland69 account. Pet. App. 5a. Google uploaded two files from the mringland65 account to NCMEC but "gave no information as to its review." *Id.* at 5a-6a. In connection with a separate investigation, NCMEC forwarded the files to police officers in South Dakota, noting that it had not reviewed them. *Id.* at 6a, 35a. South Dakota law enforcement forwarded the files to the Nebraska State Police; the officer investigating petitioner's activities received but did not view them. *Id.* at 35a & n.4.

On June 27, 2017, the Nebraska State Police officer obtained a warrant to search the mringland69 account. Pet. App. 6a. In her warrant application, the officer explained that Google had reviewed 502 of the 1216 files forwarded from this account and that "she had reviewed only the same 502 files." *Ibid.*; see *id.* at 17a, 34a-35a. Her subsequent search of materials from the email account pursuant to the warrant showed that the email address had sent child pornography to the mringland65 account. *Id.* at 6a.

In July 2017, Google sent two additional reports to NCMEC from a third email address, markringland65@gmail.com, with no information as to its review. Pet. App. 6a. NCMEC did not review the files attached

to the reports but forwarded them to the Nebraska State Police after tracing several of the related IP addresses to Omaha. *Id.* at 6a, 18a. In August 2017, in a series of nine more reports, Google uploaded 1109 more files from the markringland65 account to NCMEC, indicating that it had reviewed 773 of the files and giving no information on the others. *Id.* at 6a. NCMEC reviewed one report and found apparent child pornography, then forwarded all reports to the Nebraska State Police. *Ibid.*

The same police officer obtained a warrant to search the mringland65 and markringland65 accounts. Pet. App. 6a-7a. The officer explained in her warrant application that the mringland65 account had been sent child pornography from the mringland69 account, and that the nine reports from Google indicated that the markringland65 account "contain[ed] alleged contraband." *Id.* at 7a. The officer expressly "noted Google had not reviewed all the files in the reports and she had not viewed them either." *Ibid.*

The officer reviewed information from Google pursuant to the search warrants and concluded that several files contained images and videos of child pornography. Pet. App. 18a-19a. Based on that information, the officer obtained a warrant to track petitioner's cell phone and warrants to search and arrest petitioner. *Id.* at 7a. Police arrested petitioner, who made incriminating statements and allowed officers to retrieve an iPad from his van. *Ibid.*; see Gov't C.A. Br. 7-8.

2. A grand jury in the District of Nebraska returned an indictment charging petitioner with one count of knowingly receiving child pornography, in violation of 18 U.S.C. 2252(a)(2), and one count of knowingly possessing child pornography, in violation of 18 U.S.C.

2252(a)(4)(B) and (b)(2). Indictment 1. Petitioner moved to suppress all evidence of child pornography recovered from his three email accounts and the incriminating statements made during his arrest. Pet. App. 7a, 20a.

The district court, adopting the findings and recommendation of the magistrate judge, denied the motion. Pet. App. 15a-30a; see *id.* at 31a-47a (magistrate judge's findings and recommendation). The court rejected petitioner's argument that Google is a governmental actor. *Id.* at 23a-27a. The court further found that the police officer viewed only the 502 files already viewed by Google and relied on only those files in her initial warrant application. *Id.* at 28a. Accordingly, the court determined that even assuming that NCMEC is a governmental actor, any potentially unlawful review by it did not taint the officer's review and warrant applications. *Id.* at 28a-29a. The court then determined that the police officer's actions did not violate the Fourth Amendment because they "did not exceed the scope of the private search done by Google." *Id.* at 45a. In the alternative, the court determined that the good-faith exception to the exclusionary rule applied because the judge issuing the relevant warrants had not "abandoned a detached and neutral role" and no law enforcement officer had been dishonest or misleading in preparing a warrant affidavit. *Id.* at 29a.

Petitioner proceeded to a jury trial. The verdict form instructed the jury not to consider the possession count if it found petitioner guilty of receipt. D. Ct. Doc. 105 (Feb. 20, 2019). The jury returned a guilty verdict on the receipt count and the government accordingly dismissed the possession count. Judgment 1. Petitioner was sentenced to 168 months of imprisonment, to

be followed by ten years of supervised release. Judgment 2-3.

3. The court of appeals affirmed. Pet. App. 3a-14a.

The court of appeals rejected petitioner's argument that Google had conducted an unreasonable search in violation of the Fourth Amendment by scanning his email for child pornography. Pet. App. 10a-13a. The court explained that Google "scanned its users' emails volitionally and out of its own private business interests" and "did not become a Government agent merely because it had a mutual interest in eradicating child pornography from its platform." *Id.* at 11a. The court further explained that a statutory scheme that requires Google to report any child pornography that it found through its searches to NCMEC "does not so strongly encourage affirmative searches such that it is coercive." *Ibid.*

The court of appeals also determined that the officer's review of the child pornography images sent by Google was "appropriate under the private search doctrine" described in *United States* v. *Jacobsen*, 466 U.S. 109 (1984), because the officer "searched only the same files that Google searched" and "did not expand the search beyond Google's private party search." Pet. App. 13a. And the court observed because the officer's search-warrant applications did not contain information from NCMEC's searches and were limited only to information Google already had viewed, suppression would be unwarranted even if NCMEC's actions were deemed a governmental search that went beyond the scope of Google's search. *Id.* at 13a-14a.

ARGUMENT

Petitioner seeks (Pet. 7-14) either plenary review or summary reversal on the theory that the private-search

doctrine recognized in *United States* v. *Jacobsen*, 466 U.S. 109 (1984), was vitiated by this Court's decision in *United States* v. *Jones*, 565 U.S. 400 (2012).* Neither course is warranted here. Petitioner did not adequately preserve the argument he raises now. In any event, the court of appeals correctly recognized that no Fourth Amendment violation occurred, and its decision does not conflict with any decision of this Court or another court of appeals. Moreover, the applicability of the good-faith exception to the exclusionary rule means that petitioner's Fourth Amendment arguments would not change the result in this case.

1. The court of appeals correctly recognized that police did not violate petitioner's Fourth Amendment rights by opening and viewing child pornography images that Google had already viewed and confirmed to be child pornography. 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). Accordingly, 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.

a. In *Jacobsen*, Federal Express employees had 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

---

* The petition for a writ of certiorari in *Miller* v. *United States*, No. 20-1202 (filed Feb. 25, 2021), presents the same argument in a similar case.

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 powder. *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. The Court then explained that once the private search had occurred, "[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.* And 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 [the agent] anything more than he already had been told." *Id.* at 118-119.

The Court accordingly held 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." *Jacobsen*, 466 U.S. at 120. The Court observed 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. And the Court further determined that the field test of the white powder did not constitute a Fourth Amendment search. *Id.* at 122-126. 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*, *supra*).

b. As the court of appeals correctly recognized, this Court's analysis in *Jacobsen* resolves this case. Pet. App. 13a-14a. Google, a private actor, detected child pornography in petitioner's emails though hashing technology and other means and sent the images to NCMEC, which in turn sent the files to the police. *Id.* at 5a-7a. The officer who received the reports was careful to ensure that she viewed only the files that Google already had viewed and confirmed to be child pornography, and she relied on only those files to obtain warrants for petitioner's email accounts. *Ibid.* Accordingly, the officer's viewing of the files revealed nothing more than what Google already had discovered. *Id.* at 13a-14a.

2. Petitioner contends (Pet. 7-12) that the Court should grant a writ of certiorari to consider whether this Court's decision in *Jones*, *supra*, has abrogated *Jacobsen*. Review of that question is not warranted.

a. As an initial matter, petitioner did not adequately preserve his *Jones* argument, which proposes that a

trespass-based approach to search undermines *Jacobsen*, in the court of appeals. Although petitioner's brief below included passing references to a trespass to chattels, those references were solely in service of his separate argument—which he does not renew in this Court—that Google and NCMEC were governmental actors. Pet. C.A. Br. 31-52. Petitioner did not assert that police officers had themselves committed any such trespass to chattels, that the private-search doctrine depends solely on a reasonable-expectation-of-privacy approach to Fourth Amendment searches, or that deeming a trespass to have occurred here would vitiate that doctrine's applicability. Indeed, the only original citation of *Jones* came in the Conclusion section of the brief, in which petitioner asserted that the "rationale[] undergirding" *Jones* "can affirm society's *reasonable expectation of privacy* in its correspondence." *Id.* at 54 (emphasis added); cf. *id.* at 33 n.136 (citing a court of appeals case that cited *Jones*).

Moreover, when petitioner discussed the trespass theory, he linked the trespass to viewing of information beyond the child pornography that Google had already viewed. See Pet. C.A. Br. 32 (stating that "[t]he warrantless opening and examination of private correspondence *that could have contained much besides contraband* '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'") (emphasis added; citation omitted); *id.* at 49 (stating that "[*t*]*he repeated expansions of Google's searches by NCMEC* infringed upon Mr. Ringland's reasonable expectation of privacy and constituted a trespass to chattels").

Petitioner did not raise the trespass-to-chattels argument in the way he raises it now or set forth his current view that *Jacobsen* is no longer valid after *Jones*. The government accordingly did not respond to any such argument its court of appeals brief, see Gov't C.A. Br. 11-23; petitioner did not mention a trespass to chattels in his reply brief below, see Pet. C.A. Reply Br. 1-7; and the court of appeals did not address any such argument. This Court is "a court of review, not of first view," *Cutter* v. *Wilkinson*, 544 U.S. 709, 718 n.7 (2005), and its "traditional rule * * * precludes a grant of certiorari * * * when 'the question presented was not pressed or passed upon below,'" *United States* v. *Williams*, 504 U.S. 36, 41 (1992) (citation omitted); see, *e.g.*, *Zobrest* v. *Catalina Foothills School District*, 509 U.S. 1, 8 (1993); *Adickes* v. *S. H. Kress & Co.*, 398 U.S. 144, 147 n.2 (1970). Those principles render certiorari inappropriate.

b. Even setting aside petitioner's failure to preserve the issue, his contention that *Jones* silently abrogated *Jacobsen* lacks merit. *Jones* held "that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitute[d] a 'search'" under the Fourth Amendment. 565 U.S. at 404 (footnote omitted). The Court emphasized that it was "important to be clear about what occurred in th[e] case: The Government physically occupied private property for the purpose of obtaining information." *Ibid.* And the Court had "no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." *Id.* at 404-405.

The Court in *Jones* did not, however, extend its holding beyond "physical intrusion of a constitutionally protected area," 565 U.S. at 407, to encompass electronic searches. The Court noted that "[i]t may be that [surveillance] through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy," but stated that the case "d[id] not require [the Court] to answer that question." *Id.* at 412. The Court later did address such an issue in *Carpenter* v. *United States*, 138 S. Ct. 2206 (2018), in which it held that under a reasonable-expectation-of-privacy approach, the government's acquisition of historical cell-site location information created and maintained by a cell-service provider is a Fourth Amendment search. *Id.* at 2217 & n.3. But although the Court noted that in separate concurrences in *Jones*, "[a] majority of th[e] Court ha[d] already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements," *id.* at 2217 (citing *Jones*, 565 U.S. at 430 (Alito, J., concurring in judgment), and *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)), it did not apply *Jones*'s *physical*-trespass analysis to the electronic search at issue, *id.* at 2214 & n.1.

In any event, even assuming that viewing electronic images could be deemed materially identical to a physical trespass, *Jones* would not cast doubt on the decision below. Petitioner provides no basis for concluding that he had a constitutionally protected property interest in the matched files when the police officer opened and viewed them. He does not dispute Google's authority to send the files to NCMEC or NCMEC's authority to send the files to the police. 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 (1984) ("The law of trespass recognizes the interest in possession and control of one's property."); Restatement (Second) of Torts § 217, at 417 (1965) ("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.").

c. Other courts of appeals addressing circumstances similar to this case have likewise recognized that no Fourth Amendment violation occurred in those cases, and this Court previously has declined to review such a case. It should do the same here.

In *United States* v. *Reddick*, 900 F.3d 636 (5th Cir 2018), cert. denied, 139 S. Ct. 1617 (2019) (No. 18-6734), the defendant uploaded digital image files to Microsoft SkyDrive, a cloud-hosting service that uses PhotoDNA to automatically scan the hash values of user-uploaded files and compare them against the hash values of known child pornography. *Id.* at 637-638. Microsoft sent a report to NCMEC's CyberTipline based on the hash values of files that the defendant had uploaded to SkyDrive; NCMEC then forwarded the report to police in Corpus Christi, Texas. *Id.* at 638. A detective opened each of the suspect files and confirmed they contained child pornography. *Ibid.* The detective then obtained a search warrant for the defendant's home where additional child pornography was found, and the defendant was indicted for possession of child pornography. *Ibid.*

The Fifth Circuit recognized that "[t]he private search doctrine decides this case." *Reddick*, 900 F.3d at 637. The court observed that a private company had determined that the hash values of files uploaded by the defendant matched hash values of known child pornography and passed that information to police. *Ibid.* And

the court found that "the government's subsequent law enforcement actions in reviewing the images did not effect an intrusion on [the defendant's] privacy that he did not already experience as a result of the private search." *Ibid.* This Court denied certiorari. *Reddick* v. *United States*, 139 S. Ct. 1617 (2019) (No. 18-6734).

Similarly, in *United States* v. *Miller*, 982 F.3d 412 (6th Cir. 2020), petition for cert. pending, No. 20-1202 (filed Feb. 25, 2021), the defendant uploaded images to an email with hash values matching images of known child pornography in Google's repository; Google sent the images to NCMEC, which investigated further and sent the file to the Kentucky State Police; a police officer received the file, viewed only the images with the known hash values, and confirmed that they depicted pre-pubescent children engaged in sex acts; and the officer then used the information to obtain search warrants for Google's records of the email account and the defendant's home. *Id.* at 420-421. The Sixth Circuit recognized that the case was governed by the private-search doctrine because the government's search did not exceed the scope of Google's earlier private search. *Id.* at 427-430 (citing *Jacobsen*, 466 U.S. at 115). The court additionally recognized that the private-search doctrine applied notwithstanding any trespass to chattels, observing that the doctrine had been applied "even when a private party had committed a trespass" such as blowing open a safe and giving its contents to the government. *Id.* at 433 (citing *Burdeau*, 256 U.S. at 475); see *ibid.* ("If [the officer's] viewing of the files would qualify as a 'search' under *Jones*'s trespass approach, the DEA agent's examination the box in [*Jacobsen*] would also qualify.").

Relying on the Tenth Circuit's decision in *United States* v. *Ackerman*, 831 F.3d 1302 (2016), petitioner asserts that "one court of appeals has been willing to draw the 'obvious analogy' between compelling and opening someone's emails and 'the common law's ancient trespass to chattels doctrine,'" while other courts of appeals have concluded that *Jacobson* controls. Pet. 7 (citation omitted). The suggestion that the decision below implicates a circuit conflict is misplaced. 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. 831 F.3d at 1306. The Tenth Circuit concluded that "opening the email and viewing the three other attachments * * * was enough to risk exposing private, noncontraband information that AOL had not previously examined," and relied on that conclusion to find a Fourth Amendment violation. *Id.* at 1306-1307. But the Tenth Circuit expressly declined to resolve the question at issue in this case: whether a government agent violates the Fourth Amendment by opening an image after a private party already has determined that the file's hash value matches the hash value of a known child-pornography image. *Id.* at 1306-1308. Accordingly, as the court of appeals recognized (Pet. App. 13a), no conflict exists between *Ackerman* and the decision below.

Ackerman 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. 831 F.3d at 1307. But *Ackerman* did not hold

that *Jones* has undercut *Jacobsen*'s determination that the Fourth Amendment allows a federal agent to replicate a private search without exceeding its scope, as petitioner urges here. See *id.* at 1307-1308. And petitioner identifies no circuit that has.

3. As an alternative to plenary review, petitioner requests (Pet. 14) that this Court summarily reverse the decision below and direct the lower courts to analyze petitioner's argument under a trespass-based approach. According to petitioner (*ibid.*), by following the directly on-point precedent of *Jacobsen*, the court of appeals disobeyed this Court's instruction that the trespass-based approach for evaluating whether a search occurred is independent from the reasonable-expectation-of-privacy test. Cf. *Jones*, 565 U.S. at 409 (reasonable-expectation-of-privacy approach was "added to, not substituted for, the common-law trespassory test") (emphasis omitted). Summary reversal is unjustified.

As explained above, petitioner did not adequately preserve a trespass argument in the lower courts. Furthermore, as discussed above, this Court was well aware of the trespass-based approach when it decided *Jacobsen*, yet did not suggest that the private-search doctrine was incompatible with that approach. See *Agostini* v. *Felton*, 521 U.S. 203, 237 (1997) ("If a precedent of this Court has direct application in a case, yet appears to rest on reasons rejected in some other line of decisions, the Court of Appeals should follow the case which directly controls, leaving to this Court the prerogative of overruling its own decisions.") (citation omitted).

4. In any event, irrespective of how the question presented might be resolved, the images viewed by the police officer should not be suppressed because, as the dis-

trict court correctly recognized, the good-faith exception to the exclusionary rule applies. Pet. App. 29a-30a. And it is well settled that appellate courts generally "have discretion to affirm on any ground supported by the law and the record." *Upper Skagit Indian Tribe* v. *Lundgren*, 138 S. Ct. 1649, 1654 (2018); see *Smith* v. *Phillips*, 455 U.S. 209, 215 n.6 (1982).

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).

In this case, it would have been reasonable for an officer to believe—like the district court and the court of appeals below—that the Fourth Amendment allowed the officer to open and view the files after a private party already had determined that the files' hash values matched known child-pornography images in its database. In addition, when the officer applied for the war-

rants to search the contents of petitioner's email accounts and to search petitioner's home, the affidavits in support included the information contained in the reports to NCMEC, described how the officer had come to possess the child pornography images, and notified the court that she had opened and viewed the images. Pet. App. 6a-7a, 13a-14a, 34a-36a. Because state and federal judges issued those warrants after being apprised of that history, an officer would reasonably rely on those judicial determinations that the Fourth Amendment permitted the warrants. See *Leon*, 468 U.S. at 918-921. The matched files that the officer viewed and the evidence subsequently seized pursuant to warrants in petitioner's case were thus properly admitted into evidence.

CONCLUSION

The petition for a writ of certiorari should be denied.

Respectfully submitted.

ELIZABETH B. PRELOGAR
Acting Solicitor General
NICHOLAS L. MCQUAID
Acting Assistant Attorney General
ANN O'CONNELL ADAMS
Attorney

MAY 2021