No. 20-1737

In the Supreme Court of the United States

LUKE NOEL WILSON,

Petitioner,

v.

STATE OF CALIFORNIA,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE
CALIFORNIA COURT OF APPEAL,
FOURTH APPELLATE DISTRICT, DIVISION ONE

BRIEF IN OPPOSITION

ROB BONTA
Attorney General of California
MICHAEL J. MONGAN
Solicitor General
LANCE E. WINTERS
Chief Assistant Attorney General
JOSHUA A. KLEIN
Deputy Solicitor General
ARLENE A. SEVIDAL
Supervising Deputy Attorney General
ANDREW S. MESTMAN *
Deputy Attorney General
600 West Broadway, Suite 1800
San Diego, CA 92101
(619) 738-9035
Andrew.Mestman@doj.ca.gov
**Counsel of Record*

QUESTION PRESENTED

Petitioner uploaded to his Gmail account four image files. Google's software scanned those files and identified the "hash value" for the images—a "digital fingerprint" generated by a computer algorithm that is "unique" to the image. Pet. App. 5 & n.4, 14; 1 Clerk's Transcript 196. Those hash values revealed that the images were duplicates of images that trained Google employees had previously viewed and identified as illegal child pornography involving prepubescent children engaged in sexual activity. Google sent a report describing its identification of the images as child pornography, and forwarded the image files, to the National Center for Missing and Exploited Children, which transmitted the report and image files to a law enforcement task force. The question presented is:

Whether law enforcement agents were required to obtain a warrant before they could open the files and view the images.

DIRECTLY RELATED PROCEEDINGS

California Supreme Court:

People v. Wilson, No. S265795, review denied January 20, 2021.

California Court of Appeal, Fourth District, Division 1:

People v. Wilson, No. D074992, judgment entered October 21, 2020.

California Superior Court, San Diego County:

People v. Wilson, No. SCD263466, judgment entered October 23, 2018.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES
(continued)

Page

STATUTES

CONSTITUTIONAL PROVISIONS

OTHER AUTHORITIES

STATEMENT

Petitioner Luke Noel Wilson was convicted of one count of oral copulation of a child under 10 years old and three counts of lewd acts upon children, for paying a young woman to sexually abuse her daughter and cousin. Pet. App. 1.[1] He was sentenced to a prison term of 45 years to life. *Id*. at 2. His petition raises Fourth Amendment challenges to the admission of evidence that led to those convictions.

1. a. The evidence at trial showed that in 2009 or 2010 petitioner began paying J.A., who was 15 years old, to pose for photographs. Pet. App. 2. At first, J.A. posed clothed. *Id.* at 2-3. Eventually, while J.A. was still a minor, petitioner began paying her and giving her alcohol to pose nude and to pose for photos while she used sex toys on herself or while he performed sexual acts on her. *Id.* at 3.

When J.A. was 18, she gave birth to a baby girl. Pet. App. 3.[2] Petitioner began offering to pay J.A. to molest her baby and send photos to petitioner. *Id.* J.A. first complied when the baby was nine months old; J.A. placed her hand on the baby's buttocks, spread them apart, and sent petitioner either a picture or a video. *Id.*; 4 RT 269-270, 272.[3] When the baby was nine or ten months

---

[1] The jury also found true beyond a reasonable doubt that two counts were committed against more than one victim. Pet. App. 1.

[2] Petitioner was not the father of the baby. Pet. App. 3.

[3] "RT" refers to the Reporter's Transcript; "CT" refers to the trial court's Clerk's

old, petitioner also requested photos or video of J.A. orally copulating the baby. Pet. App. 3. J.A. again accepted, orally copulating the child and sending petitioner a video of that act. *Id.* Petitioner, who knew that J.A. frequently babysat her five-year-old cousin, repeatedly offered to pay J.A. to touch the cousin as well. *Id.* at 4. J.A. accepted on one occasion, touching the child's bare buttocks and sending photos to petitioner. *Id.*[4]

b. Before the trial, petitioner moved to suppress evidence based on events connected to an email that petitioner sent using his account on Gmail, an email service provided by Google. After the suppression hearing, the trial court denied petitioner's motion. That ruling is the focus of the Fourth Amendment question that petitioner seeks to raise in this Court.

The evidence at the suppression hearing established that Google informs users, in its terms of service, that Gmail (and other Google services) may be used only for legal purposes, and that Google "may review content to determine whether it is illegal." Pet. App. 5. Possessing or trafficking in child pornography is illegal. *See* 18 U.S.C. §§ 2251 *et seq.* Google has a team of employees trained on the definition and recognition of illegal child

---

Transcript; "Supp. CT" refers to the Supplemental Clerk's Transcript; and "Aug. CT" refers to the Augmented Clerk's Transcript.

[4] Petitioner unsuccessfully attempted to convince J.A. to molest others as well—asking J.A. to take pictures of herself orally copulating two other minor girls, and sending J.A. pictures of a fifth child whom he requested that J.A. molest. Pet. App. 4.

pornography. Pet. App. 5-6, 14; 1 CT 196. When any of those employees view an image or video file and determine that it meets the definition of child pornography, the incident is reported and the image or video file is forwarded to the National Center for Missing and Exploited Children (NCMEC), 1 CT 197, a nonprofit organization that receives an annual congressional appropriation to perform various functions relating to preventing the exploitation of children.[5] The contraband file is not retained by Google. But before deleting it, Google generates a "hash" value for the file and adds that value to a Google database. Pet. App. 5, 14; 1 CT 196. Every hash value in that database corresponds to a file that was personally viewed by a Google employee. 1 CT 196 (Google employee's declaration that "[n]o hash is added to our repository without the corresponding image first having been visually confirmed by a Google employee to be apparent child pornography").

The hash value—a "digital fingerprint" generated by a computer algorithm—is "unique" to the image. Pet. App. 5 & n.4, 14; 1 CT 196. That enables Google to automatically detect when a duplicate of the image is again present in its system. When a user uploads new content to its services, Google automatically scans and generates hash values for the files and compares those

---

[5] *See generally United States v. Cameron*, 699 F.3d 621, 628 (1st Cir. 2012). Federal law requires Google to report apparent child pornography to NCMEC once it obtains actual knowledge of its content. Pet. App. 6; 18 U.S.C. § 2258A(a). NCMEC is statutorily obligated to forward such reports to federal law enforcement. Pet. App. 6 n.5.

hash values to the hash values in Google's database. Pet. App. 5, 14. If Google's system detects a match between a hash value for uploaded content and a hash value in the database, the system generates a report. Pet. App. 5-6. That report is sent, along with the files at issue, to NCMEC in the form of a "CyberTip." *Id.* at 5-6, 14; 1 CT 196-197. Because the hash process itself reflects that a file contains an image that Google employees have already determined to fit the definition of child pornography, when a new file with the same hash is detected, a Google employee will not always view the image in that file before reporting and sending it to NCMEC. Pet. App. 6, 14; 1 CT 197.

The investigation of petitioner arose in June 2015, when Google's system detected that four image files with hash values matching those in its child pornography database had been uploaded to petitioner's account. Pet. App. 6. Google generated a CyberTip report to NCMEC and forwarded the four attached files, without the email text. *Id.* No Google employee opened those four image files to view their contents upon their detection in petitioner's account. Pet. App. 6, 14; 1 CT 197. However, the report indicated that Google employees had classified each image as "A1," with "A" denoting depiction of a prepubescent minor and "1" denoting that the minor was engaged in "sexual activity." Pet. App. 6, 14; 1 CT 197. That classification was based on Google employees' previous visual examination of four duplicate image files with the same hash values. Pet. App. 6; 1 CT 196-197. The definition of "sexual activity" for purposes of that categorization tracked the definition in federal

child pornography statutes. *Compare* 1 CT 215, *with* 18 U.S.C. § 2256(2)(A). The CyberTip report gave information about the date, time, and electronic source of the user's uploading of the images—but did not provide any text from the email that those images had been attached to. 1 CT 197; 1 Aug. RT 14-15. Without opening or reviewing the image files, NCMEC determined that the e-mail account was being used from the San Diego area and forwarded the report and images to the San Diego Internet Crimes Against Children (ICAC) task force. Pet. App. 6-7.

An administrative assistant at the ICAC printed the report and images. Pet. App. 7. A federal agent read the report, viewed the images, and confirmed that the images depicted prepubescent children engaged in sex acts. *Id.*[6] The agent then obtained a search warrant to acquire from Google content and user information associated with the identified Gmail address. *Id.* Those records contained emails from petitioner offering to pay J.A. to molest children, and

---

[6] In discussing the CyberTip's report of information from Google, the trial court stated that "[t]here was disclosure that a human didn't look at the files but, under the hash value process and system, it was determined and identified as child pornography . . . based on the A1 designation and system." 1 Aug. RT 72-73. In fact, the suppression hearing record does not explicitly indicate whether the law enforcement officials knew at the time they printed and viewed the images (as opposed to determining later) that Google's identification of the images as child pornography was based on Google employees' having viewed earlier image files with the same hash value, or whether the law enforcement officials could have believed that Google employees might have viewed the duplicate image files attached to petitioners' email. *See* 1 Aug. RT 36-37 (stating simply that it "was determined to be the case" that Google had not looked at petitioner's attachments and was relying solely upon their hash-value comparison to the previously viewed copies).

additional emails in which petitioner distributed child pornography to others. *Id.* The agent then obtained a warrant to search petitioner's residence. *Id.* While law enforcement was executing that warrant, someone threw a backpack containing a thumb drive off petitioner's balcony. *Id.* That thumb drive, and other computer equipment in petitioner's home, contained additional child pornography and further evidence of petitioner's dealings with J.A. *Id.* When police interviewed J.A., she eventually admitted to molesting children in exchange for payment from petitioner. *Id.* at 4, 7.

Petitioner moved to suppress evidence of the four initial images provided by Google, evidence recovered from petitioner's and J.A.'s homes and electronic accounts, statements from J.A.'s niece about the abuse, and physical evidence from J.A.'s niece and daughter, all on the theory that the ICAC agent had violated the Fourth Amendment by not obtaining a warrant before he first viewed the images that Google had sent to NCMEC. Pet. App. 8; Supp. CT 5-9. The trial court denied the motion. Pet. App. 9.

As an initial matter, the court reasoned, "any subjective expectation of privacy" that petitioner had in the child pornography attachments "would not be objectively reasonable or justifiable under the circumstances," given the terms of service petitioner agreed to when he created his Google account. 1 Aug. RT 70.[7] In any event, the court continued, the agent's warrantless

---

[7] The parties had agreed that petitioner had a subjective expectation of

examination of the four images received from NCMEC was permissible under *United States v. Jacobsen*, 466 U.S. 109 (1984), because the agent's examination of those images was "not a significant expansion" of the private search that Google had already conducted. 1 Aug. RT 73-74. Government agents had not examined the text of petitioner's emails, had not viewed any attachments other than the ones Google identified as duplicates of previously viewed child pornography images, and had done nothing to "risk exposing private non contraband information that [the private provider] had not previously examined." *Id.* at 71-72 (distinguishing case cited by petitioner). The court found that Google's "hash values are like fingerprints," and that because the new images were identical to the ones Google employees had seen before—to "a virtual certainty"—the agent who examined the images "could learn nothing that had not previously been learned during the private search." *Id.* at 73.

2. The court of appeal affirmed petitioner's convictions and sentence. Pet. App. 1-48. As relevant here, the court rejected petitioner's claim that the trial court erred by denying his motion to suppress evidence. *Id.* at 10-25.

Under longstanding precedent, the court observed, "the Fourth Amendment does not apply to private searches." Pet. App. 11; *see id.* at 11 n.7 (noting that "[n]o argument has been made that Google was an 'instrument or

---

privacy, but disagreed about whether that expectation was objectively reasonable. 1 Aug. RT 7.

agent' of the government here"). And under related precedent, "if a government search is preceded by a private search, the government search does not implicate the Fourth Amendment as long as it does not exceed the scope of the initial private search." *Id.* at 11 (citing *Jacobsen*, *supra*, and *Walter v. United States*, 447 U.S. 649 (1980)). Because Google had identified petitioner's four files as having "matching hash values" to images that a Google employee had previously viewed and identified as child pornography, the government's "subsequent opening and viewing of the four photographs did not significantly expand on the search that had previously been conducted by Google." *Id.* at 18. Google's actions had "frustrated any expectation of privacy [petitioner] possessed in the four photographs." *Id* at 15. The government "gained no new material information by viewing the images." *Id.* at 17. The government's actions "merely confirmed Google's report that [petitioner] uploaded content constituting apparent child pornography." *Id*. at 17-18.

Petitioner argued that the government actions here resembled those that required a warrant before law enforcement could view the suspected pornographic films in *Walter v. United States*. Pet. App. 20. But the court of appeal noted important differences. *Id.* at 20-21. In *Walter*, the private party viewed only packaging and labels; a warrant was required because agents materially exceeded that search when they used a projector and viewed the images themselves for the first time. *Id.* at 21. Here, in contrast, "the information in the four images [was] exactly the same as what was previously

viewed by a Google employee." *Id.* Google and the agents had not relied merely on "file names." *Id.* Instead, Google "employ[ed] a much more sophisticated . . . process"—a "reliable and accurate method of identifying the actual contents of the files that were provided to the government" as "duplicates of images that a Google employee previously reviewed and identified as apparent child pornography." *Id.* at 21-22. Although "the agent learned more from his review of the pictures" than he did from simply reading the NCMEC report about the matching hash values, *id.* at 23, the agent did not learn anything that *Google* did not already know, *id.* at 24. "[T]he private party" had already seen those details during "the prior visual review of the identical images by a Google employee," and "the government's search did not exceed the private search." *Id.* Because "it was a private party, not the government, who searched and seized [petitioner's] property," the court of appeal also rejected petitioner's argument that a Fourth Amendment violation could be established here based on the theory that the government somehow "trespass[ed]" on petitioner's property. *Id.* at 25.

3. The California Supreme Court denied petitioner's petition for review without dissent. Pet. App. 50.

ARGUMENT

Until very recently, the unanimous view of appellate courts has been that police are not required to obtain a warrant before looking at electronic image files sent to them by a private service provider if the files' hash value

established to the provider that they contain duplicates of images that had been previously viewed by the provider's trained employees and classified by them as child pornography. The court below reached the same conclusion. That position is consistent with and compelled by this Court's precedent, including *United States v. Jacobsen*, 466 U.S. 109 (1984). As petitioner has noted, a recent Ninth Circuit opinion—involving petitioner's separate federal prosecution for possessing and distributing child pornography—reached a different conclusion. But that opinion does not create a need for further review in this case. The Ninth Circuit's analysis was based on a record that differed in significant respects from the record that led the lower courts in this case to uphold the search. And the Ninth Circuit's opinion—which took an idiosyncratic approach to the private-search question—is unlikely to lead to the risk of entrenched disagreement among lower courts that would merit this Court's immediate resolution. Moreover, the record in this case, along with evolution in law enforcement practices since the 2015 search that is here at issue, give reason to doubt that a decision in this case would be of practical importance either for petitioner himself or more broadly. The petition for certiorari should be denied.

1. The court of appeal correctly held that police did not violate petitioner's Fourth Amendment rights by opening and viewing the child pornography images that Google had sent to NCMEC.

a. The Fourth Amendment applies to intrusions by government actors. *See Burdeau v. McDowell*, 256 U.S. 465, 475 (1921). Under longstanding precedent, Fourth Amendment protections do not apply "'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government.'" *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). Petitioner does not argue that Google was acting as a government agent when it scanned and processed hash values for image files in his account. Nor does he argue that Google was acting as a government agent when it compared those hash values to its database, and observed from the exact match that the image files in petitioner's account contained duplicates of images that Google employees had seen and recognized as child pornography featuring a prepubescent child. Instead, petitioner argues solely that after Google employees took those steps, the government agents who received the report and files from Google (via NCMEC) violated the Fourth Amendment by printing and viewing the same images without a warrant.

The court of appeal correctly rejected that argument. As this Court has made clear, a private party's actions in conducting an initial search or seizure alter the Fourth Amendment restrictions that subsequently apply to the government, in accordance with 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." *Jacobsen*, 466 U.S. at 117.

In *Jacobsen*, Federal Express employees opened a damaged cardboard box and found crumpled newspaper covering a tube containing "four zip-lock plastic bags, the outermost enclosing the other three and the innermost containing about six and a half ounces of white powder." *Jacobsen*, 466 U.S. at 111. The employees put the plastic bags back inside the tube and placed the tube and newspapers back into the box, *id.*, such that this Court assumed the contents could not be seen from the outside, *id*. at 118 & n.15. Federal agents arrived, took the bags out of the tube, and viewed the white power. *Id*. at 111. They opened each bag, removed a trace of the white powder, and conducted a field test that confirmed the powder was cocaine. *Id*. at 111-112.

This Court held that the agents' actions were constitutionally permissible notwithstanding the absence of a warrant. "The initial invasions of [the] package were occasioned by private action," the Court observed, and "did not violate the Fourth Amendment because of their private character." *Jacobsen*, 466 U.S. at 115. Given that, the subsequent actions by the agents were all "reasonable for essentially the same reason": in each instance, the "federal agents did not infringe any constitutionally protected privacy interest that had not already been frustrated as the result of private conduct." *Id* at 118, 126; *see id.* at 115 ("The 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."). The Federal Express employees had already examined the packages' contents and told agents of their obviously illegal

character. Although the contents were hidden again by the time agents arrived, the agents learned nothing by opening the bags "that had not previously been learned during the private search," *id.* at 120, and "it hardly infringed respondents' privacy" for the agents to re-expose the contents for their own view, *id.* at 119. "The advantage the Government gained thereby was merely avoiding the risk of a flaw in the employees' recollection rather than in further infringing respondents' privacy." *Id.* at 119. The private employees' report about the packaging of the powder also "made it virtually certain that the substance tested was in fact contraband" which there was no legitimate interest in possessing, *id.* at 125, 123, and the field test could "reveal . . . no other arguably 'private' fact," *id.* at 123.

As the court of appeal recognized, *Jacobsen*'s analysis resolves this case. Pet. App. 13-18. A private actor (Google) scanned petitioner's four uploaded image files and recognized that the associated hash values matched those in Google's database of hash values corresponding to child pornography images. *See supra* p. 4. According to the unrebutted testimony at the suppression hearing and the trial court's findings, the matching hash values meant that there was no significant likelihood of the two files being anything other than an exact match.[8] That meant that Google employees had previously viewed

---

[8] *See* 1 Aug. RT 48 ("[t]he likelihood of any two files having the same mathematical hash value is almost inconceivable without the file being exactly the same."); *id.* (even a "small" change would change the hash value); *id.* at 50

the images and discerned their content. *See* 1 Aug. RT 73 (trial court's finding that there was a "virtual certainty that [the agent] could learn nothing that had not previously been learned during the private search by viewing the images"). When a government agent then printed and viewed those same files, the agent saw nothing that Google employees had not already seen. The agent's viewing simply allowed him to confirm that, as Google's report indicated, the images contained prepubescent child pornography—an item that (unlike adult obscenity) is illegal even to privately possess.[9] Nothing of a personal nature was revealed—the images, far from originating with the plaintiff, were duplicates of other people's child pornography that other people had previously circulated on the Internet and that Google had already encountered and viewed. Thus, even if the opening and viewing of those images by government agents were viewed as a search, *Jacobsen* establishes that petitioner's Fourth Amendment rights were not violated.[10]

("If the hash value is the same then those files should be identical."); *id.* at 73 (trial court's finding that "there's reliability based on the fact that hash values are like fingerprints"); *cf. United States v. Miller*, 982 F.3d 412, 433 (6th Cir. 2021) ("'[t]he chance of two files coincidentally sharing the same hash value is 1 in 9,223,372,036,864,775,808'").

[9] *See* 18 U.S.C. § 2252A(a)(5); *Osborne v. Ohio*, 495 U.S. 103 (1990) (government may outlaw private possession of child pornography but not adult pornography).

[10] Unlike the trial court, *see* 1 Aug. RT 70-71, the court of appeal did not address whether petitioner's reasonably expectation of privacy might have been lessened by Google's terms of service, *see* Pet. App. 16 n.10. Nor did it consider how petitioner's privacy or property interests were affected by Google's termination of his account. *See* 1 CT 197.

b. Petitioner argues that suppression was required under this Court's decision in *Walter v. United States*, 447 U.S. 649 (1980), which pre-dated *Jacobsen*. Pet. 12. To the extent petitioner relies on a two-Justice plurality in *Walter*, *see* Pet. 12-13, as opposed to the later opinion for the Court in *Jacobsen*, that in itself suggests the weakness of his approach. *See Jacobsen*, 466 U.S. at 115 (observing that "there was no single opinion of the Court" in *Walter*); *see also Walter*, 447 U.S. at 651 (plurality opn. of Stevens, J.) (noting that *Walter*'s opinions concerned "bizarre facts"). In any event, no conflict exists between this Court's decision in *Walter* and the decision below.

In *Walter*, employees of a private company opened a carton that had been shipped by an unknown sender and misdelivered to them. 447 U.S. at 651-652 (plurality opn. of Stevens, J.). Inside, they found boxed motion picture films. *Id.* The boxes had "suggestive drawings" and "explicit descriptions" on the outside. *Id.* at 652. The private employees did not view the films themselves to discern what the films in fact depicted. *Id.* at 652 & n.2 (noting that the films were too small to be examined without a projector). They called FBI agents, who took the films and viewed them with a projector. *Id.* at 652; *see id.* (noting that at least one film was first screened months later). Although no opinion was joined by a majority of Justices, a majority of the Court concluded that the motion to suppress should have been granted.[11]

---

[11] *See Walter*, 447 U.S. at 651 (Stevens, J., joined by Stewart, J.); *id.* at 660

But the rationale of the opinions concluding that suppression was warranted on the facts in *Walter* does not apply here. In *Walter*, "the private party had not actually viewed the films," and "could only draw inferences about what was on the films" based on suggestive labels on the boxes. 447 U.S. at 657 (Stevens, J.); *see id.* at 659 n.14. The Justices in the majority therefore decided nothing about what the outcome would be where a private party actually *had* seen the images or their exact copies. *See id.* at 657 n.9 ("we have no occasion to decide whether the government would have been required to obtain a warrant had the private party been the first to view them"). Here, in contrast, the government agent viewed images that Google had identified as hash-matched duplicates of images that its employees *had* already seen and identified as prepubescent child pornography.[12]

(noting Justice Marshall's concurrence in the judgment, without opinion); *id.* at 660 (White, J., concurring in part and concurring in the judgment, joined by Brennan, J.); *but see id.* at 662 (Blackmun, J., dissenting, joined by Burger, C.J., and Powell and Rehnquist, JJ.).

[12] Petitioner appears to accept that if Google employees had taken steps to view the images again upon their detection in his account, the agent's subsequent actions would give rise to no Fourth Amendment claim. Some service providers may indeed instruct their employees to re-view files. 1 Aug. RT 26. Others, however, may prefer to limit the number of times non-law-enforcement personnel view images depicting the sexual abuse of young children, for very good reasons. *See, e.g.*, Effective Child Pornography Prosecution Act of 2007, Pub. L. No. 110-358, Tit. I, § 102(3), 122 Stat. 4001, 4001 (congressional finding that a child pornography victim is "revictimize[d] . . . each time the image is viewed"); Adam Walsh Child Protection and Safety Act of 2006, Pub. L. No. 109-248, § 501(2)(D), 120 Stat. 587, 624 (finding that "[e]very instance of viewing images of child pornography represents a renewed violation of the privacy of the victims and a repetition of their abuse").

c. Petitioner also argues that although the hash match shows there was a "numerical sameness" between petitioner's attachments and the prior images reviewed by Google, that match did not prove "the Google employee's correctness in first identifying and categorizing the information as 'A1'." Pet. 10. That argument is unpersuasive. To begin with, it understates the reliability of Google's classification of the images—which were made by employees who worked at a reputable technology company and were specifically trained to recognize child pornography. *See* 1 CT 196; *infra* p. 23 & n.17. More importantly, the application of the *Jacobsen* doctrine does not turn on whether the private party is correct about the conclusions it draws from its intrusion on the defendant's privacy interests; it turns on "the degree to which" the government "exceeded the scope of the private search." *Jacobsen*, 466 U.S. at 115. Once Google's hash technology identified the four files as containing duplicates of images that its trained employees had already viewed and recognized as prepubescent child pornography, the government agent's subsequent viewing of the same images was not a new intrusion on Fourth Amendment interests but rather a confirmation that the private employees had accurately classified what they saw—prohibited images of child sexual abuse. *See supra* pp. 13-14.[13] "Protecting the risk of misdescription [would]

---

[13] *Cf. Jacobsen*, 466 U.S. at 123 ("Congress has decided—and there is no question about its power to do so—to treat the interest in 'privately' possessing cocaine as illegitimate; thus governmental conduct that can reveal whether a substance is cocaine, and no other arguably 'private' fact, compromises no legitimate privacy interest.").

hardly enhance[] any legitimate privacy interest," and petitioner's interest in preventing the confirmation of his privately detected illegal activity is "not protected by the Fourth Amendment." *Jacobsen,* 466 U.S. at 119.

2. a. The decision below aligns with what was, until recently, the unanimous view of appellate courts. For instance, in *United States v. Reddick,* 900 F.3d 636 (5th Cir. 2018), *cert. denied*, 139 S. Ct. 1617 (2019) (No. 18-6734), Microsoft's hashing technology identified a user's files as matching "known images of child pornography," and Microsoft sent a report and copies of the files to police via NCMEC. *Id.* at 638. Without obtaining a warrant, a police detective opened the files and confirmed that each image was child pornography. *Id*. The Fifth Circuit affirmed the denial of suppression because the opening of the files by the detective constituted "no 'significant expansion of the search that had been conducted previously by a private party' sufficient to constitute 'a separate search.'" *Id.* at 639. The detective's visual review of the suspect images—"which merely dispelled any residual doubt about the contents of the files"—was "akin to the government agents' decision to conduct" a field test on the white powder in *Jacobsen*. *Id.* And "[a]s in *Jacobsen*," "'the suspicious nature of the material made it virtually certain that the substance tested was in fact contraband.'" *Id.*

Similarly, in *United States v. Miller*, 982 F.3d 412 (6th Cir. 2020), *cert. denied*, 141 S. Ct. 1797 (2021) (No. 20-1202), Google detected that hash values for files uploaded by the defendant matched hash values in its child

pornography database. *Id.* at 420. Google sent the images to NCMEC, which sent them to police. *Id.* An officer viewed the images with the matching hash values, confirmed that they depicted pre-pubescent children engaged in sex acts, and used the information to obtain search warrants for the email account and the defendant's home. *Id.* Like the lower courts here, the Sixth Circuit upheld the governmental search because it did not exceed the scope of Google's earlier private search. *Id.* at 427-430 (applying *Jacobsen*). *See also United States v. Ringland*, 966 F.3d 731, 737 (8th Cir. 2020), *cert. denied*, 141 S. Ct. 2797 (No. 20-1204) (reasoning that the government "did not expand the search beyond Google's private party search" where the government "searched only the same files that Google searched").[14]

b. As petitioner has noted (by letter dated September 21, 2021), this authority is no longer unanimous because of the new Ninth Circuit opinion in petitioner's appeal of his federal convictions. *See United States v. Wilson*, 13 F.4th 961 (9th Cir. Sept. 21, 2021). That opinion involved petitioner's conviction for receiving and possessing child pornography images other than

---

[14] The petition describes a district court case, *United States v. Keith*, 980 F. Supp. 2d 33 (D. Mass. 2013), as conflicting with the court of appeal decision here. Pet. 17. But the portions of the district court opinion on which petitioner relies not only were dicta—as petitioner acknowledges—but also addressed facts differing markedly from those here. *See, e.g., Keith*, 980 F. Supp. 2d at 37 & n.2 (noting that the service provider in *Keith* did not know "how the file came to be originally hashed and added to [its] database," and that the hash value could have been received from another company without an AOL employee viewing the files).

those involving J.A.'s relatives. The Ninth Circuit concluded that the agent's examination of the images from Google required a warrant. While that decision concerned the same government actions as the decision here, it involved a record that differed in certain critical respects.

The Ninth Circuit was "contingently" concerned that the government had "failed to carry" its burden of establishing that hashing technology reliably indicated matching images after petitioner had "challenge[d] the 'accuracy and reliability' of Google's hashing technology in the district court" in his federal case. *Wilson,* 13 F.4th at 979.[15] In this case, however, the government provided evidence not only from the agent who examined petitioner's images but also from a computer forensics agent. 1 Aug. RT 45-59. That specialist—who did not testify at the suppression hearing in the federal case—explained that the likelihood of two files having the same hash match but being different was "almost impossible." *Id.* at 48-49; *see id.* (estimating the odds against non-identical files having the same hash value as "something like 340 billion, billion, billion, billion to one"). And the state trial court made a factual finding of the hashing technology's "reliability." *Id.* at 73. Unlike in the federal case, therefore, the record in this case factually established that the images attached

---

[15] The Ninth Circuit had received an amicus brief from Google explaining the "vanishingly small risk" of a false match. Br. of Google LLC et al., as Amici Curiae, *United States v. Wilson*, No. 18-50440 (9th Cir.), at 9. But the Ninth Circuit focused on the lack of competent evidence introduced on that point at the suppression hearing itself. *See Wilson*, 13 F.4th at 979.

to petitioner's email were reliably identical to ones Google employees had already seen—an important step in establishing, for purposes of the analysis required by *Jacobsen*, that the agents did not see significantly more than the private party.

With respect to the law, the Ninth Circuit's decision is incorrect—and is a clear outlier compared to the weight of authority described above. The Ninth Circuit concluded that the government exceeded the scope of Google's private search because the government learned "new" information that it used "first to obtain a warrant and then to prosecute [petitioner]." *Wilson*, 13 F.4th at 972. The court primarily focused on a "gap" between what Google's CyberTip reported and the information that the agent who viewed the pictures chose to include in his warrant application: the CyberTip stated only that the pictures were prepubescent child pornography, whereas the warrant application briefly described the children and sexual activity. *See, e.g., id.* (quoting warrant application's description that one photo depicted two naked five-to-nine year old girls, one of whom had her vagina exposed and the other of whom had her face in the genital region of an adult). But the Ninth Circuit's analysis focused on the wrong part of Google's report. The relevant part of the report conveyed that Google's employees had determined that each image was of a prepubescent minor involved in a sex act—which would be equally true of the original image viewed as of any subsequent duplicate identified through the hash-matching technology. 1 CT 196-197, 212-213; 1 Aug. RT 57-58. That

previous viewing, moreover, exposed to the private party everything that the agent saw; as in *Jacobsen*, there was a "virtual certainty" that the investigator's search here would disclose nothing more than what a Google employee had earlier viewed. 466 U.S. at 119; *see* 1 CT 196 (Google employee's declaration that "[n]o hash is added to our repository without the corresponding image first having been visually confirmed by a Google employee"). This case thus bears no comparison to *Walter*, where the private party had not viewed the motion pictures at any point and the agent's screening revealed new information.[16]

For similar reasons, the Ninth Circuit was wrong to view Google's classification of the images as "A1" as analogous to the labels on the films in *Walter*. "The boxes describing the films in *Walter* suggested that the images on the films were obscene." *Wilson*, 13 F.4th at 973. Agents could not know who had placed the labels or drawings, whether those markings might have been a joke or marketing gimmick, or even that they were definitively intended to state (rather than "suggest[]") that the contents were obscene. Here, the classification as "A1" came from a known entity whose protocols and practices

---

[16] The Ninth Circuit also found it significant that further information about the images beyond the Google employee's classification of them as "A1" was needed to share with the fact-finder in order to obtain a conviction. 13 F.4th at 973. That reasoning was wrong, and it is not relevant here in any event. The federal child pornography indictment and conviction were based on images beyond the four in the CyberTip. And petitioner's state-court convictions for the molestation of J.A.'s relatives did not depend on those four images at all.

were well known to the agents, based on the work of employees who had been specially trained on the definition and recognition of child pornography. And the classification was made precisely for the purpose of identifying illegal child pornography—an effort that, according to a Google representative's declaration, the company viewed as "critically important" to its business. 1 CT 196.[17] The classification "A1" thus reliably informed agents (rather than "suggested") that the images depicted prepubescent children engaged in sexual activity as defined by federal law, such that the mere possession of those images was entirely illegal. *See* Pet. App. 21-22 ("[u]nlike the private party in *Walter*, Google used a reliable and accurate method of identifying the contents of the files that were provided to the government—all four images were duplicates of images that a Google employee previously reviewed and identified as apparent child pornography"). The Ninth Circuit's contrary reasoning—which contravenes not only this Court's precedent but the decisions of every other appellate court to have considered a similar question—is unlikely to persuade other courts or give rise to an entrenched circuit split.

3. Petitioner additionally contends (Pet. 19-26) that this Court should grant certiorari to address whether the agent's examination of images from

---

[17] *See also* 1 CT 196 (describing Google's "strong business interest" in ensuring that its products are free of "child sexual abuse material": "If our product is associated with being a haven for abusive content . . . users will stop using our services. Ridding our products and services of child abuse images is critically important to protecting our users, our product, our brand, and our business interests.").

petitioner's email account constituted a trespass on petitioner's property requiring a warrant under *United States v. Jones*, 565 U.S. 400 (2012). Review of that question is also unwarranted.

As an initial matter, during the suppression proceedings in the trial court, petitioner at most briefly raised the argument in his reply brief. Supp. CT 24-26.[18] He did not raise the trespass theory or cite *Jones* in his motion to suppress, Supp. CT 5-9, or discuss it at the suppression hearing, 1 Aug. RT 65-69. As a result, there was no evidence at the trial court relating to the issue. Petitioner's actions deprived both the court of appeal and this Court of the factual findings and specific evidence that would be pertinent to the issue, making this an exceptionally poor vehicle for addressing the question.[19]

In any event, petitioner's trespass theory is unsupportable on the merits. *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, in the government's efforts to

---

[18] Under California law, discussing the issue only in the trial court reply brief was not sufficient to raise and preserve the issue. *See Schram Constr., Inc. v. Regents of Univ. of California*, 187 Cal. App. 4th 1040, 1052 n.7 (2010) (failure to raise argument until reply brief at trial court is forfeiture).

[19] The court of appeal rejected petitioner's trespass theory based on its private-search holding under *Jacobsen*, Pet. App. 25, so it did not need to consider how particular features of petitioner's Gmail account might bear on the appropriateness of petitioner's attempted analogy to physical trespass.

obtain information, it had "*physically* occupied private property"—a car. *Id.* (emphasis added). 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. But the Court did not extend that holding beyond "physical intrusion," *id.* at 407, to encompass electronic searches of third-party data. *See id.* at 412 (noting that the decision did not purport to "answer th[e] question" whether surveillance "through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy"). When the Court did address electronic surveillance in a later case, *Carpenter v. United States*, 138 S. Ct. 2206 (2018), it applied a reasonable-expectation-of-privacy approach—not the trespass theory from *Jones*—in determining that the government's acquisition of historical cell-site location information created and maintained by a cell-service provider is a Fourth Amendment search. *See id.* at 2217 & n.3.

And even if petitioner had supplied evidence showing that certain features of Gmail supported his attempt to analogize viewing electronic images in an account to a physical trespass, *Jones* would not cast doubt on the decision below. Petitioner does not dispute Google's authority to send the files to NCMEC or NCMEC's authority to send the files to the police. He therefore lacks 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 (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.").[20]

Indeed, petitioner identifies no court that has accepted his trespass theory in any similar context. The Ninth Circuit's decision in petitioner's federal case expressly declined to reach the argument. *Wilson*, 13 F.4th at 967 n.7. And although the petition (at p. 21) cites *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), that decision does not aid him.

In *Ackerman*, an America Online (AOL) user sent an email with four attachments. Just one of the attachments was revealed by hash technology to be a match to an image that AOL employees had previously viewed and determined to be child pornography. *Ackerman*, 831 F.3d at 1294. But after AOL forwarded the entire email (including all four attachments) to NCMEC, a NCMEC employee opened and examined not only the hash-match file, but also

---

[20] Possession of child pornography images also differs from possession of the physical property in *Jones*, in that the intrusion in *Jones* was on a car (which a person may legally possess or control) whereas any intrusion here was only as to identified images of a third party's sexual abuse of prepubescent children (which a person may not legally possess or control). *See supra* p. 14 n.9. Agents did not receive or view anything that petitioner might legally possess—such as the text of petitioner's email or images that Google had not specifically identified as child pornography—until after they applied for and received a warrant. *See supra* pp. 4-5, 7.

the email text and the other three attachments, all without receiving a warrant. *Id.* The Tenth Circuit held that the NCMEC employee was acting as a government agent and suppressed the search. *Id.* at 1295. Here, petitioner forfeited below—and does not raise now—any argument that NCMEC was acting as a government agent.[21] In any event, *Ackerman* made clear that the need to suppress evidence in that case was based on the government agents' opening of the email and attachments that did *not* have hash values identical to items AOL employees had previously examined and determined to be child pornography. *See id.* at 1306-1307 ("[O]pening the email and viewing the [other] three attachments . . . was enough to risk exposing private, noncontraband information that AOL had not previously examined."). Because *Ackerman* did not state that a similar conclusion would have resulted if the government agent had "accessed (only) the (one) attached image with the matching hash value," *id.* at 1306, it creates no conflict with the decision here or any other appellate decision of which the State is aware. Indeed, this Court

---

[21] The lower court observed that petitioner had not argued that NCMEC was a government agent. Pet. App. 15 n.9. Petitioner disagrees, quoting 10 words from his reply brief in the court of appeal that he contends raised the issue. Pet. 15 n.7. But that would not establish preservation under California law. *People v. Rangel*, 62 Cal.4th 1192, 1218 (2016) ("'Obvious reasons of fairness militate against consideration of an issue raised initially in the reply brief.'"). In any event, his certiorari petition does not argue that NCMEC was a government agent, and the question presented (Pet. i) does not mention NCMEC at all.

has recently denied other petitions for certiorari raising the same issue.[22] Petitioner identifies no persuasive reason for a different result here.

4. Finally, a realistic look at the context of this dispute reveals that the issues are of limited and diminishing importance. Petitioner argues that "billions of Gmails are now vulnerable to subsequent government searches without constitutional protection." Pet. 19. But that ignores both the limits of the court of appeal's decision and the real-world context of this case. The decision addresses only the warrantless viewing of an image file with a hash value identical to one that has already been viewed by trained personnel at an electronic service provider and identified as child pornography. Nothing in the decision below allows law enforcement to view an email's text without a warrant, or to view image files that have not been assigned such a unique hash value based on a prior review.

In any event, the actions by Google and law enforcement that gave rise to this case took place in 2015. Pet. App. 6.[23] As the record in this case establishes, the task force that investigated petitioner had already changed its practices by the time petitioner's motion to suppress was heard in 2017. Now, when an electronic service provider such as Google has not viewed the images

---

[22] *See Ringland*, 141 S. Ct. 2797 (2021); *Miller*, 141 S. Ct. 1797 (2021).

[23] Other reported cases concerning similar processes concern similarly dated searches. *See Miller*, 982 F.3d at 420 (2015 search); *Reddick*, 900 F.3d at 638 (2015 search); *Ringland*, 966 F.3d at 733 (2017 search).

contained in a CyberTip, the images arrive at the ICAC "in a locked fashion," and are unlocked only once a search warrant is obtained. Pet. App. 8; 1 Aug. RT 24-27.

Indeed, this Court's resolution of the questions presented might not even have a substantial effect with respect to petitioner himself. Unlike in the federal case, *see Wilson*, 13 F.4th at 966 & n.4, in this case the State has preserved the argument that the agents who viewed the image files acted in good faith and an objectively reasonable manner. *See* 1 CT 185-187 (raising good-faith arguments); *United States v. Herring*, 555 U.S. 135, 141-146 (2009). If this Court were to rule that a warrant should have been obtained, the good-faith arguments for not suppressing evidence would be strong. *See* 1 Aug. RT 28-29 (noting that warrant application, which stated that the agent had viewed the images without mentioning a prior warrant, was approved by judge after review by district attorney's office); 1 CT 243-244; *supra* pp. 18-19 (noting numerous appellate cases approving of the process used here). The State also argued below that much of the evidence against petitioner could not be suppressed as the fruit of the agent's viewing of the four image files because of intervening events, such as petitioner's abandoning the backpack that contained a thumb drive with thousands of images of child pornography by throwing it over a balcony. 1 CT 189. Those arguments mean that even a ruling in petitioner's favor from this Court would be unlikely, ultimately, to change the result in his case.

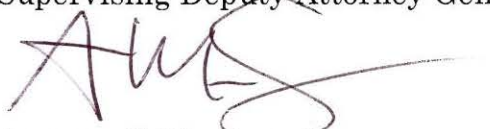
CONCLUSION

The petition for a writ of certiorari should be denied.

Dated: November 29, 2021

Respectfully submitted,

ROB BONTA
Attorney General of California
MICHAEL J. MONGAN
Solicitor General
LANCE E. WINTERS
Chief Assistant Attorney General
JOSHUA A. KLEIN
Deputy Solicitor General
ARLENE A. SEVIDAL
Supervising Deputy Attorney General



ANDREW S. MESTMAN
Deputy Attorney General