In the United States Court of Appeals for the Second Circuit

AUGUST TERM 2023

No. 23-6181-cr

UNITED STATES OF AMERICA,
Appellee,

v.

RYAN M. MAHER,
Defendant-Appellant,

On Appeal from the United States District Court
for the Northern District of New York

ARGUED: MAY 15, 2024
DECIDED: OCTOBER 30, 2024

Before: RAGGI, CHIN, and PÉREZ, *Circuit Judges*.

Defendant Ryan M. Maher appeals his conviction in the United States District Court for the Northern District of New York (Suddaby, *J.*) on charges of receiving and possessing child pornography. Maher argues that the district court erred in relying on the "private search" doctrine to deny his motion to suppress evidence that was obtained by, or that is the fruit of, a warrantless visual police search of a digital file that Maher uploaded to his Google email account. We agree.

Without itself ever visually examining the contents of Maher's uploaded file, Google reported that it contained child pornography because the hash value for the image contained therein matched the hash value that Google had assigned an image previously located in another file, which image a Google employee or contractor had visually examined and identified as child pornography. In these circumstances, neither the private search doctrine relied on by the district court nor the Google Terms of Service agreement cited by the government supports the challenged warrantless search. That, however, does not mean that Maher is entitled to relief from conviction. As the district court correctly ruled in the alternative, the good faith exception to the exclusionary rule supports denial of Maher's suppression motion because, at the time authorities opened his uploaded file, they had a good faith basis to believe that no warrant was required.

AFFIRMED.

MELISSA A. TUOHEY, Assistant Federal Public Defender, Office of the Federal Public Defender, Syracuse, NY, *for Defendant-Appellant*.

MICHAEL D. GADARIAN, Assistant United States Attorney, *for* Carla B. Freedman, United States Attorney for the Northern District of New York, Syracuse, NY, *for Appellee*.

REENA RAGGI, *Circuit Judge*:

Defendant Ryan M. Maher stands convicted following a guilty plea in the United States District Court for the Northern District of New York (Glenn T. Suddaby, *Judge*) of both receiving and possessing approximately 4,000 images and five videos depicting child pornography. *See* 18 U.S.C. § 2252A(a)(2)(A), (a)(5)(B), (b)(1)-(2). Sentenced to a total 294 months' incarceration and life supervised release, Maher now appeals from his February 9, 2023 judgment of conviction, arguing that the district court erred in relying on the "private search" doctrine to deny his motion to suppress evidence that was obtained by, or that is the fruit of, a warrantless visual police search of a digital file that Maher uploaded to an email account that he maintained with Google (the "Maher file"). *See* Decision and Order, *United States v. Maher*, No. 21 Cr. 275 (N.D.N.Y Aug. 22, 2022), ECF No. 48. We agree.

No one at Google visually examined the contents of the Maher file before reporting it to the National Center for Missing and Exploited Children (the "NCMEC") as "apparent child pornography." App'x 29. Rather, that report was based on a computer-conducted algorithmic search of the Maher file, which identified a match between the hash value for the image contained in the Maher file (the "Maher file image") and the hash value of an image (the "original file image") that Google had earlier located in another file (the "original file").[1] Thus, when law enforcement authorities

[1] A "hash" or "hash value" is "(usually) a short string of characters generated from a much larger string of data (say, an electronic image) using an algorithm—and calculated in a way that makes it highly unlikely another set of data will produce the same value." *United States v. Ackerman*, 831 F.3d 1292, 1294 (10th Cir. 2016) (Gorsuch, *J.*).

visually examined the contents of the Maher file, they went beyond the scope of Google's private algorithmic search in that they learned more than the hash value for the Maher file image; they learned exactly what was depicted in that image.[2]

Nor is a different conclusion warranted because, before assigning a hash value to the original file image, a Google employee or contractor had visually examined that file image and determined that it depicted child pornography. That visual examination was not a private search that extinguished any of Maher's Fourth Amendment rights because such rights are personal, and Maher had no reasonable expectation of privacy in the original file, which did not belong to him. But just as Maher could not challenge any search of the original file, so the government cannot argue that Google's visual examination of the contents of that file extinguished Maher's Fourth Amendment rights as to a file—the Maher file—in which he did have a privacy interest and whose contents were never visually examined but only hash matched by Google.

In these circumstances, Google's hash match may well have established probable cause for a warrant to allow police to conduct a visual examination of the Maher file. But, for reasons stated in this opinion, we conclude that neither the private search doctrine relied on by the district court nor the Google Terms of Service agreement cited by the government

[2] Google apparently does not retain images determined to depict child pornography after assigning them a hash value. Thus, Google did not—and could not—report to the NCMEC what specifically was depicted in either the Maher file image or the original file image based on their matching hash value.

authorized the police to open the Maher file and to conduct such a visual examination of its contents without a warrant.

That, however, does not mean that Maher is entitled to relief from conviction. As the district court correctly recognized in the alternative, the good faith exception to the exclusionary rule defeated Maher's suppression motion because, at the time police opened the Maher file and visually inspected its contents, they had a good faith basis to believe that no warrant was required to do so. Accordingly, on that basis, we affirm the judgment of conviction.

BACKGROUND

I. Google's Use of Hash Values To Identify Child Pornography

While the facts relevant to this appeal are not disputed, their discussion requires some understanding of how Google identifies and reports child pornography found on its platform. In this case, that understanding derives largely from a declaration filed with the district court by Claire Lilley, a Google Manager for Child Safety and Abuse Enforcement. Lilley states that, consistent with Google's "strong business interest" in "ensuring its services are free of illegal content," the company's "Terms of Service" prohibit persons from using Google's services "in violation of law." App'x 108.[3] These Terms of Service advise users that Google "may review content" on its platform "to determine whether it is illegal or violates our policies," and "may remove or refuse to display content that we reasonably believe violates our policies or the law." *Id.* at 113–14. In the very next

[3] Google's Terms of Service make this point in the affirmative rather than the negative: "You may use our Services only as permitted by law." *Id.* at 113.

sentence, Google states: "But that does not necessarily mean that we review content, so please don't assume that we do." *Id.* at 114. The Terms of Service also state that Google "may . . . report" a detected "violation [of law or its policies] to appropriate authorities." *Id.* at 142. Elsewhere, they state that Google "will share personal information outside of Google" where necessary to "[m]eet any applicable law . . . or enforceable governmental request." *Id.* at 131.

As Lilley further explains, Google uses "a proprietary hashing technology" to monitor its platform for "apparent child sexual abuse material." *Id.* at 109. Toward this end, certain Google employees and contractors are "train[ed] . . . on how to recognize" child pornography. *Id.*[4] When, based on a visual inspection, such an employee or contractor identifies material on the company's platform as child pornography, Google gives the image "a digital fingerprint" known as a "hash" or "hash value." *Id.* The company then apparently removes the image from its platform but adds the image's hash value to a "repository of hashes of apparent child pornography" maintained by the company. *Id.* Google's computers can then automatically compare the hash values of content later uploaded to its platform to such stored hash values and thereby digitally "identify exact or very similar images of apparent child pornography." *Id.*

[4] On this point, Lilley states that, "[u]nder guidance of its lawyers, Google trains Google Reviewers on the legal obligation to report such material, on the statutory definition of child pornography, and on how to recognize it on our products and services." *Id.* She does not state what, if any, particular findings Google requires reviewers to make in identifying child pornography. Nor does she identify the Google employee or contractor who identified the original file image in this case as child pornography.

Google reports such hash matches to the NCMEC by filing a CyberTipline Report.[5] Before doing so, a Google employee or contractor will sometimes conduct a "manual, human review" of the hash matched image to confirm that it depicts child pornography. *Id.* at 110. But in many cases—as here—Google "automatically reports" the computer matched image to the NCMEC as "apparent child pornography" without any person viewing it. *Id.* In those cases, Google advises the NCMEC that the report is based on a hash match to an image previously viewed by a Google employee or contractor and identified as "apparent child pornography." *Id.* at 29. Because Google apparently does not retain the previously viewed image, it cannot, based only on a hash match, describe the specific contents of either matched file, *i.e.*, it cannot describe the age of any child depicted, the number of children depicted, whether any adults are also depicted, or the particular circumstances depicted that might be deemed child pornography. *See* Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38, 40 (2005) (explaining that "[o]ne can calculate a hash value from input, but cannot derive the input from the hash value," such that hash value of photograph "cannot be 'reversed' to generate the photo itself").

---

[5] The NCMEC is an entity "organized as a private nonprofit but established by Congress," *United States v. Johnson*, 93 F.4th 605, 609 (2d Cir. 2024), and "statutorily obliged to operate the official national clearinghouse for information about missing and exploited children," *United States v. Ackerman*, 831 F.3d at 1296. Although the law does not mandate that electronic communication service providers such as Google "affirmatively search, screen, or scan" for images of child sexual exploitation found on their platforms, *see* 18 U.S.C. § 2258A(f)(3), it does require them to report such images to the NCMEC through its CyberTipline once they have "actual knowledge" that such material resides on their platforms, *id.* § 2258A(a)(1)(A), (B).

II. Maher Uploads Child Pornography to His Google Account

On January 27, 2020, Ryan Maher uploaded the Maher file to one of his Google email accounts. Using its hash algorithm, a Google computer determined that the Maher file contained an image whose hash value matched the hash value—2eb373380383f50820e648d1c304a3db—that Google had earlier assigned to an image found in the original file, which a Google employee or contractor had visually examined and identified as depicting child pornography.

On January 28, 2020, Google transmitted the Maher file to the NCMEC, reporting it as "apparent child pornography." App'x 29. In response to a question on the NCMEC CyberTipline Report form asking whether Google had viewed the "entire contents" of the reported file, the company answered: "No." *Id.* at 31. Google further explained that such a response "means that while the contents of the [reported] file were not reviewed concurrently to making the report, historically a person had reviewed a file whose hash (or digital fingerprint) matched the hash of the reported image and determined it contained apparent child pornography." *Id.* at 29.

Google further advised the NCMEC that the reported file had been uploaded to email address newbennings8608@gmail.com, which was registered to Ryan Maher, and which had a secondary email address of newbeginnings8608@gmail.com. Google further provided the NCMEC with a mobile phone number associated with the account, as well as with IP addresses from which the accounts had recently been accessed and associated geographical coordinates.

III. New York State Police Investigation of Maher

After receipt of Google's report, the NCMEC also did not open the Maher file or visually examine its contents. Rather, almost two months later, on March 16, 2020, the NCMEC sent Google's report and the unopened Maher file to the New York State Police, describing it as "Apparent Child Pornography (Unconfirmed)." *Id.* at 27.

The State Police did not replicate Google's algorithmic search of the Maher file. Nor did they replicate Google's visual search of the original file image that was hash matched to the Maher file image by the algorithmic search—something that was no longer possible.[6] Rather, without obtaining a search warrant, State Police Investigator Laura Croneiser opened the Maher file and visually examined its contents, a search never conducted by Google. She reported what she saw—"a prepubescent female, who appears approximately six to seven years old, exposing her vagina,"—in a July 21, 2020 affidavit submitted to a state court judge in support of a warrant to search Maher's newbennings8608@gmail.com and newbeginnings8608@gmail.com email accounts. *Id.* at 44–46. In explaining how police came to view the contents of the Maher file, Investigator Croneiser stated that on "January 28, 2020, Google reported to the [NCMEC]" that the newbennings8608@gmail.com account had "uploaded an image of child pornography on January 27, 2020," which image was "stored in the Google Gmail infrastructure." *Id.* at 44. She did not state that Google's report of child pornography was based solely on a computer match of hash values made by a computer and not any human visual examination of the Maher file image.

---

[6] *See supra* note 2.

Upon issuance of the requested warrant, State Police searched the two email accounts and confirmed that they belonged to Maher. Also, in searching the newbennings8608@gmail.com account, police found the same Maher file reported by Google to the NCMEC, containing the same image of child pornography visually examined by Investigator Croneiser.

Using the totality of information thus learned, State Police then sought and obtained a second warrant to search the residence where Maher was then living with his grandparents, including any electronic devices found therein. That warranted search resulted in the seizure of the approximately 4,000 images and five videos of child pornography charged in the counts of conviction.

IV. Procedural History

Following these seizures, federal authorities filed child pornography charges against Maher in the Northern District of New York. On August 17, 2021, Maher waived indictment and pleaded guilty to two counts of receiving and possessing child pornography. 18 U.S.C. § 2252A(a)(2)(A), (a)(5)(B), (b)(1)-(2). Several months later, the district court granted Maher leave to withdraw his guilty plea based on defense counsel's belated realization that Maher had a colorable basis to move for suppression of the seized evidence.

In so moving, Maher argued that the State Police had violated the Fourth Amendment by conducting a warrantless search of the Maher file, and then relying on the tainted fruits of that search to obtain search warrants for his email accounts, residence, and computers. The government opposed the motion on the grounds that (1) Maher lacked a reasonable expectation of privacy in the Maher file because Google's Terms of Service expressly

reserved the right to monitor users' accounts for illegal material and to inform law enforcement when such material is found; (2) under the private search doctrine, State Police did not need a warrant to open the Maher file; and (3) even if a warrant were required, suppression is properly denied under the good faith exception to the exclusionary rule.

In a written opinion dated August 22, 2022, the district court denied Maher's suppression motion. *See* Decision and Order, *United States v. Maher*, No. 21 Cr. 275, ECF No. 48. Finding it unnecessary to hold a hearing because the parties did not dispute the relevant facts, *id.* at 14, and without deciding whether Maher had a reasonable expectation of privacy in the Maher file, the district court held that the police's warrantless search of that file was lawful under the private search doctrine, which authorizes a government actor to repeat a search already conducted by a private party without securing a warrant. *See id.* at 21–29.

In so ruling, the district court determined that Google had conducted a private search of the Maher file before turning it over to the NCMEC, which therefore permitted the New York State Police to conduct a warrantless review of that same file. Maher had urged otherwise, arguing that no Google employee had ever opened or visually examined the contents of the Maher file, as Inspector Croneiser subsequently did. The district court was not persuaded, observing that the private search doctrine applies so long as the challenged government search "was 'of no greater scope or intensity than' Google's review of the image." *Id.* at 25 (quoting *United States v. $557,933.89, More or Less, in U.S. Funds*, 287 F.3d 66, 87 (2d Cir. 2002) (Sotomayor, *J.*)). The district court held that was the case here because a Google employee or contractor had "viewed the image at issue in this action in the past" (*i.e.*, when the employee or contractor viewed the contents of

the original file); determined "the image depicted child pornography"; "assigned [that image] a unique hash value that was added to Google's repository"; and matched that hash value to the Maher file image. *Id.* at 25–26. In these circumstances, the district court concluded that, when police opened the Maher file, there was a "virtual certainty" that what they would see "would be child pornography." *Id.* at 28.[7] Nor was the district court persuaded otherwise by Maher's argument that the police would "inevitably learn[] more from opening the image" in the Maher file than Google had learned from the hash match. *Id.* at 26. The court reasoned that "Google had previously viewed the image" to which it assigned the hash value matching the image in the Maher file, which was sufficient to "frustrate[]" Maher's "expectation of privacy in the image." *Id.*

Alternatively, the district court held that the good faith exception to the exclusionary rule defeated Maher's suppression motion because, when Investigator Croneiser opened the Maher file, she had an objectively good faith basis to believe that no warrant was necessary. *See id.* at 29–31.

Following this ruling, Maher again pleaded guilty to charges of receiving and possessing child pornography, reserving his right to appeal

[7] The district court supported that conclusion by citing out-of-circuit cases recognizing hash values to be "specific to the makeup of a particular image's data," *id.* at 29 (quoting *United States v. Reddick*, 900 F.3d 636, 639 (5th Cir. 2018)), and "the chance of two [digital] files coincidentally sharing the same hash value is 1 in 9,223,372,036,854,775,808," *id.* (quoting *United States v. Miller*, 982 F.3d 412, 430 (6th Cir. 2020)). In those cases, however, record evidence was offered to support these conclusions. By contrast, here, the government appears not to have offered any evidence as to the reliability of Google's particular hash matching technology.

the denial of his motion to suppress. *See* Fed. R. Crim. P. 11(a)(2). After sentencing and entry of judgment, Maher timely filed this appeal.

DISCUSSION

I. Standard of Review

On appeal from the denial of a motion to suppress, we review a district court's findings of fact for clear error and its legal rulings *de novo*. *See United States v. Haak*, 884 F.3d 400, 408 (2d Cir. 2018). Because the parties here do not dispute relevant facts, but only the lawfulness of police searches, our review is *de novo*.

II. Warrantless Search of the Maher File

Maher's search challenges are based on a common argument: that the police's initial warrantless visual examination of the contents of the Maher file violated the Fourth Amendment. We agree.

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. As the Supreme Court has recognized, "warrantless searches" of a person's papers or effects are "presumptively unreasonable" and, thus, violative of the Fourth Amendment, *United States v. Jacobsen*, 466 U.S. 109, 114 (1984), at least insofar as the person has a "reasonable expectation of privacy" in his property, *United States v. Jones*, 565 U.S. 400, 406 (2012). At the same time, the Court has recognized certain "well-delineated exceptions" to the warrant requirement. *United States v. Lewis*, 386 F.3d 475, 481 (2d Cir. 2004). This case involves one such exception: the private search doctrine.

The private search doctrine instructs that where a private party has already searched property belonging to another person, government authorities may repeat that search without a warrant so long as they do "not exceed the scope of the private search." *United States v. Jacobsen*, 466 U.S. at 116. Applying that doctrine to the particular circumstances of this case, we conclude that Google's use of its proprietary hashing technology to identify the contents of the Maher file as "apparent child pornography," App'x 29, did not permit State Police thereafter to conduct a warrantless visual examination of that contents. Such an examination did not simply replicate Google's own algorithmic search of the Maher file for a hash match, but expanded on it in a way not employed by Google, *i.e.*, human visual inspection, which allowed the police to learn more than Google had learned. Specifically, Google's use of its hashing technology to search the Maher file revealed only that the numerical hash value for its contents matched the numerical hash value for an image previously located in another file, which image a Google employee or contractor had then visually examined and identified as child pornography. But a computer's discovery of a hash match in the Maher file revealed nothing, either to Google or to those with whom it shared the match, about what in particular the image depicted (or even what the original file image depicted). To obtain that specific information about the Maher file image—which was "more than [police] already had been told" by Google or the NCMEC—authorities needed to exceed the scope of Google's hash value search of the Maher file. *United States v. Jacobsen*, 466 U.S. at 119. They needed to open the Maher file, and a human being had to conduct a visual examination of its contents. Such an expanded search required a warrant.

A. Maher's Reasonable Expectation of Privacy in the Maher File Was Not Extinguished by Google's Terms of Service

In explaining that conclusion, we first consider the government's argument that Maher lacked a reasonable expectation of privacy in the contents of the Maher file. *See United States v. Jones*, 565 U.S. at 406 (holding that person must have "reasonable expectation of privacy" in property searched to complain of Fourth Amendment violation). Such an argument, if successful, would mean that Maher could not complain about the government's warrantless search of the Maher file regardless of whether Google had conducted a private search of that item. In fact, the argument fails for reasons that we now explain.[8]

At the outset, we note that the government does not here contend that, as a general matter, persons lack a reasonable expectation of privacy in their email communications. On that point, we here hold what this court has previously assumed, *i.e.*, "that a United States person ordinarily has a reasonable expectation in the privacy of his e-mails sufficient to trigger a Fourth Amendment reasonableness inquiry." *United States v. Hasbajrami*, 945 F.3d 641, 666 (2d Cir. 2019). As the Sixth Circuit has observed in that regard, "[g]iven the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection." *United States v. Warshak*, 631 F.3d

[8] *Jones* instructs that common-law trespass as well as reasonable expectations of privacy properly inform Fourth Amendment analysis. *See id.* at 409 (explaining that Fourth Amendment "reasonable-expectation-of-privacy test has been *added* to, not *substituted* for, the common-law trespassory test" (emphasis in original)). Because the challenged search here fails the reasonable-expectation-of-privacy test, we need not consider how it fares under the common-law trespassory test.

266, 285–86 (6th Cir. 2010); *see United States v. Ackerman*, 831 F.3d at 1304 (analogizing email to physical mail, search of which requires warrant, in observing that "[n]o one in this appeal disputes that an email is a 'paper' or 'effect' for Fourth Amendment purposes, a form of communication capable of storing all sorts of private and personal details").[9]

Rather, the government argues that Maher's expectation of privacy in the Maher file that he emailed to his own Google account was extinguished by Google's Terms of Service, which advise users that Google (1) "may review content to determine whether it is illegal or violates our policies," App'x 113, (2) "may" report "illegal content" to "appropriate authorities," *id.* at 142, and (3) "will share" users' information with law enforcement when necessary to comply with applicable law, *id.* at 131.

This court has not had occasion to address what effect, if any, a private company's terms of service might have on a defendant's reasonable expectation of privacy. It may well be that such terms, as parts of "[p]rivate contracts[,] have little effect in Fourth Amendment law because the nature of those [constitutional] rights is against the government rather than private parties." Orin S. Kerr, *Terms of Service and Fourth Amendment Rights*, 172 U. PA. L. REV. 287, 291 (2024) (summarizing case law). We need not here draw any categorical conclusions about how terms of service affect a user's expectation of privacy as against the government. On this appeal, it suffices that we conclude that Google's particular Terms of Service—which advise

[9] The Ninth Circuit has suggested that a reasonable expectation of privacy in emails lasts only until the email is delivered to the recipient. *See United States v. Mohamud*, 843 F.3d 420, 442 (9th Cir 2016). We need not pursue that point here because Maher emailed the Maher file to himself, thereby retaining an expectation of privacy in its contents.

that Google "may" review users' content, App'x 113—did not extinguish Maher's reasonable expectation of privacy in that content as against the government.

In reaching that conclusion, we adopt the reasoning of the Sixth Circuit in *United States v. Warshak*, 631 F.3d at 286–87 (holding that government violated Fourth Amendment when, without warrant, it compelled internet service provider to surrender contents of user emails). There too, the government argued that an internet service provider's contractual reservation of the right to access user emails extinguished a defendant's expectation of privacy in his emails. In rejecting the argument—at least with respect to a reservation phrased in terms of what the provider *may* do, *see id.* at 287 (quoting Acceptable Use Policy provision stating that provider "*may* access and use individual Subscriber information in the operation of the Service and as necessary to protect the Service" (emphasis in original))—the Sixth Circuit held that "the mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy" as against the government, *id.* at 286 (emphasis in original). As the court explained, that conclusion finds support in the seminal Fourth Amendment case, *Katz v. United States*, 389 U.S. 347 (1967), where "the Supreme Court found it reasonable to expect privacy during a telephone call despite the ability of an operator to listen in." *United States v. Warshak*, 631 F.3d at 287 (noting that telephone companies could then "listen in when reasonably necessary to protect . . . against the improper and illegal use of their facilities" (internal quotation marks omitted)). It also finds support in cases recognizing that hotel guests retain a reasonable expectation of privacy in their rooms, "even though maids routinely enter hotel rooms." *Id.*; *see United States v. Stokes*,

733 F.3d 438, 443 n.7 (2d Cir. 2013) ("Hotel guests retain a legitimate expectation of privacy in the hotel room and in any articles located in their hotel room for the duration of their rental period."). We too conclude from these precedents that Google's Terms of Service, advising users of what the company "may review," App'x 113, did not extinguish Maher's reasonable expectation of privacy in his emails as against the government.

Nor is a different conclusion compelled by the fact that Google's Terms of Service also warn users that the company "*will* share personal information outside of Google if . . . reasonably necessary to[] . . . [m]eet any applicable law." *Id.* at 131 (emphasis added). As noted *supra* at 7 n.5, federal law requires electronic service providers such as Google to file a report with the NCMEC when they have "actual knowledge" of child pornography on their platforms. 18 U.S.C. § 2258A(a)(1)(A), (B). But the same law specifically does *not* require Google "affirmatively [to] search, screen, or scan" for such material. *Id.* § 2258A(f)(3). Not surprisingly then, Google does not tell users that it *will* engage in the sort of content review for illegality that could trigger disclosure obligations under § 2258A(a)(1)(A), (B). Rather, it tells users only that it "may" engage in such review. App'x 113. Indeed, in the next sentence, Google emphasizes that it "does not necessarily . . . review content," and tells users, "*please don't assume that we do*." *Id.* at 114 (emphasis added). Such qualified language is hardly a *per se* signal to Google users that they can have no expectation of privacy in their emails, even as against the government. *Cf. United States v. Rosenow*, 50 F.4th 715, 730 (9th Cir. 2022) (stating, with respect to § 2258A, that "[m]andated *reporting* is different than mandated *searching*" (emphasis in original)).

In a different context that is nevertheless instructive here, the Supreme Court declined to construe even unqualified language in a private

contract as extinguishing a person's expectation of privacy as against the government. *See Byrd v. United States*, 584 U.S. 395 (2018). There, a car rental agreement expressly forbade anyone not identified in the contract from operating the leased vehicle. The government argued that this meant any driver not so identified had no reasonable expectation of privacy in the vehicle. The Court, however, declined to derive such a *"per se* rule" from the contract's identified-operator provision. *Id.* at 405. Recognizing that "car-rental agreements are filled with long lists of restrictions," *id.* at 407, the Court adhered to the "general rule" that a person "in otherwise lawful possession and control of a rental car has a reasonable expectation of privacy" against the government in that vehicle even if he is not authorized by the rental agreement to be operating the car, *id.* at 398–99.

Here, we need not decide whether terms of service pertaining to content review might ever be so broadly and emphatically worded as to categorically extinguish internet service users' reasonable expectations of privacy in the contents of their emails, even as against the government. *See United States v. Warshak*, 631 F.3d at 287 (declining to foreclose possibility). We conclude only that Google's Terms of Service, repeatedly qualifying the content review that the company "may" conduct, do not effect such a complete extinguishment.

Thus, to justify its warrantless search of the Maher file, the government had to show that it simply repeated the private search of that file already conducted by Google. We now turn to that point.[10]

[10] Citing *United States v. Lewis*, 62 F.4th 733, 742 (2d Cir. 2023), the government argues that Maher failed, in any event, to offer any evidence that he had a

B. Private Search Doctrine

1. Legal Precedents

The private search doctrine permits government officials, without a warrant, to repeat a search of personal papers and effects already conducted by a private party, so long as the government does not expand upon the prior private search. *See United States v. Jacobsen*, 466 U.S. at 114–22.

The doctrine is grounded in the longstanding recognition that the Fourth Amendment proscribes only "governmental action." *Burdeau v. McDowell*, 256 U.S. 465, 475 (1921). In *Burdeau,* the Supreme Court held that the government does not violate the Fourth Amendment when it prosecutes a defendant using evidence obtained in the first instance—even unlawfully—by a private party. The Court reasoned that so long as no government official "had anything to do with the [private party's] wrongful seizure of the petitioner's property . . . there was no invasion of the security afforded by the Fourth Amendment against unreasonable search and seizure, as whatever wrong was done was the act of individuals in taking the property." *Id.* Similarly, in *Coolidge v. New Hampshire*, 403 U.S. 443 (1971), the Supreme Court rejected a Fourth Amendment challenge to the

---

subjective expectation of privacy in the contents of the Maher file. *Lewis*, however, required only that a defendant seeking to suppress evidence "respond to the Government's argument" that he lacked a reasonable expectation of privacy, whether by pointing to relevant evidence or making "any arguments pertinent to his reasonable expectation of privacy . . . in his motion papers." *Id.* at 741. Maher made such an argument below, and the government cites no case requiring him further to file a declaration attesting to his subjective expectation of privacy. On this record, we see no basis to question whether Maher—who emailed the Maher file to himself—subjectively expected the file to be private as against the government.

government's use of incriminating evidence that the defendant's spouse had voluntarily given to law enforcement officials, explaining, "it is no part of the policy underlying the Fourth and Fourteenth Amendments to discourage citizens from aiding . . . in the apprehension of criminals." *Id.* at 487–88.

The principles supporting these precedents, in turn, informed the Supreme Court's discussion of the private search doctrine in two cases challenging warrantless government searches following private searches of the same or related property: *Walter v. United States*, 447 U.S. 649 (1980), which produced no majority opinion, and *United States v. Jacobsen*, 466 U.S. 109 (1984), which did.

In *Walter*, boxes containing pornographic films were delivered to the wrong recipient. *See* 447 U.S. at 651 (plurality opinion). Employees of the mistaken recipient opened the boxes and saw on the films' labels "suggestive drawings" and "explicit descriptions" of the films' contents. *Id.* at 652. After one employee "attempted without success to view portions" of one of the films "by holding it up to the light," the recipient company contacted the FBI. *Id.* Taking possession of the boxes and their contents, an FBI agent, without a warrant, proceeded to view the films contained therein using a projector. *See id.*

Five members of the Court concluded that the FBI's warrantless viewing of the films violated the Fourth Amendment for varying reasons, none of which commanded a majority. In the plurality opinion, Justice Stevens, writing for himself and Justice Stewart, so concluded because the agent's viewing of the films exceeded the scope of the private search. He explained that while "a wrongful search or seizure conducted by a private

party . . . does not deprive the government of the right to use evidence that it has acquired lawfully," the government "may not *exceed the scope* of the private search unless it has the right to make an independent search" or has obtained a warrant. *Id.* at 656–57 (emphasis added). In these two Justices' view, the agents' viewing of the films with a projector "was a significant expansion of the search that had been conducted previously by a private party and therefore must be characterized as a separate search" that, without a warrant, violated the Fourth Amendment. *Id.* at 657. They did not think that employees' viewing of images and descriptions on the outside of the films—a fact emphasized by the four dissenting justices—warranted a different conclusion because that private action "frustrated" the defendants' expectation of privacy only "in part," which did not "automatically justify a total invasion" of privacy by the government. *Id.* at 659 & n.13.

Concurring in the Court's identification of a Fourth Amendment violation, Justice White, joined by Justice Brennan, expressed general reservations about the private search doctrine: "The notion that private searches insulate from Fourth Amendment scrutiny subsequent governmental searches of the same or lesser scope is inconsistent with traditional Fourth Amendment principles." *Id.* at 660.[11]

The four dissenters—Justice Blackmun, joined by Chief Justice Burger and Justices Powell and Rehnquist—agreed with Justices Stevens and Stewart that the private search doctrine could provide an exception to the Fourth Amendment warrant requirement. *See id.* at 662 (stating that

[11] Justice Marshall also concurred in the judgment, but without authoring or joining in an opinion. *See id*.

plurality opinion "at least preserves the integrity of the rule specifically recognized long ago in *Burdeau v. McDowell*"). But they thought the employees' review of pictures and descriptions on the films' labels sufficed to extinguish any reasonable expectation of privacy that defendants had in the specific contents of the films, thereby permitting the FBI, without a warrant, to use a projector to view the films. *See id.* at 663–66.

Four years later, the Supreme Court revisited the private search doctrine in *United States v. Jacobsen*, 466 U.S. 109 (1984). In that case, Federal Express ("FedEx") employees, per company policy, opened a package damaged in transit and therein saw crumpled newspaper cushioning a tube constructed of duct tape. Inside the tube, employees found four plastic bags filled with white powder. *See id.* at 111. FedEx notified the Drug Enforcement Administration ("DEA") but, before an agent arrived at the scene, employees had put the plastic bags back into the tube and the tube and newspapers back into the box. *See id.* Upon arrival, a DEA agent reopened the box; removed the tube from the box, the plastic bags from the tube, and a small amount of white powder from one of the bags; and conducted a chemical "field test" on the powder, which reacted positively for cocaine. *Id.* at 111–12 & n.1.

This time, Justice Stevens wrote for a six-member majority in concluding that the private search doctrine supported the agent's warrantless removal of the tube from the box and the plastic bags from the tube because these actions merely duplicated the search previously conducted by FedEx employees. *See id.* at 115 (stating that these "initial invasions of respondents' package were occasioned by private action," which necessarily "did not violate the Fourth Amendment"). Nevertheless, citing approvingly to the *Walter* plurality, the Court held that any

"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." *Id.* at 115; *see also id.* at 117 n.12 (observing that plurality and dissent in *Walter* agreed that this was "the standard to be applied"). Explaining the distinction that could thus arise when applying the private search doctrine, the Court in *Jacobsen* stated that "[o]nce frustration of the original expectation of privacy occurs" by a private party, "the Fourth Amendment does not prohibit governmental use of the now-nonprivate information." *Id.* at 117. But "[t]he Fourth Amendment is implicated . . . if the authorities use information with respect to which the expectation of privacy has not already been frustrated," because "[i]n such a case the authorities have not relied on what is in effect a private search, and therefore presumptively violate the Fourth Amendment if they act without a warrant." *Id.* at 117–18. Thus, when authorities look to exceed the scope of a prior private search, *i.e.*, when they look to learn *more* than what had been revealed by the private search, they must ordinarily obtain a warrant. *See id.* at 119-20.

Applying this test to *Jacobsen*'s facts, the Supreme Court held that, even though FedEx employees had put the plastic bags containing white powder back into the tube and had placed the tube together with surrounding sheets of newspaper back into the original package, the DEA agent's warrantless removal of the tube from the package and the plastic bags from the tube did not violate the Fourth Amendment because those actions simply repeated the private search conducted by FedEx employees and enabled the agents "to learn nothing that had not previously been learned during the private search." *Id.* (observing that when agent opened box and removed contents, "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" by the FedEx employees who had conducted the private search).

At the same time, however, the Court ruled that by then conducting a field test on some of the white powder—something FedEx employees had not done—the agent effected an "additional intrusion" that "exceeded the scope of the private search" and, thus, did not fall within that particular exception to the warrant requirement. *Id.* at 122. Instead, the Court ruled that no warrant was required for the field test because it "could disclose only one fact previously unknown to the agent—whether or not a suspicious white powder was cocaine." *Id.* Specifically, if the test indicated the powder was not cocaine, it "could tell [the agent] *nothing more*, not even whether the substance was sugar or talcum powder." *Id.* (emphasis added). Thus, the Court concluded that, Congress having decided "to treat the interest in 'privately' possessing cocaine as illegitimate," a simple binary field test "that can reveal whether a substance is cocaine, and no other arguably 'private' fact, compromises no legitimate privacy interest." *Id.* at 122–23.

In sum, as construed by the Supreme Court in *Walter* and *Jacobsen*, the private search doctrine is properly understood to authorize law enforcement authorities to conduct a warrantless search only when they repeat a search already conducted by a private party to the same degree it "frustrate[s]" a person's expectation of privacy. *Id.* at 117. If law enforcement authorities "exceed[] the scope of the private search," seeking to learn "anything more" than the private party had learned from its search, they must either secure a warrant or have some further legal basis for not doing so. *Id.* at 115–22; *see United States v. Knoll*, 16 F.3d 1313, 1319–21 (2d Cir. 1994) (citing plurality opinion in *Walter* for proposition that government

"may not expand the scope of an ongoing private search unless it has an independent right to do so").

2. Application of Private Search Doctrine to This Case

Following the principles articulated in these precedents, we now consider whether the private search doctrine permitted State Police visually to examine the contents of the Maher file without a warrant.

In conducting that inquiry, we recognize that this court has applied the private search doctrine in various cases involving searches of physical items. *See, e.g.*, *United States v. $557,933.89, More or Less, in U.S. Funds*, 287 F.3d at 87–88 (holding that officer did not violate Fourth Amendment when, without warrant, he opened briefcase earlier reviewed by airport security personnel, so long as officer's search "was of no greater scope or intensity than the airport security personnel's"); *United States v. Knoll*, 16 F.3d at 1320–21 (holding no warrant required for law enforcement authorities to read documents already searched by burglars, while noting that, "[i]f the files were closed and their contents not apparent from the exterior, the reasonable expectation of privacy continued so long as the files had not been searched before contact with the government occurred").

This court has not, however, had occasion in a published opinion to apply the doctrine to searches of electronically stored data. We did not do so in *United States v. DiTomasso*, 932 F.3d 58, 67–68 (2d Cir. 2019), because the defendant there appealing his child pornography conviction did not challenge the district court's reliance on the private search doctrine to deny a motion to suppress evidence. Meanwhile, in *United States v. Wilbert*, 818 F. App'x 113, 114 (2d Cir. 2020), this court decided in a non-precedential summary order that (1) a law enforcement official did not need a warrant to

view an image that a defendant uploaded to an online chat service because an employee of that service had previously reviewed the image; but (2) the officer violated the Fourth Amendment when, without a warrant, he expanded upon the private search by also viewing an image that the employee had not reviewed.[12]

A number of our sister circuits, however, have issued published opinions applying *Jacobsen* to warrantless searches of electronically stored digital information. Almost uniformly, these courts have held that the private search doctrine authorizes law enforcement officers to conduct warrantless examinations of digital files that a private person has already visually examined.[13] Were that the circumstance here, we would readily

---

[12] The algorithm used in *Wilbert* to flag potentially suspicious images appears to differ from that used by Google here. *See United States v. Wilbert*, No. 16 Cr. 6084, 2018 WL 6729659, at *3 (W.D.N.Y. Aug. 20, 2018) (stating that algorithm there relies on "shapes, colors and . . . [image] features").

[13] *See United States v. Rivera-Morales*, 961 F.3d 1, 5–6, 8–15 (1st Cir. 2020) (holding warrant not required for authorities to view image of child pornography on defendant's cell phone when defendant's wife had already discovered image on phone and showed it to local police); *United States v. Runyan*, 275 F.3d 449, 463–64 (5th Cir. 2001) (holding that police could conduct warrantless review of computer disks already viewed by private party, but not of disks that had not been so viewed); *Rann v. Atchison*, 689 F.3d 832, 836–37 (7th Cir. 2012) (holding warrant not required for police to view digital images seen by victim's mother and turned over by her to authorities); *United States v. Goodale*, 738 F.3d 917, 921 (8th Cir. 2013) (holding warrant not required for authorities to view child pornography websites on defendant's laptop computer when victim's mother had brought laptop to police station and showed officers websites in viewing history); *United States v. Phillips*, 32 F.4th 865, 875 (9th Cir. 2022) (holding warrant not required for law enforcement authorities to view child pornography images on defendant's laptop computer when former fiancée had discovered images on laptop and showed

reach the same conclusion, which requires nothing more than a straightforward application of *Jacobsen* to modern technology. When a private person has already visually examined a defendant's digital image, he has thereby "frustrated" the defendant's expectation of privacy in that image, such that when law enforcement authorities also visually examine it, they learn "nothing more" by doing so than what had "previously been learned during the private search." *United States v. Jacobsen*, 466 U.S. at 120. Thus, the private search doctrine there relieves the government of the need to obtain a warrant.[14]

---

them to authorities); *United States v. Benoit*, 713 F.3d 1, 8–11 (10th Cir. 2013) (holding warrant not required for police to view images of child pornography on defendant's computer that girlfriend had discovered and shown to police); *United States v. Castaneda*, 997 F.3d 1318, 1326–29 (11th Cir. 2021) (holding warrant not required for FBI agent to view child pornography file opened by defendant's friends who alerted FBI); *cf. United States v. Lichtenberger*, 786 F.3d 478, 488–89 (6th Cir. 2015) (holding private search doctrine inapplicable where "there was a very real possibility" that officer's warrantless search uncovered information that no private party had seen). In *United States v. Fall*, the Fourth Circuit found it unnecessary to "address[] the private search doctrine in the context of electronic devices," because the "good faith exception to the exclusionary rule" supported affirmance there in any event. 955 F.3d 363, 370–71 (4th Cir. 2020).

[14] The conclusion may be more obvious when the search at issue pertains to a particular digital image rather to an electronic device. *See United States v. Phillips*, 32 F.4th at 873 (observing "that it may be more difficult to have 'virtual certainty' that a search of an electronic device does not reveal more than the private search had already revealed, given the dynamic nature of such devices"); *United States v. Wilson*, 13 F.4th 961, 977 n.13 (9th Cir. 2021) (noting circuit split on question of whether individual's expectation of privacy in digital device is "entirely frustrated whenever any part of the container is searched" or if, instead, device owner retains expectation of privacy in files on device that have not been searched). We need not pursue this point here because the warrantless search at issue pertains to a single digital image.

This case, however, presents a different scenario raising a more challenging question, *i.e.*, whether the private search doctrine authorizes law enforcement authorities to conduct a warrantless visual examination of the contents of a digital file where a private party has not visually examined the contents of *that* file but, rather, has used a computer to match the hash value of the contents of that file to the hash value of an image previously located in another file, which image, upon visual examination, was determined to depict child pornography. Three Courts of Appeals have considered that question, with the Fifth and Sixth Circuits answering it in the affirmative and the Ninth Circuit responding in the negative. *Compare United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021), *with United States v. Miller*, 982 F.3d 412 (6th Cir. 2020), *and United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018).[15] We here join the Ninth Circuit in concluding that such a hash match may well provide strong probable cause for a warranted visual examination of the as-yet-unviewed matched image, but the private search doctrine does not authorize a warrantless visual examination of that computer-matched image.

We start by explaining why we are not persuaded by the reasoning of the Fifth and Sixth Circuits. In *United States v. Reddick*, the Fifth Circuit ruled that the private search doctrine authorized police to conduct a warrantless visual examination of an image that a private party found to have the same hash value as an image that the party had earlier determined to depict child pornography because "opening the [matched] file merely confirmed that the

[15] The Tenth Circuit, in *United States v. Ackerman*, declined to address this particular question, there concluding only that where a private party reported that one email attachment contained known child pornography, the government could not open *other* images attached to the same email without a warrant. *See* 831 F.3d at 1306–07.

flagged file was indeed child pornography, as suspected." 900 F.3d at 639. We do not adopt this reasoning because we do not understand the Fourth Amendment to permit law enforcement officials to conduct warrantless searches of unopened property to confirm a private party's report—however strong—that the property contains contraband. Indeed, in *United States v. Jacobsen*, the Supreme Court stated that police violate the Fourth Amendment when they "simply learn from a private party that a container contains contraband . . . and conduct a warrantless search." 466 U.S. at 120 n.17. This court has also held that the private search doctrine does not authorize the warrantless opening of a package even when police were told by the party who packed and mailed the package that it contained stolen property. *United States v. Martin*, 157 F.3d 46, 55 (2d Cir. 1994); *see generally Horton v. California*, 496 U.S. 128, 137 n.7 (1990) (stating that "no amount of probable cause can justify a warrantless search or seizure absent exigent circumstances"(internal quotation marks omitted)). Here, Google's report that the unopened Maher file contained an image whose hash value matched that of an image previously found in another file that, upon visual inspection, was determined to depict child pornography may well have provided authorities with strong probable cause to believe that the image in the Maher file also depicted child pornography and, thus, supported issuance of a warrant. But the reported hash match did not authorize them to conduct an unwarranted search of the unopened Maher file to confirm that belief.

Rather, the private search doctrine authorizes government officials to conduct a warrantless search only insofar as they effectively duplicate the search conducted by a private party, thereby frustrating no greater expectation of privacy and learning nothing more than what had been

learned during the private search. *See United States v. Jacobsen*, 466 U.S. at 119–20, 122. That does not appear to have been the case in *Reddick.* It is certainly not the case here. A Google computer "searched" the Maher file only for a hash value, which the computer then matched to a hash value already in its repository: 2eb373380383f50820e648d1c304a3db. That hash value search of the Maher file, however, did not reveal the particulars of the file's contents. To learn that additional information required a further search. It required a police officer to open the Maher file and visually to examine its contents—a more expansive search never conducted by Google in this case and, thus, not falling within the private search doctrine.

In concluding otherwise, the Fifth Circuit analogized visual examination of a hash matched file to the "chemical tests on the white powder in *Jacobsen*," also a form of examination not employed by the private party in that case. *United States v. Reddick*, 900 F.3d at 639. But the Supreme Court did not approve the warrantless field test in *Jacobsen* under the private search doctrine. To the contrary, the Court observed that no such test having been conducted by the searching private party, the field test there "exceeded the scope of the private search." *United States v. Jacobsen*, 466 U.S. at 121. Rather, the Court concluded that a field test did not require a warrant because its further intrusion was limited to a binary disclosure, *i.e.*, it "could disclose *only* . . . whether or not a suspicious white powder [discovered by the private search] was cocaine," and "could tell [the agent] *nothing more*, not even whether the substance was sugar or talcum powder." *Id.* at 122 (emphasis added).

That is not the case here. Unlike a field test, a human visual examination of a computer hash matched image does not disclose *only* whether or not the image depicts child pornography. Visual examination

necessarily also reveals the particulars supporting either a "yes" or "no" answer. In the case of an affirmative answer, those particulars would include the individual children depicted, the number of such children, their approximate ages, any adults also depicted, whether the defendant is depicted, the circumstances of depiction indicative of child pornography, etc.[16] Google did not learn any of these particulars in its computer hash value search of the Maher file. Also, in the case of a negative answer, a human visual examination would still reveal particulars, ranging from the innocuous to the embarrassing, that the account holder reasonably expected were private. Thus, a visual examination's revelation of particulars is a far cry from a field test's disclosure of nothing more than a binary answer.[17]

In *United States v. Miller*, the Sixth Circuit recognized that warrantless visual examination of a hash matched image cannot be analogized to a

---

[16] While we do not here describe any of the disturbing 4,000 images and five videos at issue in this case, they all too sadly evidence the variety of particulars that can be depicted in child pornography.

[17] For much the same reason, the warrantless visual examination in this case cannot be analogized to a dog sniff, another sort of binary test invoked by the government. *See United States v. Place*, 462 U.S. 696, 707 (1983) (upholding warrantless dog sniff that "discloses only the presence or absence of narcotics"); *Illinois v. Caballes*, 543 U.S. 405, 408 (2005) (stating that dog sniff, as "governmental conduct that *only* reveals the possession of contraband[,] compromises no legitimate privacy interest" (emphasis in original and internal quotation marks omitted)). *But see United States v. McKenzie*, 13 F.4th 223, 232 (2d Cir. 2021) (holding that when canine sniff pertains to constitutionally protected areas, such as exterior of home, it can implicate privacy interests so as to require warrant). In any event, we note that when authorities want to open and inspect the contents of a *closed* container to which a trained dog reacted for contraband, the Supreme Court has held that a warrant is required. *See United States v. Chadwick*, 433 U.S. 1, 3–4, 13–15 (1977), *abrogated on other grounds by California v. Acevedo*, 500 U.S. 565 (1991).

binary field test. *See* 982 F.3d at 429 (rejecting Fifth Circuit reasoning). Nevertheless, that court also concluded that the private search doctrine supported a warrantless visual examination of a hash matched image, reasoning that the high reliability of hash matching technology created the same "virtual certainty" as in *Jacobsen* that the warrantless search would reveal the same evidence uncovered in the private party search. *Id.* at 429–30 (stating that private search doctrine applies "if there is a 'virtual certainty' that [police] viewing of the [matched] files would disclose the same images that Google's employees had already viewed" and identified as child pornography).[18] We are not persuaded.

Jacobsen is distinguishable from *Miller* and this case in an important respect. In *Jacobsen*, a DEA agent conducted a warrantless search of the *same*

---

[18] In reaching this conclusion, the Sixth Circuit referenced findings by the magistrate judge, adopted by the district judge, that hash matching technology was "highly reliable—akin to the reliability of DNA." *Id.* at 430 (noting finding supported by another district court case and publication of Federal Judicial Center, which indicated that likelihood of different images sharing the same hash value was one in one billion, or even one in 9.2 quintillion (internal quotation marks and citations omitted)). We do not pursue this reliability point except to note that the Sixth Circuit appears to have assigned defendant the burden of disproving the reliability of hash matching technology. *See id.* (stating that "Miller, who bore the burden of proof, never challenged the reliability of hashing in the district court" (internal quotation marks omitted and alteration adopted)). Because our own court places the burden on the government to show that a challenged search fell within an exception to the warrant requirement, *see, e.g., United States v. Kiyuyung*, 171 F.3d 78, 83 (2d Cir. 1999) ("If the place or object subjected to the warrantless search is one in which the defendant had a reasonable expectation of privacy, the burden of showing that the search fell within one of the exceptions to the warrant requirement is on the government."), we think that where the government relies on hash matching or other technology to carry that burden, it assumes the obligation of demonstrating the technology's reliability.

container already privately searched by FedEx employees. It was in that context that the Court concluded that, even though FedEx employees had placed all items found in their search back into that container, no warrant was necessary for a DEA agent to search that same container because there was a "virtual certainty" that nothing more would be found than what FedEx employees had already seen. *United States v. Jacobsen*, 466 U.S. at 119. By contrast, in *Miller* and here, police conducted a warrantless visual search of a digital file (here, the Maher file) that no Google employee or contractor had ever opened or visually examined. Rather, what a Google employee or contractor had earlier opened and visually examined was a *different* file—*i.e.*, the original file—wherein it identified an image depicting child pornography.

Maher had no expectation of privacy in the original file that could have been extinguished by Google's visual examination of its contents. Maher did, however, have an expectation of privacy in the Maher file, which he uploaded to one of his own email accounts. To the extent Google subsequently "searched" the Maher file, it did so only to the limited degree of having a computer determine that the hash value derived from the file's contents matched the hash value derived from the original file's contents. The State Police never replicated that computer search. Rather, they employed a completely different and more intrusive search method—human visual examination—to learn more than could be learned from Google's hash matching algorithm.

Thus, even if the government in this case had offered evidence that Google's hash matching technology made it virtually certain that the images

contained in two hash matched files were identical,[19] the match did not permit the government to go further than Google had and to examine visually the contents of the Maher file without a warrant. *See United States v. Jacobsen*, 466 U.S. at 120 n.17 (acknowledging that police cannot conduct warrantless search of unopened container based on private party report that it contains contraband); *United States v. Martin*, 157 F.3d at 55 (noting that police cannot conduct warrantless search of mailed container even though party who packed and mailed it reported that it contained stolen property). Google's hash value search did not tell Google anything about the particulars depicted in the Maher file—or even the original file image, which Google apparently had not retained. To learn those additional particulars, police needed to exceed the scope of Google's computer search by opening the Maher file and having an officer visually examine its contents. The private search doctrine did not permit them to conduct this more intrusive search without a warrant. *See United States v. Jacobsen*, 466 U.S. at 120.

In so concluding, we join the Ninth Circuit, which has ruled that the private search doctrine does not permit police to conduct a warrantless visual examination of a digital file that a private party has not itself viewed but only computer hash matched to the contents of another digital file previously determined to contain child pornography. *See United States v. Wilson*, 13 F.4th at 961. In reaching that conclusion, the Ninth Circuit deemed it "critical" that "no Google employee viewed" the particular

[19] As earlier noted, *supra* at 12 n.7, the government offered no such evidence in this case. In fact, the affidavit submitted to the district court in this case by Google Manager Lilley qualified the precision of the company's hash matches: "Comparing these hashes to hashes of content uploaded to Google's services allows Google to identify exact or *very similar* images of apparent child pornography." App'x 109 (emphasis added).

contents of defendant's hash matched files before the government did so. *Id.* at 974. We agree. As that court stated on this point: "When the government views anything other than the specific materials that a private party saw during the course of a private search, the government search exceeds the scope of the private search." *Id.* (referencing distinction drawn in *Jacobsen* between government's visual search of container contents already examined by private party and government's field test of white powder found in container, which "exceeded the scope of the private search" (emphasis omitted) (quoting *United States v. Jacobsen*, 466 U.S. at 122)).

Also, like the Ninth Circuit, we do not think it can be said that "because Google had already classified the [original file] as child pornography," the government could learn "nothing new" by visually examining an image with the same hash value when it appeared in another file. *Id.* at 972 (rejecting argument). Even assuming the high reliability of Google's hash matching technology, it could reveal only that two images are virtually certain to be identical. It could not—and here did not—reveal what in particular was depicted in the identical images.[20]

[20] As the Ninth Circuit observed in *Wilson*, "Google does not keep a repository of child pornography images, so no Google employee or contractor could have shown the government the images it believed to match Wilson's. Nor does the record identify the individual who viewed those images." 13 F.4th at 972. While the record in *Wilson* indicates that Google "tags" images in its child pornography repository "with one of four generic labels," *id.* (noting that image whose hash value matched Wilson's was tagged A1, which indicated the depiction of "a sex act involving a prepubescent minor"), the record in this case contains no comparable evidence of tagging.

In these circumstances, Google's hash matching technology might better be understood to have *labeled* the Maher file image as "apparent child pornography," App'x 29, much as the pictures and images on the film labels in *Walter v. United States*, 447 U.S. at 654, indicated that the films' content was pornographic. *See United States v. Wilson*, 13 F.4th at 973 (drawing analogy). Such labels can provide the probable cause necessary to secure a warrant to search the contents of closed containers bearing those labels. But such a search is certainly going to reveal more than the label itself.[21] That is evident here where Google's computer hash value search of the Maher file by a computer supported the company's labeling the file image as "apparent child pornography" in its report to the NCMEC. But an entirely different search, specifically, a human visual examination of the Maher file, was necessary to learn the exact child pornography depicted: "a prepubescent

[21] "Labeled" items should not be confused with those whose containers or packaging "by their very nature cannot support any reasonable expectation of privacy because their contents can be inferred from their outward appearance." *Arkansas v. Sanders*, 442 U.S. 753, 765 n.13 (1979), *abrogated on other grounds by California v. Acevedo*, 500 U.S. 565 (1991). This exception applies only where an owner stores his property in a container that makes its content apparent, thus disclaiming an expectation of privacy. *Cf. United States v. Dien*, 609 F.2d 1038, 1045 (2d Cir. 1979) (holding defendant retained expectation of privacy in sealed cardboard box emanating smell of marijuana because fact that box was sealed "manifested an expectation that the contents would remain free from public examination"), *adhered to on reconsideration*, 615 F.2d 10 (2d Cir. 1980). Nothing about the Maher file or the Google email account to which Maher uploaded it indicated Maher's intent to disclaim a privacy interest in the file, the specific contents of which could not be known until it was visually examined, which Google never did. *See generally United States v. Knoll*, 16 F.3d at 1320 (stating, with respect to non-digital files that if they "were closed and their contents not apparent from the exterior, the reasonable expectation of privacy continued so long as the files had not been searched before contact with the government occurred").

female, who appears approximately six to seven years old, exposing her vagina." App'x 44. In short, Investigator Croneiser's visual inspection of the Maher file image was a search of far greater "scope" for purposes of the Fourth Amendment than Google's algorithmic search only for matching hash values "because it allowed the government to learn new, critical information" that could be used "to prosecute" Maher. *United States v. Wilson*, 13 F.4th at 971–72; *see United States v. Jacobsen*, 466 U.S. at 119–20 (holding private search doctrine authorizes warrantless search doctrine only when there is "virtual certainty" latter will "not tell [police] anything more than" already revealed by private search).

In urging otherwise, the government argues that the relevant private search here is not simply Google's computer hash match of the Maher file image to the original file image, but also a Google employee or contractor's earlier visual examination of the latter image. We are not persuaded for a further reason relied on by the Ninth Circuit: Fourth Amendment rights are personal to an individual. *See United States v. Wilson*, 13 F.4th at 974; *see generally, e.g.*, *Plumhoff v. Rickard*, 572 U.S. 765, 778 (2012); *Rakas v. Illinois*, 439 U.S. 128, 133–34 (1978). Thus, just as Maher cannot claim any expectation of privacy in Google's earlier visual examination of the original image, which did not belong to him, but which contained the image first assigned hash value 2eb373380383f50820e648d1c304a3db, so the government cannot claim that Google's visual search of that third-party file somehow defeated Maher's expectation of privacy in the contents of his own unopened, unreviewed file as against the government. As the Ninth Circuit stated on this point, "whether Google had previously reviewed, at some earlier time, *other individuals'* files is not pertinent to whether a private search eroded *Wilson*'s expectation of privacy" in his file. *United States v.*

Wilson, 13 F.4th at 974–75 (construing precedent to require "focus on the extent of Google's private search of *Wilson*'s effects, not of other individuals' belongings") (all emphases in original).

Insofar as Google searched the Maher file for a hash value that matched the hash value previously assigned to an image identified by a Google employee or contractor as depicting child pornography, the private search doctrine likely would have permitted police to rely on that computer match to demonstrate probable cause to support warrants for their own searches of Maher's Google accounts and residence. It might also have permitted the government—with sufficient foundation—to offer evidence of the match at trial. But here, the police understandably wanted to obtain evidence of more than a hash match. They wanted evidence of the particulars depicted in the matched Maher file image. Because no one at Google had ever opened or visually examined the contents of the Maher file, and because such a visual examination would reveal more information than Google knew at the time it reported the Maher file to the NCMEC, such a visual examination by the police did not fall within the private search doctrine's exception to the warrant requirement.

In sum, we here conclude that the private search doctrine does not authorize government authorities to conduct a warrantless human visual examination of the contents of an unopened file attached to an email based on Google's computer hash value match of an image in that file to another image previously identified by a Google employee or contractor as child pornography. The former search does not duplicate the latter but rather exceeds its scope, thereby allowing authorities to learn more than had been revealed by the private search. *See United States v. Jacobsen*, 466 U.S. at 118–22. In so holding, we suggest no constitutional limitation on Google's own

ability, as a private actor, to search for and remove child pornography on its platform. *See generally Burdeau v. McDowell*, 256 U.S. at 475 (stating that Fourth Amendment is "not intended to be a limitation upon other than governmental agencies"). Nor do we limit government authorities from using a private party's reliable hash matches between an identified image of child pornography and an unviewed file image to demonstrate probable cause for a warrant to conduct more expansive searches. *See United States v. Cartier*, 543 F.3d 442, 444–46 (8th Cir. 2008) (holding government established probable cause to search defendant's home after detecting defendant sent images whose hash values matched images of known child pornography). But as the Ninth Circuit has explained, the reliability of a company's hash matching technology "is pertinent to whether probable cause could be shown to obtain a warrant, not to whether the private search doctrine precludes the need for the warrant." *United States v. Wilson*, 13 F.4th at 979.

Thus, we hold that police here violated the Fourth Amendment by visually examining the contents of the reported Maher file without a warrant.

III. The Good Faith Exception to the Exclusionary Rule Supports Affirmance

Our identification of a Fourth Amendment violation in this case does not afford Maher relief from conviction because, like the district court, we conclude that Maher's suppression motion failed in any event under the good faith exception to the exclusionary rule.

As the Supreme Court has instructed, "[t]he fact that a Fourth Amendment violation occurred—*i.e.*, that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rule

applies." *Herring v. United States*, 555 U.S. 135, 140 (2009). Rather, exclusion of evidence is properly a court's "last resort, not [its] first impulse." *Id.* (internal quotation marks omitted). Thus, a court will suppress illegally obtained evidence "only where it results in appreciable deterrence" and not when an officer acts in an "objectively reasonable" manner. *Id.* at 141–42 (internal quotation marks omitted and alteration adopted).

That last caveat, the basis for the good faith exception to the exclusionary rule, most commonly applies when officers act "in objectively reasonable reliance" on a judge's issuance of a search warrant that is, in fact, legally defective. *See United States v. Leon*, 468 U.S. 897, 922 (1984). Nevertheless, the exception can also apply where officers "committed a constitutional violation" by acting without a warrant under circumstances that "they did not reasonably know, at the time, [were] unconstitutional." *United States v. Ganias*, 824 F.3d 199, 221–22 (2d Cir. 2016) (*en banc)* (referencing *United States v. Thomas*, 757 F.2d 1359, 1368 (2d Cir. 1985); *see id.* (holding warrant required for dog sniff conducted outside closed apartment but recognizing that, at time, officers acted in good faith in thinking no warrant required)); *United States v. Raymonda*, 780 F.3d 105, 118 n.5 (2d Cir. 2015) (presuming that "'basic insight of the *Leon* line of cases' that exclusion should be limited to cases of 'deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights,' applies equally to searches conducted with or without a warrant" (quoting *Davis v. United States*, 564 U.S. 229, 238 (2011))); *see also United States v. Goldstein*, 914 F.3d 200, 204–05 & n.28 (3d Cir. 2019) (holding that good faith exception applied when "government obtained [cell site location information] without a warrant" before practice was held unlawful by Supreme Court and collecting cases from other circuits so holding).

In assessing the reasonableness of an officer's mistaken belief that no warrant was required in a particular circumstance, we consider not only our own precedents but also those of other courts. *See United States v. Felder*, 993 F.3d 57, 75–76 (2d Cir. 2021) (relying on good faith exception to deny suppression in circumstances where, prior to Supreme Court ruling, those courts of appeals to have considered question had concluded no warrant required). When we do that here, we conclude that, in or about July 2020, when Investigator Croneiser opened the Maher file and visually examined its contents, she had a reasonable basis to believe that she did not need a warrant to do so.

At that time, neither the Supreme Court nor this court had considered whether a warrant is required for government authorities to open and visually examine a digital image that the service provider has reported depicts child pornography on the basis of a hash match to an image previously reviewed and labelled as child pornography by the service provider. The single appellate court to have done so, the Fifth Circuit, had held that no warrant was required in those circumstances. *See United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018). Two years after *Reddick* was decided, a second appellate court, the Sixth Circuit, reached the same conclusion. *See United States v. Miller*, 982 F.3d 412 (6th Cir. 2020). Not until September 2021—more than a year after the challenged warrantless search here—did the Ninth Circuit become the first appellate court to hold that a warrant was required for the government visually to examine a hash matched image in a file not opened by the service provider. *See United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021). In such circumstances, we think it was objectively reasonable for Investigator Croneiser to think that she did not need a warrant to visually examine the Maher file image reported by Google as

"apparent child pornography" based on a hash match to a file image previously "reviewed" by a Google employee or contractor and "determined [to] contain[] apparent child pornography." App'x 29.

In urging otherwise, Maher argues that Inspector Croneiser could not have been acting in good faith "because no binding precedent authorized the [warrantless] search in this case." Appellant Br. at 34. He is mistaken. While the good faith exception certainly applies "when binding appellate precedent specifically authorizes a particular police practice," *Davis v. United States*, 564 U.S. at 241 (emphasis omitted), it can also apply "[w]here a relevant legal deficiency was not previously established in precedent," such that "the agent's failure to recognize that deficiency cannot vitiate good faith," *United States v. Raymonda*, 780 F.3d at 119 (internal quotation marks omitted); *see also United States v. Hernandez*, No. 22-471, 2024 WL 47666, at *3 (2d Cir. Jan. 4, 2024) (summary order) (holding that where precedent rendering search impermissible was decided after search occurred, precedent was not "previously established" and good faith exception applied), *cert. denied*, 144 S. Ct. 1470 (2024). That is the case here where, at the time of the challenged search, the only appellate court to have ruled on the question had held that no warrant was required to open a digital file identified as child pornography based on a hash match, and where more than a year would pass before any appellate court held otherwise.

Maher nevertheless argues that evidence obtained by warranted searches of his Google accounts and residence should be suppressed because State Police misled the state court by failing to disclose in their supporting affidavits "potentially adverse information to the issuing judge," specifically, that no one at Google had visually examined the Maher file image. Appellant Br. at 33 (quoting *United States v. Ganias*, 824 F.3d at

221). We disagree. The first search warrant affidavit for Maher's two Google accounts states that "Google reported to [the NCMEC]" that one of the subject accounts "uploaded an image of child pornography on January 27, 2020." App'x 44. The second search warrant affidavit for Maher's residence states that, "[o]n January 27, 2020, Google Inc. reported an incident of Apparent Child Pornography to the [NCMEC]." *Id.* at 60. While neither affidavit states the basis for Google's report, *i.e.*, that it was a hash match rather than a visual examination, the omission was not misleading. Nor do we think its inclusion was required as material adverse information. While a hash match search of the Maher file did not reveal particulars depicted in an image contained therein so as to support a warrantless government search of that file under the private search doctrine, the hash match of that image to one earlier identified by Google as depicting child pornography provided strong probable cause to search the Maher file visually for child pornography. Thus, disclosure that Google's report of child pornography in the Maher file was based on a hash match rather than a visual examination would only have supported, not undercut, probable cause for issuance of the warrant.

Insofar as the warrant affidavits both state that their respective affiants—Investigator Croneiser for the first warrant and Investigator Esche for the second—had personally viewed the Maher file image and detailed what it depicted, *see id.* at 44, 60, we identify no basis to think that the issuing judge was misled to think that such viewing was warranted. Certainly, the affidavits did not say so. Rather, we think it likely that the issuing judge (the same for both warrants) would have understood silence on this point to mean that viewings of the Maher file image were not warranted because, in seeking warrants, law enforcement authorities generally report when

evidence already obtained was searched pursuant to a warrant. And, here, Investigator Esche, in seeking the second warrant, made a point of stating that the search of Maher's Google accounts had been pursuant to a warrant. In any event, for the same reasons we conclude that Investigator Croneiser had a good faith basis to think that she could conduct a warrantless visual examination of the Maher file image that Google reported to the NCMEC as containing apparent child pornography, we also conclude that Investigators Croneiser and Esche had a good faith basis to think that they did not need to state in a warrant affidavit that such an examination had been warrantless.

We therefore hold that while Investigator Croneiser's warrantless examination of the Maher file image was not authorized by the private search doctrine, the good faith exception to the exclusionary rule supports affirmance of the district court's denial of Maher's motion to suppress that image and the evidence subsequently obtained.

CONCLUSION

To summarize, we conclude that,

1. Google's Terms of Service did not extinguish Maher's reasonable expectation of privacy as against the government in the contents of his Google emails or images uploaded to such emails.
2. The private search doctrine did not authorize State Police to conduct a warrantless visual examination of the Maher file image. While Google matched the hash value for that image to the hash value of an image previously located in another file, which a Google employee or contractor, on visual examination,

identified to depict child pornography, (a) Google's examination of that third-party file did not extinguish Maher's reasonable expectation of privacy in his own unopened file, and (b) Google's hash value search of Maher's file did not reveal the particulars depicted therein that constituted child pornography. To secure that further evidence, police had to conduct a visual examination of the unopened Maher file image. Because that search went beyond Google's own hash value search of the Maher file, it required a warrant.

3. The warrantless police search of the Maher file does not entitle Maher to relief from conviction because, at the time of that search, police had a good faith basis to believe that no warrant was required. Thus, the good faith exception to the exclusionary rule here supports affirmance.

Accordingly, we **AFFIRM** the February 9, 2023 judgment of conviction.