No. _____

IN THE

SUPREME COURT OF THE UNITED STATES

RICHARD EDWARD BRILLHART,
Petitioner,

v.

UNITED STATES OF AMERICA,
Respondent.

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

APPENDIX TO THE PETITION FOR A WRIT OF CERTIORARI

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

Counsel for Petitioner

APPENDIX

TABLE OF CONTENTS

Opinion of the United States Court of Appeals for the Eleventh Circuit (July 9, 2026) 1a

Order of the United States Court of Appeals Denying Rehearing (September 1, 2026) 38a

Opinion and Order of the United States District Court Denying Suppression (May 7, 2023) 40a

U.S. Constitution, Amendment IV 62a

28 U.S.C. §§ 1254(1) and 1257(a) 63a

Suppression Hearing Transcript (Feb. 22, 2023), pp. 105–107, 124, 169–173, 179–181 (Dkt. No. 192) 64a

FOR PUBLICATION

In the
United States Court of Appeals
For the Eleventh Circuit

No. 24-13226

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

versus

RICHARD EDWARD BRILLHART,

Defendant-Appellant.

Appeal from the United States District Court
for the Middle District of Florida
D.C. Docket No. 2:22-cr-00053-SPC-NPM-1

No. 24-13232

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

versus

RICHARD EDWARD BRILLHART,

Defendant-Appellant.

Appeal from the United States District Court
for the Middle District of Florida
D.C. Docket No. 2:03-cr-00121-JES-KCD-1

Before NEWSOM, LUCK, Circuit Judges, and LEIBOWITZ,* District Judge.

NEWSOM, Circuit Judge:

Richard Brillhart was convicted of possessing and distributing child pornography and sentenced to 480 months' imprisonment. On appeal, he raises a host of challenges arising out of the investigation and prosecution of his crimes.

Most prominently, Brillhart argues that law-enforcement agents violated his Fourth Amendment rights when they searched a file that Google had found in his Gmail account and turned over to the National Center for Missing and Exploited Children. The key question before us is whether Google's initial determination that the file contained child pornography—which it reached by employing an automated "hash-value matching" protocol—was the sort of "private search" that may, in appropriate circumstances, authorize a later government search. For reasons we'll explain, we

---

* Honorable David S. Leibowitz, United States District Judge for the Southern District of Florida, sitting by designation.

hold that it was and, therefore, that the government's subsequent search of the file, which revealed no new material information, didn't violate the Fourth Amendment.

Brillhart separately challenges the government's decision to charge him with both distribution and possession of child pornography, as well as the district court's admission (or exclusion) of various pieces of evidence, its denial of his motion for judgment of acquittal, and several of its sentencing decisions. On these issues, we affirm the district court in all respects save one: its application of a five-level "pattern of activity" sentencing enhancement under U.S.S.G. § 2G2.2(b)(5). Because we vacate and remand for resentencing to correct that error, we needn't address Brillhart's challenges to his supervised-release-revocation sentence.

I

A

Tech companies face an issue that social-media users know to be all too real: A non-negligible amount of unlawful activity occurs on their platforms. That creates legal and reputational risks. To combat the posting and sharing of harmful content, and to mitigate the associated perils, the companies have developed a variety of tools—some manual, others automated. This case turns, at least in part, on the particulars of one of the tools that Google has deployed to thwart the proliferation of child pornography.

Google apprises users of its anti-pornography initiatives in two ways. First, and most directly, its "terms of service," to which customers must consent, expressly prohibit the use of its service

"in violation of the law"—and, more expressly still, prohibit the distribution of "child pornography." Tr. of Mot. to Suppress Hr'g at 90, Dkt. No. 192. Second, and more indirectly, Google issues "transparency report[s]" that publicize its efforts to "identify, remove and report" child pornography using a "combination" of human review and "automated detection tools." *Id.* at 97.

Specifically at issue here is one of those "automated detection tools" called hash-value matching. A hash value is a string of characters that together represent a file's unique, algorithmically generated "digital fingerprint." *Id.* at 121, 123. As relevant here, that means that if a photographic file is altered in any way, the hash value will change. *Id.* at 172. By contrast—and we'll elaborate on the nuances in good time—if "two files ha[ve] the same hash value, they're the same file[.]" *Id.* at 20. To be sure, our flesh-and-blood senses rebel at the notion that a digital image can be reduced to a collection of non-visual characters. But the fact is that a computer never "sees" the image as we do. To the computer, a hash value is a perfectly adequate—and accurate—digital stand-in.

Here's how Google's hash-value matching protocol works: When the company detects a suspicious file—whether through a user report, automated scanning, or some other process—it immediately compares the file's hash value to those in an internal "CSAM" (*i.e.*, child sexual abuse material) repository. That repository contains the hash values of files previously determined by Google's expert human reviewers to depict child pornography. Ac-

companying these hash values are standard "industry classification[s]"—jointly established by several internet service providers—that categorize the type of content in the file. So, for example, the classification "B1" means that the file depicts a "[p]ubescent minor involved in [an] overt sex act." *Id.* at 114.

If the hash value of the suspect file matches one in the repository designated and classified as child pornography, then Google sends the file, along with its hash and classification, to the National Center for Missing and Exploited Children (NCMEC)—which, in turn, forwards the material to the appropriate law-enforcement officials. If the file's hash value doesn't match one in the repository, a Google employee will conduct a manual review. If he determines that it depicts child pornography, he may note the hash value and add it to the company's internal repository along with his judgment about the image's proper categorization. But the information he relays to NCMEC—file, hash value, categorization—are the same as that he would have conveyed had there been a hash match.

B

Enter Richard Brillhart. In May 2021, Yahoo and Google independently flagged email accounts transmitting what the companies believed to be child pornography. Two of those accounts—reb3280e@yahoo.com and reb3280@gmail.com—had a few common, revealing identifiers pointing to Brillhart: Both were created under the name "Reb Reb," both listed the same recovery phone number tied to Brillhart, both used his birthdate (March 2, 1980) in

the usernames, and one listed his birthdate in its subscriber information.

Reviews of the email accounts yielded a lot of incriminating material. Brillhart's Yahoo accounts were used to transmit 241 videos and images of suspected child pornography, including some depicting toddlers and prepubescent children engaged in sexual acts with adult men. One message included a selfie, which company investigators used to identify Brillhart. Consistent with Yahoo corporate policy, each file was manually reviewed by a human being and confirmed to be child pornography. The company then sent the files, along with Brillhart's identifying information and sex-offender status, to NCMEC.

Google's investigation determined that three of Brillhart's email accounts contained a total of four illicit files. Three files were confirmed to depict child pornography by way of human review, the fourth through the hash-matching protocol already described. Like Yahoo, Google relayed the results of its investigation to NCMEC.

In possession of the files and Brillhart's identifying information, NCMEC identified his residence and promptly forwarded all the incriminating files and accompanying information to Officer Katrina Lee of the Fort Myers Police Department. From the companies' "CyberTips," Officer Lee could tell that they had already identified each of the files as child pornography. Importantly here, Google's report specifically indicated that it had verified one of the files through hash matching. Officer Lee understood that to mean

that "while the contents of the file were not reviewed concurrently to making the report, historically, a person had reviewed a file whose hash, or digital footprint, matched the hash of the reported image and determined it contained apparent child pornography." *Id.* at 171. In short, she knew (1) that an actual Google employee had previously reviewed the image as part of another user's file, determined it to be child pornography, and ensured that it was assigned a hash value, and (2) that Google had thereafter digitally matched the hash value of the file in Brillhart's account to the value of the previously reviewed image. Acting without a warrant, Officer Lee proceeded to review all the files for herself and confirmed that they did in fact depict child pornography. She relayed her conclusions to agents at Homeland Security Investigations (HSI), who relied on the information to obtain search warrants for Brillhart's apartment, car, and Yahoo and Google accounts.

On the morning of September 8, 2021, HSI Special Agent Elijah Cook executed the warrant on Brillhart's apartment. Brillhart shared the two-bedroom apartment with Rodney Dutra—himself a convicted child-pornography possessor who was later arrested for a parole violation arising out of this investigation. In Brillhart's bedroom, Special Agent Cook recovered a cellphone containing a micro-SD card. The card held 40 videos and 60 images of child pornography, including some involving victims as young as six months old. Six of the images matched files previously sent from reb3280@yahoo.com. Like the email accounts, the SD card contained selfies of Brillhart.

HSI agents separately executed a search warrant on Brillhart's Yahoo accounts, where they found emails welcoming Brillhart to Kik—an online messaging platform. The agents then searched "Reb Reb" on Kik and found another account, "flped4u," registered in August 2021. Upon searching Kik's records, the agents found more child pornography and Brillhart selfies, and they discovered that other Kik users had reported the account holder for introducing himself as "41M, pedo" from Fort Myers and for sending child pornography.

C

A grand jury indicted Brillhart on two counts: (1) distributing visual depictions of a minor engaged in sexually explicit conduct "on or about May 10, 2021," in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1); and (2) possessing and accessing with intent to view visual depictions of a prepubescent minor engaged in sexually explicit conduct "from on or about April 14, 2021, through on or about September 8, 2021," in violation of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2). Brillhart initially moved to dismiss the charges on the ground that the facts underlying them overlapped and, accordingly, that they violated the Double Jeopardy Clause. The district court denied the motion, concluding that the two counts were based on different images and conduct.

As relevant for purposes of appeal, Brillhart then moved to suppress the evidence gathered from his Google account, contending that the government's search violated the Fourth Amendment. The district court denied that motion as well, alternatively holding

(1) that Brillhart had no reasonable expectation of privacy in videos and images that he had voluntarily uploaded to his email accounts; (2) that the so-called "private search" doctrine vitiated any Fourth Amendment concerns because Google had discovered the child pornography in Brillhart's account through both human review and hash matching and because the government's ensuing search didn't reveal anything additional; and (3) that, in any event, the "good faith" exception protected Officer Lee's initial warrantless search.

On the eve of his trial, Brillhart moved under Federal Rule of Evidence 403 to prevent the government from introducing into evidence, publishing, or presenting testimony about graphic images or video clips depicting violence against infants or toddlers. The district court denied the motion, reasoning that the material constituted direct evidence of the charged offenses. Without personally reviewing the files in question, the court held that because the government intended to introduce only a limited number of images and videos, the danger of unfair prejudice didn't substantially outweigh their probative value.

The government also filed a motion in limine to prevent Brillhart from introducing a series of emails exchanged between his roommate, Dutra, and Dutra's then-girlfriend, Katie Morris, several of which referenced Brillhart and the HSI raid of their shared residence. Brillhart insisted that the emails supported his theory that Dutra had framed him. Although he acknowledged that not every email was relevant, he maintained that they were admissible

for the purpose of impeaching Dutra and Morris. The district court disagreed, excluding the emails as irrelevant and on hearsay grounds.

At trial, following the close of the government's case in chief, Brillhart argued that the evidence was insufficient to convict him and filed a motion for judgment of acquittal, which the district court denied. He also requested a jury instruction on his "theory of defense"—*i.e.*, that he was framed—asking the court to tell the jury "that [Dutra] had access to [Brillhart]'s room, email, phone, and other devices and downloaded the child pornography at issue." The court denied the request, deeming it sufficient to instruct jurors that Brillhart "can only be found guilty for what he has done." The jury convicted Brillhart on both counts.

At sentencing, Brillhart moved for additional psychological evaluations to assist the court in determining an appropriate sentence. The district court denied the motion, noting that Brillhart's mental-health history was already well documented: a bipolar-disorder diagnosis in 2000 and hebephilia[1] and sexual-sadism-disorder diagnoses in 2018. Brillhart also moved to continue sentencing, asserting a desire to attend a mental-health appointment and file an untimely new-trial motion. The court denied that motion, as well.

The district court enhanced Brillhart's sentence by five levels on the ground that he had engaged in a "pattern of activity involving the sexual abuse or exploitation of a minor" within the

[1] Hebephilia refers to an interest in early-adolescent pubescent children.

meaning of U.S.S.G. § 2G2.2(b)(5). It did so based on two of Brillhart's past offenses: a conviction for fourth-degree criminal sexual conduct arising out of a sexual encounter with a 15-year-old, and a probation violation arising out of a sexual encounter with a 16-year-old. Brillhart objected, arguing that controlling precedent required that each instance of abuse or exploitation itself match one of the statutory references listed in the Guidelines' commentary. He maintained that the probation violation involving the 16-year-old didn't match and therefore couldn't count toward the "pattern." The district court disagreed and sentenced Brillhart to the statutory maximum of 480 months on the distribution count and a concurrent 240 months on the possession count. At the same hearing, the court further found that the distribution and possession convictions violated the terms of Brillhart's supervised release related to an earlier conviction and, accordingly, imposed an additional two-year term of imprisonment. Sent'g Tr. at 4, 76, 86, Dkt. No. 245.

II

On appeal, Brillhart raises a total of 11 issues. First, and most significantly, he argues that the district court erred in relying on the "private search" doctrine to uphold against a Fourth Amendment challenge the warrantless search of a file identified as child pornography by Google through a hash-matching procedure; this automated process, he says, doesn't qualify as the sort of private search to which the doctrine applies. Second, Brillhart contends that child-pornography possession is a lesser-included offense of distri-

bution, and that by charging him with both the government violated the Double Jeopardy Clause. Third, he asserts that there was insufficient evidence to convict him on either count. Fourth, he argues that the district court abused its discretion by allowing the government to display child pornography to the jury—doubly so, he says, because the court did so without first reviewing the evidence. Fifth, Brillhart contends that the district court abused its discretion by excluding emails between his roommate, Dutra, and Dutra's then-girlfriend, Morris, which he says would have shown Dutra's motive and ability to frame him. Sixth, he asserts that the district court erred when it declined his proposed "theory of defense" jury instruction. Seventh, Brillhart argues that the district court abused its discretion at sentencing when it denied his motions for additional psychological examinations and a continuance. Eighth, he contends—and the government helpfully concedes—that the district court erred in applying the five-level pattern-of-activity enhancement under U.S.S.G. § 2G2.2(b)(5). Finally—ninth, tenth, and eleventh—Brillhart claims that his supervised-release-revocation sentence is invalid because the district court miscalculated the applicable Guidelines range, denied him an opportunity to allocute, and imposed a substantively unreasonable sentence.

A

We begin with Brillhart's most prominent contention—that Google's digital hash-matching protocol wasn't a valid private search, and that law enforcement's subsequent warrantless review of a file that Google had earlier confirmed to be child pornography

via hash matching thus violated the Fourth Amendment.[2] The government responds with three alternative bases for affirmance. First, at the threshold, it contends that Brillhart lacked any reasonable expectation of privacy in his illicit files and, therefore, that he enjoyed no Fourth Amendment protection. Second, the government argues that Google's hash match was a valid private search that permitted a law-enforcement officer to conduct a subsequent warrantless visual inspection of the images. And finally, it argues that regardless of the legality of the search, the applicability of the private-search doctrine is sufficiently debatable to implicate the good-faith exception to the warrant requirement.

The expectation-of-privacy issue is close, but we find that we needn't address it. Even if Brillhart had the requisite reasonable expectation of privacy, so as to trigger the Fourth Amendment's protection, we conclude—for reasons we will explain—that the private-search doctrine insulates law enforcement's warrantless review of Brillhart's emails here. And, because we hold that the private-search doctrine applies, we needn't address the downstream question whether the good-faith exception applies.

1

The private-search doctrine comprises two corollary principles. First, and most obviously, the Fourth Amendment "is wholly

[2] We review a denial of suppression for clear error on the facts and the application of law to facts de novo. *United States v. Perkins*, 787 F.3d 1329, 1344 (11th Cir. 2015).

inapplicable to a search or a seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official." *United States v. Castaneda*, 997 F.3d 1318, 1327 (11th Cir. 2021) (quoting *United States v. Jacobsen*, 466 U.S. 109, 113 (1984)). And second, so long as any ensuing search by government officers doesn't "exceed[] the scope of the private search," no Fourth Amendment issue arises. *Jacobsen*, 466 U.S. at 115. Accordingly, the key question in many private-search cases—including this one—is whether the government's search revealed anything materially more or different than what the private party had already discovered.

United States v. Jacobsen is the leading case. There, employees of a private-freight carrier discovered a damaged package. *Id.* at 111. Upon further inspection, they noticed something suspicious, so they summoned a DEA agent, alerting him to "a tube containing plastic bags and, ultimately, white powder." *Id.* at 111, 118. At that point, there was "a virtual certainty that nothing else of significance was in the package and that a manual inspection of the tube and its contents would not tell [the agent] anything more than he already had been told." *Id.* at 119. So even though the agent proceeded to visually inspect the contents of the package in greater detail, doing so "enabled [him] to learn nothing that had not previously been learned during the [company's] private search." *Id.* at 120. Accordingly, the Supreme Court held that the government's seizure and visual inspection of the package didn't violate the suspect's Fourth Amendment rights. *Id.* at 121–22.

Put simply, the private-search doctrine permits government agents to replicate and verify a private party's earlier search. And importantly, the fact that the government's search might be more thorough isn't disqualifying. In *United States v. Garcia-Bercovich*, 582 F.3d 1234 (11th Cir. 2009), for instance, we held that where a single shrink-wrapped pallet contained 13 boxes covered by a single shipping manifest, a private search of one of the boxes justified the warrantless search of the other 12. *Id.* at 1238. We reasoned that the district court's finding that "it was all one package" wasn't clearly erroneous and, therefore, that federal agents' additional investigation didn't exceed the scope of the earlier private search—and thus didn't violate the Fourth Amendment. *Id.* Our decision in *United States v. Simpson*, 904 F.2d 607 (11th Cir. 1990), is to the same effect. There, a FedEx employee found a package containing a folder with images of nude children, magazines with depictions of minors that might constitute child pornography, and videotapes that the employees determined contained sexually explicit material with actors that appeared to be minors. *Id.* at 609. We ultimately determined that the FBI's subsequent investigation of the same material didn't exceed the scope of the private search "simply because they took more time and were more thorough than the Federal Express agents." *Id.* at 610. It was enough that "[t]he box's contents had already been examined, their illicit character had been determined, and they were open for viewing by the time the [federal agents] arrived on the scene." *Id.*

To be sure, the private-search doctrine has limits. For instance, in *Walter v. United States*, a splintered Supreme Court held

that when a private actor opened a misdirected package and did nothing more than read the descriptive labels on videotapes without actually examining their contents, the government impermissibly expanded the scope of the search when it viewed the videos. 447 U.S. 649, 656 (1980) (plurality opinion); *see also id.* at 660–62 (White, J., concurring in part and concurring in the judgment). Our more recent decision in *United States v. Sparks*, 806 F.3d 1323 (11th Cir. 2015), nicely illustrates the doctrine's contours. That case involved multiple videos depicting child pornography. We concluded that a federal agent exceeded the scope of the private search when he viewed one of the videos, which the private party had never watched. *Id.* at 1336. But with respect to a video that the private party *had* watched, we reasoned that "[t]hough [the federal agent] may have looked at . . . the video more closely than did [the private actor] . . . the private party's earlier viewing of the same . . . video insulated law enforcement's later, more thorough review of [it] from transgressing the Fourth Amendment." *Id.*

2

As our descriptions indicate, to this point, most private-search cases (at least in this circuit) have involved a flesh-and-blood individual's review of a disputed piece of evidence. The central question here is whether Google's digital hash-value matching protocol should be treated the same way for private-search purposes. Recall, first, the nature of the hash value: A hash value is a string of characters that together constitute a file's unique "digital signature or fingerprint," such that "if two files ha[ve] the same hash value, they're the same file[.]" Tr. of Mot. to Suppress Hr'g at 20.

Recall, next, Google's particular hash-matching protocol: After an individual Google employee confirms through human review that a particular file depicts child pornography, that file's hash value is added to a company database along with a corresponding "industry classification" describing the file's contents. *Id.* at 101, 105. If, thereafter, an automated process reveals that another file's hash value matches one in the database, Google concludes—without further human review—that it's the same file and forwards it along with its classification to NCMEC. *Id.* at 121–22, 124.

Our sister circuits are split over whether hash matching constitutes a valid private search. The Fifth and Sixth Circuits have held that it does and, therefore, that a subsequent search by law enforcement of the same images falls within the scope of the hash-match search, and thus of the private-search doctrine. *See United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018)[3]; *United States v. Miller*, 982 F.3d 412 (6th Cir. 2020). In so holding, both courts emphasized the "near-perfect accuracy" of hash-value matching—which, they say, ensures that law enforcement "learn[s] nothing . . . that it had not already learned from the private search." *Reddick*, 900 F.3d at 640; *Miller*, 982 F.3d at 418.

The Second, Fourth, and Ninth Circuits have held, to the contrary, that a hash-value match cannot constitute a valid private search. *See United States v. Maher*, 120 F.4th 297, 314 (2d Cir. 2024);

[3] *Reddick* concerned Microsoft's hash-matching protocol. At least at the time of that case, this process was materially identical to Google's here. *See Reddick*, 900 F.3d at 637.

United States v. Lowers, 170 F.4th 134, 156 (4th Cir. 2026); *United States v. Wilson*, 13 F.4th 961, 971 (9th Cir. 2021). Although their approaches differ at the margins, all three courts have conceived of a digital file as akin to a "container[]" or a "sealed manila envelope" whose precise contents can't really be known until a human opens it. *Lowers*, 170 F.4th at 149 & n.9; *Maher*, 120 F.4th at 317 (analogizing digital files found on two separate email accounts to two different sealed containers in the physical world); *Wilson*, 13 F.4th at 973, 977 n.13 (emphasizing that the image files were "unopened"). They have also emphasized that because Fourth Amendment rights are "personal," a private search that uses information gleaned from a file that was once in the possession of a third party can't defeat the suspect's privacy interests, even in the very same file. *Lowers*, 170 F.4th at 153–54; *Maher*, 120 F.4th at 319; *Wilson*, 13 F.4th at 975.

3

We agree with the Fifth and Sixth Circuits, and thus hold that Google's application of its hash-matching protocol to Brillhart's file qualifies as a valid private search. Through hash matching, Google simply used a computer to save one flesh-and-blood individual the trouble of having to confirm what another (or perhaps even the same) flesh-and-blood individual had already concluded. It's worth noting at the outset that, at least as Google employs it, hash-value matching doesn't replace human review entirely. Rather, at step one, so to speak, an individual Google employee reviews a file, determines that it depicts child pornography,

assigns it a hash value and classification, and enters it into the company's database. *See* Tr. of Mot. to Suppress Hr'g at 76, 101. It is only at step two that the automated hash match occurs: A computer compares a new file's hash value against those in the database known to depict child pornography and, if (but only if) there's a match, reports the new file as child pornography. *Id.* at 124.[4]

Under Supreme Court precedent, the controlling question is whether there is "virtual certainty" that law enforcement will find "nothing else of significance" in its own review that hadn't already been revealed by the private search—here, that the digital file depicts child pornography. *Jacobsen*, 466 U.S. at 119. We are satisfied that the search at issue here satisfies that test.

To be sure, a degree of apprehension is understandable; to date, the norm has been stem-to-stern human review. In point of fact, though, a computer comparing digital hash values is almost surely *less* likely to slip up and mismatch two images than is a human being eyeballing them. After all, "[m]ost people who view images do not use a magnifying glass to undertake a pixel-by-pixel inspection" of the sort that hash matching inherently entails. *Miller*, 982 F.3d at 430.

[4] As there was prior human review of the file at issue in this case, we needn't decide whether the Fourth Amendment requires that a qualifying private search entail human involvement.

And to be clear, hash matching's "near-perfect accuracy," *id.* at 418, isn't just theoretical; uncontested record evidence demonstrates it. As already noted, at the suppression hearing in this case, an e-crimes investigator described a hash value as "a unique digital signature"—meaning, she said, that "if two files had the same hash value, they're the same file." Tr. of Mot. to Suppress Hr'g at 7, 20. The flip side, she said, is also true: There is no "reason why [two files] would have different hash values if they're the same file." *Id.* at 73. Importantly, she distinguished a hash value from a file name: Unlike a unique hash value, she explained, "we could have ten images that have the same filename that are all different images." *Id.* A custodian of records at Google later confirmed that a hash value is a "digital fingerprint," widely used to "fight online [child porn] across industry." *Id.* at 101, 121. There was no evidence to the contrary.[5]

Even beyond the record in this case, there is a broad consensus among courts that have considered the issue that hash matching is a practically fool-proof way to confirm that two files are indeed one and the same. In *Miller*, for instance, the Sixth Circuit pointed to an article published by the Federal Judicial Center, which confirms that hash values are "so distinctive that the chance that any two data sets will have the same one, no matter how similar they appear, is less than one in one billion." *Miller*, 982 F.3d at

[5] In this sense, our record is distinguishable from that the Fourth Circuit confronted in *Lowers*; there, "no record evidence" supported the finding that hash-matching technology was "exceedingly reliable." *Lowers*, 170 F.4th at 148.

430 (quoting Barbara J. Rothstein et al., *Managing Discovery of Electronic Information: A Pocket Guide for Judges* 38 (2d ed. Fed. Jud. Ctr. 2012)). That court also noted a manual published by a state government agency stating that "[t]he chance of two [different] files coincidentally sharing the same hash value is 1 in 9,223,372,036,854,775,808." *Id.* (quoting *United States v. Dunning*, 2015 WL 13736169, at *2 (E.D. Ky. Oct. 1, 2015)).

Other courts—notably including even those that have held that hash matching does *not* constitute a valid private search—have likewise credited findings that, practically speaking, "no two dissimilar files will have the same hash value." *United States v. Cartier*, 543 F.3d 442, 446 (8th Cir. 2008); *accord United States v. Wellman*, 663 F.3d 224, 226 n.2 (4th Cir. 2011) ("In the present case, the district court found that files with the same hash value have a 99.99 percent probability of being identical."); *United States v. Owens*, 18 F.4th 928, 932 n.1 (7th Cir. 2021) (noting that experts on both sides agreed that "if the hash value of two files matches up, then the chances are 'astronomically small' that the two files are different"); *United States v. Rosenschein*, 136 F.4th 1247, 1258 (10th Cir. 2025) (crediting evidence that describes a hash-value error rate as "one in fifty billion"); *United States v. Gasperini*, 729 F. App'x 112, 114 (2d Cir. 2018) ("Matching of hash values is an established method for authenticating digital evidence."); *Wilson v. Gamboa*, 2025 WL 2977246, at *1 (9th Cir. Oct. 22, 2025) ("Both the [defendant's] proposed expert and the State's expert affirm that hash values, even if they do not portray the contents of an image, are unique and thus identify an image.").

4

Respectfully, we aren't persuaded by the Second, Fourth, and Ninth Circuits' reasons for refusing to apply the private-search doctrine to tech companies' hash-matching investigations. Those courts, we think, have made three key missteps.

a. First, and perhaps most notably, they analogized a file's hash value to the descriptive film-box "label" in *Walter*, the viewing of which was deemed insufficient to authorize law enforcement's later examination of the film itself. *See Maher*, 120 F.4th at 318; *Lowers*, 170 F.4th at 155; *Wilson*, 13 F.4th at 973. The label in *Walter* consisted of "suggestive drawings" and "explicit descriptions of the contents," 447 U.S. at 652—or, as the lower court there explained, the "title of the individual movie" and "a detailed description, in explicit terms, of the . . . acts depicted in the film," *United States v. Sanders*, 592 F.2d 788, 791 (5th Cir. 1979), *rev'd sub nom. Walter*, 447 U.S. 649.

The label analogy doesn't hold up, and a bit more tech talk will explain why. At bottom, a digital image file is a grid of pixels, each of whose color and brightness are encoded as patterns of 1s and 0s. *See* Christopher J. Buccafusco, *Gaining/Losing Perspective on the Law, or Keeping Visual Evidence in Perspective*, 58 U. Mia. L. Rev. 609, 614–15 (2004) (explaining that in the case of digital photographs, "the light entering the lens of the digital camera is reflected off a sensor that records the data in binary form and stores it in a file"). So when a person "opens" a file, he isn't really revealing what's "inside"; rather, he's instructing the computer to render a

collection of 1s and 0s into a colorful grid. A hash value is a fixed-length string of characters produced by a computer function. That function takes the binary 1s and 0s that constitute an image and, through a series of operations that repeatedly deconstruct, manipulate, and reshuffle the underlying data, produces a hash string. This resulting string is shorter than the 1s-and-0s binary, which facilitates mass storage and easy retrieval, but it's long enough to minimize (essentially to zero) the risk of misidentification.[6]

In plain English: A hash value isn't a "label" describing what's inside a file; it's a one-way transformation of the file's insides, produced from the same 1s and 0s that form the image that appears on the screen. Put a little differently, a hash value isn't a badge meant to describe the content "contained" inside a file, *Lowers*, 170 F.4th at 155—it *is* the content. In this case, at some point in the past a human being at Google determined that the 1s and 0s

[6] In an "MD5" hash like the one that seems to be at issue here, *see* Tr. of Mot. to Suppress Hr'g at 20, 135, a character that would show as a 1 or a 0 in binary is instead rendered as one of 16 "hexadecimal" characters: 0-9 or a-f. This allows for a more condensed presentation of data, as each "hex" character represents a unique configuration of four 1s and 0s. *See Pyrotechnics Mgmt. v. XFX Pyrotechnics*, 38 F.4th 331, 335 n.4 (3d Cir. 2022). By way of illustration, 0111 is "7" in hexadecimal. *See Lotus Dev. Corp. v. Paperback Software Intern.*, 740 F. Supp. 37, 44 (D. Mass. 1990). Though an MD5 hash-value is typically fixed at 32 characters and therefore inevitably and irreversibly condenses files larger than 128 bits, the transformation is still based on—and uniquely linked to—a file's complete set of bits. *See generally* Ronald Rivest, *The MD5 Message-Digest Algorithm*, MIT Lab'y for Comp. Sci. & RSA Data Sec., Inc. (1992), https://datatracker.ietf.org/doc/html/rfc1321 [https://perma.cc/DKY2-HMTA] (describing the MD5 process).

that constituted the image in question, when rendered into visual form, depict child pornography; the subsequent hash match merely replicated that determination digitally. So again, the analogy to the label in *Walter* just doesn't reflect technical reality.

b. The Second, Fourth, and Ninth Circuits separately concluded that a hash-match search isn't sufficiently detailed to qualify for private-search treatment. *See Maher*, 120 F.4th at 315; *Lowers*, 170 F.4th at 154–55; *Wilson*, 13 F.4th at 972. The Fourth Circuit, for instance, asserted that a hash value provides "no useful information" and, unlike a police report following a manual search, fails to "describ[e] the contents of the image." *Lowers*, 170 F.4th at 154–55. Technical misconceptions aside—again, the hash value is a fingerprint that represents and identifies "the contents of the image"—we think those courts imposed too heavy a burden. In *Jacobsen*, the Supreme Court never said anything about the details of the private parties' inspection and subsequent tip—only that "[w]hen they observed the white powder in the innermost bag, they notified" the DEA. 466 U.S. at 111. The Court there emphasized that what matters is the "virtual certainty that nothing else of significance [is] in the package" beyond what the private search revealed "and that a manual inspection of the [package] would not tell [a law-enforcement officer] anything more" than he already knew. *Id.* at 119.

Nor has this Court read *Jacobsen* to require a private party's search to be particularly thorough—let alone as thorough as the

search subsequently conducted by law enforcement. To the contrary, we've held that it's enough that a private search "examine[d]" the contents of a package in sufficient detail to "determine" its "illicit character." *Simpson*, 904 F.2d at 610. A requirement that private entities furnish law enforcement with comprehensive reports detailing their exact impressions would—we think perversely—condition the private-search doctrine's application on the quality and accuracy of a private party's investigatory capabilities. *Cf. Wilson*, 13 F.4th at 972–74 (emphasizing the lurid, specific details the government uncovered through its investigation that weren't contained in the private tip, including vivid descriptions of the victim and the sexual acts depicted).

Where we and others have determined that a governmental search exceeded the scope of an earlier private search, it has been because government officers viewed items (videos, files, etc.) that the private party hadn't. *See, e.g.*, *Sparks*, 806 F.3d at 1336 (reasoning that law enforcement's examination of a previously unreviewed video violated the private-search doctrine, whereas its examination of a previously reviewed video did not); *see also, e.g.*, *United States v. Ackerman*, 831 F.3d 1292, 1306 (10th Cir. 2016) (Gorsuch, J.) ("[T]he undisputed facts before us indicate that NCMEC opened Mr. Ackerman's email first and did so before and in order to view not just the attachment that was the target of AOL's private search [conducted via hash matching] but three others as well . . . . [E]ach of these steps—opening the email and viewing the three other attachments—was enough to risk exposing private,

noncontraband information that AOL had not previously examined."). These decisions indicate that the "scope" of a private search relates more to its "breadth"—whether a private party's review extended to a particular file—than its "depth." An industry-standard hash-match report—which provides the file's hash value and the same file's prior human-reviewed classification—is therefore sufficiently detailed to ensure that further police review will reveal nothing materially new or different about the file.

c. Finally, stressing that Fourth Amendment rights are "personal," the Second, Fourth, and Ninth Circuits concluded that an earlier determination by a private party that a file *in another individual's possession* constituted illicit material can't inform the validity of the search of the suspect's own files. *See Lowers*, 170 F.4th at 153–54; *Maher*, 120 F.4th at 319; *Wilson*, 13 F.4th at 974. For support, the Fourth Circuit invoked the hornbook principle that *"a defendant* can mount a Fourth Amendment challenge only if *he* has *his own* cognizable Fourth Amendment privacy interest in the invaded place"—and, importantly, asserted that the "inverse must also be true." *Lowers*, 170 F.4th at 153–54 (emphases added) (quoting *United States v. Green*, 106 F.4th 368, 375 (4th Cir. 2024)). That is, "[i]f [the defendant] could not challenge a government search of someone else's files because that search did not implicate his privacy interests, then [a private party's] visual examination of a third-party's files could not affect, much less frustrate, [the defendant's] expectation of privacy in his own unopened files." *Id.* at 154.

We're not so sure. The question here isn't whether a defendant can invoke his Fourth Amendment rights in this context but, rather, whether he has any Fourth Amendment interests to invoke. And for reasons we've explained, at the point that a private party conducts a search, those interests—at least insofar as the government's ensuing search doesn't exceed the scope of the private party's—dissipate.

By its very nature, hash matching ensures a decisive personal link to the suspect. As it applies here, it guarantees that the same file that an individual Google employee previously flagged as depicting child pornography has reappeared in the suspect's own account. Accordingly, a Google employee's earlier judgment about the same file is, by virtue of the hash match, pertinent to the company's determination that the suspect, based on *his own* actions, has acquired child pornography.

* * *

For the foregoing reasons, we hold that the private-search doctrine applies and that law enforcement's search following Google's hash match didn't violate Brillhart's Fourth Amendment rights.

B

Next up, double jeopardy. In relevant part, the Fifth Amendment states that "[n]o person shall be . . . subject for the same offence to be twice put in jeopardy of life or limb." U.S. Const. amend. V. Brillhart contends that his double-jeopardy rights were violated when he was convicted of both possession and

distribution of child pornography.[7] To determine if two "offence[s]" are "the same" within the meaning of the Double Jeopardy Clause, we examine whether "each provision requires proof of a fact which the other does not." *Blockburger v. United States*, 284 U.S. 299, 304 (1932). "[T]he *Blockburger* test focuses on the proof necessary to prove the statutory elements of each offense, rather than on the actual evidence to be presented at trial." *Illinois v. Vitale*, 447 U.S. 410, 416 (1980). The questions for us, therefore, are (1) whether under 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) possession requires distribution; and (2) whether under 18 U.S.C. §§ 2252(a)(2) and (b)(1) distribution requires possession.

We hold that distribution and possession of child pornography are distinct offenses. It is self-evident, we think, that the possession of a thing doesn't require its distribution. The real question is whether the distribution of a thing requires its possession. We've previously held, albeit in the drug context, that it doesn't: "While possession will undoubtedly be present in most instances of distribution, neither the statutory language nor the cases involving distribution support the proposition that a showing of possession is required." *United States v. Brunty*, 701 F.2d 1375, 1381 n.16 (11th Cir. 1983). That logic applies every bit as much to child pornography as it does to narcotics. And it's not quite as counterintuitive as it might initially seem. Distribution of an illicit thing, after all,

[7] We review de novo the question whether a defendant's convictions violate the Double Jeopardy Clause. *United States v. Ford*, 784 F.3d 1386, 1392 (11th Cir. 2015).

"may also consist of or include other acts perpetrated in furtherance of sale" that don't necessarily require possession of the thing, "such as arranging or supervising the delivery or negotiating for or receiving the purchase price." *Id.* at 1381; *see also United States v. Oquendo*, 505 F.2d 1307, 1310 (5th Cir. 1975) (upholding the distribution conviction of a defendant who arranged the sale of a small amount of heroin without ever possessing the substance).[8] A child-pornography broker or a digital-platform operator fits that bill.

In so holding, we join several of our sister circuits, which have extended the distribution-doesn't-require-possession logic from drugs to child pornography. *See United States v. Chiaradio*, 684 F.3d 265, 280 (1st Cir. 2012); *United States v. Woerner*, 709 F.3d 527, 539 (5th Cir. 2013); *United States v. McElmurry*, 776 F.3d 1061, 1064–65 (9th Cir. 2015). Brillhart's reliance on *United States v. Schaff*, 838 F. Supp. 2d 1376, 1377 (S.D. Ga. 2011), which in turn relies on *United States v. Bobb*, 577 F.3d 1366 (11th Cir. 2009), is misplaced. *Bobb* addressed *receipt* and possession, not distribution and possession. Needless to say, "if a person takes 'receipt' of a thing, [he] necessarily must 'possess' the thing." *Id.* at 1373. But for reasons already explained, the same doesn't necessarily hold for distribution.

Because possession of child pornography is distinct from—and not "the same offence" as—distribution, Brillhart's indictment

[8] Former Fifth Circuit decisions issued before October 1, 1981, are binding precedent in this Circuit. *Bonner v. City of Prichard*, 661 F.2d 1206, 1209 (11th Cir. 1981) (en banc).

and conviction on both counts didn't violate the Double Jeopardy Clause.

C

Brillhart also contends that the evidence was insufficient to sustain his convictions.[9] We disagree.

We start with the distribution count, for which the evidence was ample. First, a Yahoo account flagged for sending child pornography included Brillhart's initials and birthdate in the address, was registered under his initials, and was verified with his phone number. *See* Trial Tr. vol. 1, Feb. 5, 2024, at 29–32, 42, Dkt. No. 194; Trial Tr. vol. 2, Feb. 6, 2024, at 68–72, Dkt. No. 195. Second, an email containing a selfie of Brillhart was sent from his phone to his Yahoo account and then forwarded to a recipient to whom he had previously sent child pornography. *See* Trial Tr. vol. 2, Feb. 6, 2024, at 71. And finally, six child-pornography files were later found on Brillhart's phone that matched the email attachments sent from this Yahoo account. *Id.* at 79–80. Based on that evidence, a reasonable jury could clearly have concluded that Brillhart distributed child pornography.

The evidence supporting Brillhart's possession conviction is also plentiful. Most damningly, there was child pornography on

[9] We review challenges to the sufficiency of the evidence de novo, with all evidence viewed in the light most favorable to the jury's verdict and all reasonable inferences and credibility choices made in favor of the verdict. *United States v. Gamory*, 635 F.3d 480, 497 (11th Cir. 2011).

Brillhart's phone and SD card, both of which were found in his bedroom. *Id.* at 18–21, 42. Brillhart claims that he was framed by his roommate, Dutra. But his theory is belied by two key pieces of evidence. First, on August 9, 2021, Brillhart used his phone to take selfies, and, during the same five-and-a-half-minute span, his phone recorded child-porn downloads. *See id.* at 93–94, 100–01. And second, on August 14 and 15, a user "Reb Reb" from Fort Myers introduced himself as "41M, pedo" in Kik chatrooms shortly before sharing child pornography; at that time, Dutra had suffered a stroke and was hospitalized and mostly incapacitated. *See id.* at 148–49, 178–80, 187–89, 233, 244, 247–50. In any event, "we are bound by the jury's determination of [Brillhart's] credibility . . . and by its rejection of the inferences raised by [him]." *United States v. Glinton*, 154 F.3d 1245, 1258 (11th Cir. 1998).

D

Brillhart separately challenges the district court's admission and display of several images and videos depicting child pornography.[10] He first contests the district court's refusal to exclude the evidence as unduly prejudicial under Federal Rule of Evidence 403. Rule 403 permits a district court to exclude otherwise relevant evidence "when its probative value is substantially outweighed by its unfairly prejudicial nature." *United States v. Alfaro-Moncada*, 607 F.3d 720, 735 (11th Cir. 2010) (citing Fed. R. Evid. 403). However, exclusion under Rule 403 "is an extraordinary remedy which the

[10] We review all evidentiary rulings for abuse of discretion. *United States v. Dodds*, 347 F.3d 893, 897 (11th Cir. 2003).

district court should invoke sparingly." *Id.* (citation modified). We've affirmed district courts' admission of child pornography as probative of both the "thing" possessed and defendants' knowledge that the "thing" is in fact child pornography. *E.g.*, *id.*; *United States v. Dodds*, 347 F.3d 893, 899 (11th Cir. 2003); *see also United States v. Ewing*, 140 F.4th 1339, 1350 (11th Cir. 2025). So too here. The district court did not abuse its discretion in opting not to exclude the evidence under Rule 403.

Brillhart separately asserts that the district court erred by declining to view the images before they were presented to the jury. This Court recently rejected an identical argument in *Ewing*, and we are bound by that decision here. Like the defendant there, Brillhart made no "specific objection" to particular photos and videos at trial, but rather objected (and continues to object) to the general obscenity in the videos and the "blind rage" they would inspire in the jury. *Compare Ewing*, 140 F.4th at 1350, *with* Br. of Appellant at 17. While district courts "should ordinarily review pornographic images before ruling on an objection to those images under Rule 403," failure to do so in these circumstances is not an abuse of discretion. *Ewing*, 140 F.4th at 1350–51 ("[W]e cannot say the district court erred in denying [Ewing's] general objection without first viewing specific images.").[11]

[11] Reprising his theory that he was framed, Brillhart also argues that the district court abused its discretion by excluding as irrelevant and/or hearsay certain emails between his roommate Dutra and Dutra's then-girlfriend Katie Morris that were exchanged the year after Brillhart was charged. Although Brillhart asserts that the emails prove that Dutra had access to his phone and had a

E

We turn next to Brillhart's objections to the district court's jury instructions.[12] Brillhart contends that the district court erred by refusing to instruct the jury that "another person, the defendant's roommate at the time, had access to the defendant's room, email, phone, and other devices and downloaded the child pornography at issue." Brillhart's Proposed Am. Jury Instrs. at 22, Dkt. No. 153. We disagree. Brillhart's proposed instruction was "more in the nature of a jury argument than a charge"; accordingly, "far from being erroneous," it was "actually quite correct" for the district court to refuse to give it. *United States v. Barham*, 595 F.2d 231, 244–45 (5th Cir. 1979); *see also United States v. Hill*, 643 F.3d 807, 856 (11th Cir. 2011) (same). The district court instructed the jury that Brillhart could be found guilty only if the government proved that he committed each element of the statutory offense. Trial Tr. vol. 3, Feb. 7, 2024, at 144, Dkt. No. 196. That was sufficient. *See United States v. Ndiaye*, 434 F.3d 1270, 1293 (11th Cir. 2006) (explaining that

---

motive to accuse him, none of the emails even mention Brillhart's phone or the digital accounts that underlie his indictment, and were otherwise irrelevant in that they reflected (at most) the relationship between the parties months after the HSI raid. *See United States v. De La Cruz Suarez*, 601 F.3d 1202, 1216 (11th Cir. 2010) (excluding a statement "made after the fact, not at the time of the incident"). Accordingly, we hold that the district court did not reversibly err in excluding the emails.

[12] We review a district court's refusal to give a requested jury instruction for abuse of discretion. *United States v. Carrasco*, 381 F.3d 1237, 1242 (11th Cir. 2004).

"[t]he district court should instruct the jury on the defendant's defense theory if the theory has a foundation in evidence and legal support" but that "a more specific instruction on a 'theory of the defense' is not warranted when the charge given adequately covers the substance of the requested instruction" (citation modified)).

F

Brillhart raises two sentencing-related challenges. First, citing both 18 U.S.C. § 3552(c) and 18 U.S.C. § 4241(a), he argues that he was entitled to a last-minute psychological exam and a continuance during which the exam could be conducted.[13] But in the circumstances presented, neither statute required the district court to grant him the requested relief. Using permissive language, § 3552(c) states that "[i]f the court . . . desires more information than is otherwise available to it . . . the court *may* order the same psychiatric or psychological examination and report thereon as *may* be ordered under section 4244(b) of this title." 18 U.S.C. § 3552(c) (emphases added). Here, though, the district court had sufficient information to assess Brillhart's mental condition based on his previous examinations and diagnoses, the most recent of which was from 2021, the year Brillhart committed his crimes. *See* Sent'g Tr. at 42. And § 4241(a) requires "reasonable cause" to conclude that a defendant is "suffering from a mental disease or defect rendering

[13] We review the district court's denial of a presentence psychological examination, as well as its denial of a motion of continuance, for abuse of discretion. *United States v. Nickels*, 324 F.3d 1250, 1251 (11th Cir. 2003); *United States v. Valladares*, 544 F.3d 1257, 1261 (11th Cir. 2008).

him mentally incompetent" for sentencing purposes. 18 U.S.C. § 4241(a). But Brillhart never claimed to be incompetent, and there weren't any independent bases suggesting that his mental-health issues deprived him of the "sufficient present ability to consult with his lawyer with a reasonable degree of rational understanding" or "a rational as well as factual understanding of the proceedings against him," as would have been required to demonstrate incompetence. *United States v. Cruz*, 805 F.2d 1464, 1479 (11th Cir. 1986) (quoting *Dusky v. United States*, 362 U.S. 402, 402 (1960)). In the circumstances presented, the district court didn't abuse its discretion in denying either the motion for investigation or the continuance.

Second, Brillhart objects to the district court's application of a five-level pattern-of-activity enhancement under U.S.S.G. § 2G2.2(b)(5).[14] The government agrees with Brillhart that the district court erred in applying the enhancement, and so do we. In *Alberts*, we held that "only conduct that falls within one of the statutory sections referenced in the definition of 'sexual abuse or exploitation' in § 2G2.2(b)(5)'s application notes can justify a 'pattern of activity' enhancement." 859 F.3d at 984.[15] Brillhart has only one

[14] We review the district court's application of the Sentencing Guidelines de novo and factual findings for clear error. *United States v. Alberts*, 859 F.3d 979, 982 (11th Cir. 2017).

[15] Neither party argued here or below that the holding of *Alberts* was in any way disturbed by *United States v. Dupree*, 57 F.4th 1269 (11th Cir. 2023) (en banc). We therefore decline to consider any ramifications that our decision there might have on the continuing force of *Alberts* here. *See United States v.*

qualifying episode: a conviction in Michigan for fourth-degree sexual misconduct involving a 15-year-old. *See* Sent'g Tr. at 9. His only other relevant violation, arising out of a sexual encounter with a 16-year-old, doesn't match any of the crimes enumerated in § 2G2.2(b)(5)'s application notes. *See* U.S.S.G. § 2G2.2(b)(5) cmt. n.1; Sent'g Tr. at 13–14. So we're left with one, and a pattern of one is no pattern. Accordingly, the district court erred in applying this enhancement.[16]

III

To recap what is an unavoidably long opinion, we hold as follows: First, Google's identification of one of Brillhart's child-pornography files through its semi-automated hash-matching pro-

---

Lusk, 119 F.4th 815, 826 n.7 (11th Cir. 2024) (declining to decide a *Dupree* objection that wasn't properly preserved); *United States v. Jews*, 74 F.4th 1325, 1327 n.2 (11th Cir. 2023) (distinguishing *Dupree* on the ground that neither party contested the validity of the Guidelines commentary).

[16] Because we vacate and remand for resentencing, Brillhart's appeal of his supervised-release-revocation sentence—which was determined at the same hearing, premised on the underlying convictions, and imposed alongside his other sentence—is moot. *Cf. United States v. Fowler*, 749 F.3d 1010, 1015 (11th Cir. 2014) ("A criminal sentence in a multi-count case is, by its nature, 'a package of sanctions that the district court utilizes to effectuate its sentencing intent consistent with the Sentencing Guidelines' and with the § 3553(a) factors." (quoting *United States v. Stinson*, 97 F.3d 466, 469 (11th Cir.1996))).

On remand, the district court may wish to consider the applicability of 18 U.S.C. § 3583(k).

tocol was a valid "private search" that authorized law enforcement's subsequent warrantless review of that same file. Second, possession of child pornography is not the same offense as distribution of child pornography for double-jeopardy purposes. Third, fourth, fifth, and sixth, the district court did not err in denying Brillhart's motion for judgment of acquittal, denying his motion to exclude from the jury's consideration several images depicting child pornography, excluding emails between Brillhart's roommate and the roommate's then-girlfriend, and declining to instruct the jury regarding his argument that he had been framed. Seventh, the district court did not err in denying Brillhart's sentencing-phase request for additional psychological evaluations and a continuance. With respect to all of those issues, we affirm.

But eighth, the district court did err in applying the pattern-of-activity enhancement under U.S.S.G. § 2G2.2(b)(5). With respect to that issue, we vacate and remand for resentencing, and dismiss as moot Brillhart's claims that relate to the validity of his supervised-release-revocation sentence.

AFFIRMED IN PART, VACATED AND REMANDED IN PART, DISMISSED IN PART.

Dr

In the

United States Court of Appeals

For the Eleventh Circuit

No. 24-13226

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

versus

RICHARD EDWARD BRILLHART,

Defendant-Appellant.

Appeal from the United States District Court
for the Middle District of Florida
D.C. Docket No. 2:22-cr-00053-SPC-NPM-1

No. 24-13232

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

versus

RICHARD EDWARD BRILLHART,

Defendant-Appellant.

Appeal from the United States District Court
for the Middle District of Florida
D.C. Docket No. 2:03-cr-00121-JES-KCD-1

Before NEWSOM, LUCK, Circuit Judges, and LEIBOWITZ,* District Judge.

PER CURIAM:

The Petition for Rehearing En Banc is DENIED, no judge in regular active service on the Court having requested that the Court be polled on rehearing en banc. FRAP 40. The Petition for Panel Rehearing also is DENIED. FRAP 40.

---

*Honorable David S. Leibowitz, United States District Judge for the Southern District of Florida, sitting by designation.

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
FORT MYERS DIVISION

UNITED STATES OF AMERICA

v. CASE NO.: 2:22-cr-53-SPC-NPM

RICHARD EDWARD BRILLHART

OPINION AND ORDER[1]

Before the Court is Defendant Richard Brillhart's Motion to Suppress (Doc. 56), along with the Government's opposition (Doc. 57). The Court held an evidentiary hearing, which Defendant attended with counsel. (Doc. 70). The Court reserved ruling at the hearing's conclusion but now issues this decision to explain why it denies the Motion.

BACKGROUND

This case is about child pornography—distribution and possession. (Doc. 1). And Defendant's motion is about how law enforcement discovered the contraband. The short story is Defendant allegedly emailed hundreds of child pornography images and videos through his Yahoo and Google accounts and uploaded files to Google Photos. Defendant did so all within about a one month

[1] Disclaimer: Papers hyperlinked to CM/ECF may be subject to PACER fees. By using hyperlinks, the Court does not endorse, recommend, approve, or guarantee any third parties or their services or products, nor does it have any agreements with them. The Court is not responsible for a hyperlink's functionality, and a failed hyperlink does not affect this Order.

span.[2] When Yahoo and Google discovered Defendant's conduct, they notified the National Center for Missing and Exploited Children (NCMEC), which is a clearinghouse for electronic service providers to report child sexual abuse material. Yahoo and Google also attached the offending files. NCMEC then forwarded the files to law enforcement, who viewed them without a warrant. Based on what they saw and further investigation, law enforcement secured search warrants, the evidence from which led to Defendant being indicted for child pornography offenses.

Defendant now seeks the Fourth Amendment's protection. He moves to suppress all evidence against him because law enforcement performed an unlawful search by viewing the images and videos from Yahoo and Google without a warrant. At the hearing, the Government introduced twenty-one exhibits and called three witnesses: (1) Jordyn Kramer, a Yahoo custodian of records and investigator on its E-Crimes Investigation Team; (2) Anjali Shrestha, a Google custodian of records and team lead for its Legal Investigations Support team; and (3) Katrina Lee, a South Florida Internet Crimes Against Children Task Force Officer ("TFO Lee").[3] (Doc. 70-1).

[2] This all allegedly occurred approximately five months of Defendant being released from federal prison for possessing child pornography. *See United States v. Brillhart*, No. 2:03-cr-121-JES-121 (M.D. Fla. 2006) (sentencing Defendant to 240 months' imprisonment for possession of materials involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2252(a)(4)(B) and 2252(b)(2)).

[3] TFO Lee's last name was O'Brien during the relevant parts of the investigation.

Defendant introduced three exhibits but offered no witnesses. (Doc. 70-23). The relevant facts are not in dispute. Even so, the Court makes these factual findings material to the Motion based on the evidence presented:

Between April 15 and May 25, 2021,[4] Yahoo and Google filed seven cybertips to NCMEC about child pornography found on Defendant's accounts. Their information led to NCMEC generating nine CyberTipline Reports: four reports and two supplements based on Defendant's Yahoo activity, and three reports based on his Google activity. Information from Yahoo and Google common in all the Reports included details on the

- user names provided when he registered the accounts, a birthday, mobile phone numbers, email addresses, and IP addresses
- MD5 hash values,[5] and where the files were located (e.g., email attachments)
- emails the user exchanged with the child pornography, including dates and times, sent and received, and attachments

(Doc. 70-2 to Doc. 70-10).

Aside from Yahoo's and Google's information, NCMEC added its own material to the Reports. For example, NCMEC pinpointed Defendant's

[4] Unless otherwise indicated, all dates in this Opinion and Order occurred in 2021.

[5] A hash value is a unique string of letters and numbers that reflects the content of an image or video file and is created using a common algorithm like MD5. The series of letters and numbers are a file's digital fingerprint. Generally, electronic service providers assign a hash value to a known child pornography image or video. They scan a designated repository for files with the same value. When they get a "match," they know the scanned file is a duplicate of the child pornography without needing to open or view the file.

approximate geolocation running the IP addresses that Yahoo and Google gave through "a publicly-available online query." NCMEC also used "publicly-available, open-source websites" to identify Defendant as a registered sex offender, and it named other related CyberTipline reports. Now for specifics on each report.

a. Yahoo CyberTipline Report 89005640 and Supplemental Report 89347533

On April 15, Yahoo alerted NCMEC about six child pornographic images, which led to CyberTipline Report 89005640. (Doc. 70-2). Yahoo identified "richard bri" as the suspect who sent six emails through its platform, each of which attached an image categorized as "A1."[6] A Yahoo employee viewed each image to confirm its content before sending them to NCMEC. Upon receiving the information, an NCMEC staff member viewed one file. NCMEC also used its hash tag technology to confirm all the images were child pornography.

On April 23, Yahoo submitted a supplemental report to NCMEC that said more about Defendant and the images:

> The Yahoo accounts jobs4rich@yahoo.com reported for sharing [child sexual abuse imagery ("CSAI")] using Yahoo Mail, as observed in CyberTip 89005640. The

[6] The A1 label is based on an industry classification system that electronic service providers use to identify content in illicit material. A1 means content showing a prepubescent minor engaging in a sex act. A "sex act" is defined as "[a]ny image of sexually explicit conduct (actual or simulated sexual intercourse genital-genital, oral-genital, anal-genital, or oral-anal whether between persons of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value." (Doc. 70-2).

> CSAI reported in this CyberTip includes approximately 6 images of nude prepubescent female children, some of whom are engaged in sexual acts with adult males.
>
> Based on the login records and subscriber information for the user's Yahoo account along with open source research, the user appears to be an individual named Richard Edward Brillhart III (BRILLHART), residing in or around Fort Myers, Florida. A further investigation by the Verizon Media E-Crimes Investigations Team (VM-ECIT) has revealed that Brillhart appears to be a Registered Sex Offender in Florida for a prior sex crime conviction involving a child (committed in Michigan).

(Doc. 70-6). It also provided two IP addresses "located in or around Fort Myers, Florida" for "recent successful logins" from the Yahoo account. (Doc. 70-6 at 4). Finally, it provided an address for Defendant: 5446 Tenth Avenue in Fort Myers, Florida 33907.

b. Yahoo CyberTipline Report 90109206

Yahoo provided a second Cybertip on May 12 that led to Report 90109206. (Doc. 70-3). This time, Defendant operated under the account name "REB REB" and used the email address reb3280@@yahoo.com to exchange about two dozen emails with 271 videos and images attached. A Yahoo employee viewed each file to confirm the child pornography content before sending them to NCMEC. Many files were also designated as A1 material.

When NCMEC received the report, a staff member viewed twenty-two files to confirm the child pornography and the other images were run through its hash tag technology.

c. Yahoo CyberTipline Report 90418734

On May 17, Yahoo again contacted NCMEC about more emails involving child pornography that Defendant exchanged. (Doc. 70-4). According to the report, reb3280e@yahoo.com exchanged four emails with ten attached videos with another user. For each video, a Yahoo employee viewed the entire content to confirm child pornography, four of which included A1 material. NCMEC staff later viewed three of the ten videos and submitted the CyberTipline Report to law enforcement.

d. Yahoo CyberTipline Report 90572327

On May 19, Yahoo submitted a fourth cybertip about Defendant's child pornography. (Doc. 70-5). It uploaded eight files—seven of them categorized as A1—from emails involving "yngluv01@yahoo.com." Although the email address changed,[7] Defendant's registered name of "Reb Reb" and verified mobile phone number did not. (Doc. 70-5 at 5). The report again confirmed

[7] Kramer testified that Yahoo deactivates an account that's no longer accessible to a user after child pornography is confirmed and a CyberTipline is reported. Yahoo, however, does not prevent the same user from opening a new account under a different name and email address.

that a Yahoo employee viewed the entire content of each file to confirm it was child pornography. An NCMEC staff later viewed five videos.

e. Yahoo Supplemental Report 91186992

On May 25, Yahoo submitted a second supplemental report that linked to three CyberTipline Reports. (Doc. 70-7 at 7). It again named Defendant as the suspect and listed the same address, mobile number, and birthday. Yahoo also confirmed Defendant's status as a registered sex offender and added that he had "been recently released from Federal Prison following a 240 month sentence for the sexual exploitation of minors." (Doc. 70-7 at 1). The supplemental report expanded on the images and videos: "nude female and partially clothed female children, ranging in age from approximately toddler to preteen, many of whom are engaged in sexual acts with adult males." (Doc. 70-7 at 4-5). Finally, it provided the IP addresses for recent successful logins to the Yahoo accounts to be in south Florida.

f. Google CyberTipline Report 90034851

On May 10, Google submitted a Cybertip about two images stored on its Gmail platform. (Doc. 70-8). Google's information led to NCMEC submitting CyberTipline Report 90034851, which identified the suspect as "Reb Reb" at reb3280@gmail.com. For the first file, someone at Google viewed all the content and categorized it as B1 material "concurrently to or immediately

preceding the sending of the CyberTip." (Doc. 70-8 at 3).[8] Although Google did not open the second file concurrently with sending its cybertip, an individual at some point earlier reviewed it and matched the hash value of the reported image to determine it contained child pornography. (Doc. 70-8 at 3). When NCMEC received Google's information, it too matched both files to hash values in its repository for child pornography content.

g. CyberTipline Report 90533145

On May 19, NCMEC received a second report from Google about one file stored on Google Photos for "Reb Reb" at the verified email address of reb3280e@gmail.com. (Doc. 70-9). For this file, a B1 designation, someone for Google viewed it to "confirm that it contained apparent child pornography concurrently to or immediately preceding the sending of the CyberTip." Although NCMEC did not view the file, it had a hash match.

h. Google CyberTipline Report 91101569

On May 25, Google submitted a third report of child pornography and uploaded one video stored in Google Photos. (Doc. 70-10). Again, the suspect was "Reb Reb" at the verified email address of luvemyng04@gmail.com. Google categorized the video as B1. And it was able to do so because "[a] person at

[8] A B1 designation is part of the same industry classification system that electronic service providers use to identify content in illicit material. B1 means content showing a pubescent minor engaging in a sex act.

Google viewed the file to the extent necessary to confirm that it contained apparent child pornography concurrently to or immediately preceding the sending of the CyberTip." (Doc. 70-10 at 3). For NCMEC, it had a hash match of the video.

All nine CyberTipline Reports and Supplemental Reports eventually landed on TFO Lee's desk. Upon receiving them, she focused on the files that Yahoo and Google uploaded because she knew that someone at the companies had (at some point) viewed the files to confirm they contained child pornography. And for the files with the A1 and B1 categorization, she knew they depicted prepubescent and pubescent minors engaging in sex acts. So TFO Lee opened the files to verify their contents. Based on TFO Lee's review, law enforcement got search warrants for Defendant's Yahoo accounts, Google accounts, home, and car. (Doc. 70-11; Doc. 70-12; Doc. 70-13; Doc. 70-14). These searches led to the Indictment and Defendant's motion to suppress.

DISCUSSION

Defendant argues the Court should exclude all evidence against him because TFO Lee violated his Fourth Amendment rights when she viewed the images and videos without a warrant. From there, he asserts the private search doctrine does not save the warrantless search for two reasons. First, because the names of Yahoo's and Google's employees who viewed the files are unknown, the Court only has hearsay evidence that somebody viewed the files,

which does not satisfy his Sixth Amendment confrontation rights. Second, Defendant argues that NCMEC is a government entity who exceeded Yahoo's and Google's searches because they processed the photos through their hash tag repositories and investigated IP addresses for geolocations.

For its part, the Government maintains that Defendant "frustrated or eliminated his expectation of privacy by uploading and sending child pornography over Yahoo and Google, which are private companies that routinely report to NCMEC when they become aware that a customer is sending child pornography using their products or services." (Doc. 57 at 20). It also argues that TFO Lee replicated Yahoo's and Google's private searches, so the Fourth Amendment did not require her to secure any warrant before viewing the reported images and videos. Finally, the Government raises the good-faith exception to the exclusionary rule.

The Court will address all arguments, starting with the private search exception to the warrant requirement.

A. Private Search Doctrine

The Fourth Amendment protects individuals against the government performing unreasonable searches and seizures. U.S. Const. amend. IV. The government usually needs a warrant before it may search a person or his effects. A warrantless search is thus invalid unless an exception applies to the

warrant requirement. *See Katz v. United States*, 389 U.S. 347, 357 (1967). The exception the Government relies on is the private search doctrine.

The Fourth Amendment protects individuals from government actors, not private ones. A private party may thus conduct a search that would be unconstitutional if the government did it. From this principle comes the private search doctrine. When a private party acts on its own accord and provides evidence against a defendant to the government, the police need not "avert their eyes." *Coolidge v. New Hampshire*, 403 U.S. 443, 489 (1971). So the Fourth Amendment lets police replicate a past private search provided it stays within the same parameters. *See United States v. Sparks*, 806 F.3d 1323, 1334 (11th Cir. 2015) ("So once an individual's expectation of privacy in particular information has been frustrated by a private individual, the Fourth Amendment does not prohibit law enforcement's subsequent use of that information, even if obtained without a warrant." (citations omitted)), *overruled on other grounds by United States v. Ross*, 963 F.3d 1056 (11th Cir. 2020).

The Supreme Court formalized the private search doctrine decades ago in two cases: *Walter v. United States*, 447 U.S. 649 (1980)[9] and *United States*

[9] In *Walters*, the Supreme Court concluded that FBI agents exceeded the scope of a private search by corporate employees who opened packages that contained boxes of eight-millimeter films "depicting homosexual activities," because the agents had to watch the films—when no employee had done so—to know whether the defendants committed any crime. 447 U.S. at 649-54, 657 (1980).

v. Jacobsen, 466 U.S. 109, 120 (1984).[10] Both considered a warrantless government search after a private party gave the government information for its investigation. Together, the cases determined that a past private search excuses the government from getting a warrant to repeat the search but only when the government's search does not exceed the scope of the private one.

Here, it is undisputed that Yahoo and Google are private entities that acted independently of law enforcement and without the government's knowledge or participation in discovering the child pornography files. Still, Defendant makes much ado about not knowing the identities of the individuals at Yahoo and Google who viewed the files. Without names, Defendant asserts Yahoo's and Google's custodians only offer hearsay evidence about the human review, which violates his right to confront those individuals. But this argument misses the mark for two basic reasons. First, Yahoo and Google, along with their employees and contractors are private people. So the who and how those private companies search their programs does not lessen the private search doctrine's application here. *See United States v. Montijo*, No. 2:21-cr-75-SPC-NPM, 2022 WL 93535, at *5 (M.D. Fla. Jan. 10, 2022); *see also United*

[10] In *Jacobsen*, the Supreme Court concluded DEA agents did not exceed the scope of a private search by Federal Express employees who opened a damaged package with a tube holding zip-lock bags of a white powder, because (1) the agents gleaned no new information than what the employees told; and (2) "the federal agents did not infringe any constitutionally protected privacy interest that had not already been frustrated as the result of the private conduct." 466 U.S. at 120-21, 126 (1984).

States v. Bonds, No. 521CR00043KDBDCK, 2021 WL 4782270, at *4 (W.D.N.C. Oct. 13, 2021) (rejecting the defendant's argument that the anonymous Google employee was unreliable because law enforcement could not contemporaneously verify the information before conducting its search).

Second, the Court can rely on hearsay and other evidence at a suppression hearing that may not otherwise be admissible. *United States v. Raddatz*, 447 U.S. 667, 679 (1980) ("At a suppression hearing, the court may rely on hearsay and other evidence, even though that evidence would not be admissible at trial."); *see also* Fed. R. Evid. 104(a), 1101(d)(1).

Having settled that, the Court turns to whether the private search doctrine applies here. To start, the Court finds that Kramer and Shrestha testified credibly about Yahoo's and Google's internal procedures for identifying, confirming, and reporting child pornography material. They clarified that Yahoo and Google screen for child pornography, not at the direction of law enforcement, but for their own reasons—to protect their brands, reputations, and services from harmful content. Kramer and Shrestha both confirmed that Yahoo and Google followed their procedures when assessing Defendant's files. Defendant offers no evidence that the CyberTipline Reports, nor Kramer's and Shrestha's testimony does not mean what they say: Yahoo and Google reviewed the contents of the actual files, and not just the associated hash tags, before the file was forwarded to NCMEC,

and then to law enforcement. *See, e.g.*, *United States v. Bohannon*, No. 19-CR-00039-CRB-1, 2023 WL 2347420, at *1 (N.D. Cal. Mar. 2, 2023) (finding a Microsoft employee viewed the contents of the defendant's OneDrive file before forwarding it to NCMEC).

Moving on, law enforcement did not exceed the scope of Yahoo's or Google's searches because TFO Lee only viewed the images and videos they provided. When TFO Lee viewed Defendant's files, she knew they would contain child pornography and that many would show A1 and B1 content. Defendant makes no argument—nor does the Court see how one can be made—that TFO Lee learned more from viewing the files than Yahoo and Google provided. Because individuals for Yahoo and Google reviewed the files before they were forwarded to NCMEC, who confirmed they were child pornography, TFO Lee did not need to view them to know Defendant committed a federal crime. Yahoo and Google already told her so with the A1 and B1 labels. *See generally Rogers v. Sec'y, Dep't of Corr.*, No. 8:17-CV-2680-T-33SPF, 2019 WL 2646544, at *6 (M.D. Fla. June 27, 2019) (finding a § 2255 petitioner did not "identif[y] any clearly established federal law holding that when a private searcher views at least one image on a disk and tells police that the disk contains contraband, police exceed the scope of the private search by viewing other images on that same disk"), *aff'd,* 829 F. App'x 437 (11th Cir. 2020).

So this not a case where a private citizen stumbled across child pornography on a laptop and gave the device to law enforcement who then searched the device's entire contents. Rather, individuals at Yahoo and Google, who are trained on what constitutes child pornography under federal law, verified the illicit content on the files. And because TFO Lee only viewed the files that Yahoo and Google provided, she got the same information discovered during the private search. Under these facts, TFO Lee did not need to avert her eyes from the videos and images when she received the CyberTipline Reports. *Coolidge*, 403 U.S. at 489.

Finally, as much as Defendant argues that NCMEC is a governmental agency that expanded on Yahoo's and Google's private searches because it searched for geolocations, his argument misses the mark. Yahoo and Google gave NCMEC several IP addresses for the suspect, and from there, NCMEC investigated more through open sources. Even so, it is well established that law enforcement need not get a search warrant to investigate an IP address. *See United States v. Ryan Anthony Adams*, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at *3 (M.D. Fla. Aug. 10, 2016) ("Computer users lack a legitimate expectation of privacy in information regarding the to and from addresses for emails, the IP addresses of websites visited, the total traffic volume of the user, and other addressing and routing information conveyed for the purpose of transmitting Internet communications to or from a user."

(citations omitted)); *see also United States v. Solove*, No. 21-11747, 2022 WL 152240, at *1 (11th Cir. Jan. 18, 2022) (holding the *Carpenter* exception to the third-party doctrine does not extend to email and IP addresses). What's more, Yahoo provided Defendant's home address in its first supplemental report based on its own investigation. And, in the end, the search warrant for Defendant's home is that same address from Yahoo. *Compare* Doc. 70-6 at 4, *with* Doc. 70-13 at 53. So neither NCMEC nor law enforcement needed to do any additional search—Yahoo did it for them.

In conclusion, the Court finds the private search doctrine applies to justify the warrantless search of the videos and images uploaded to the CyberTipline Reports.

B. Reasonable Expectation of Privacy

The Court further finds that Defendant did not have a reasonable expectation of privacy in the videos and images he uploaded to Yahoo's and Google's platforms. And Defendant neither presents evidence nor argues to the contrary.

A defendant can only invoke the Fourth Amendment's protection where he has a legitimate expectation of privacy in the item searched. *See Rakas v. Illinois*, 439 U.S. 128, 148-49 (1978). The privacy interest is both subjective and objective: a defendant must show he subjectively expected privacy, and the expectation is one that society recognizes as reasonable. *See United States v.*

Ford, 34 F.3d 992, 995 (11th Cir. 1994) (citation omitted). But an individual's expectation of privacy is not always forever. A common example of when an expectation of privacy is frustrated is when information is revealed to a third party. *See Jacobsen*, 466 U.S. at 117 ("It is well-settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information. Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information[.]" (citation and footnote omitted)).

Defendant revealed the videos and images not only to his intended email recipients, but also to Yahoo and Google. He risked that both would turn them over to the Government. And the Court need look no further than Yahoo's and Google's written policies to know it gave Defendant fair warning of that risk.

Yahoo posts a Transparency Report on its website that tells users how it uses automated scanning technologies and human review to detect unlawful child pornography on its platforms. (Doc. 70-17). From there, Yahoo advises how its team of human reviewers evaluate detected images to confirm the content as child pornography. It is also clear that Yahoo reports all child pornography to NCMEC and includes subscriber information on who uploaded the files.

Yahoo's Transparency Report isn't the only place where Yahoo shares how it spots and reports child pornography. Its Terms of Service echo the procedure: "You agree not to use the Services to: . . . make available any content that is harmful to children, threatening, abusive, harassing, tortious, defamatory, vulgar, obscene, libelous, invasive of another's privacy, hateful, or racially, ethnically, or otherwise objectionable[.]" (Doc. 70-15 at 2; Doc. 70-16 at 3)). A user also agrees not to use Yahoo's service to "violate any applicable laws or regulations." (Doc. 70-15 at 2; Doc. 70-16 at 3).

Like Yahoo, Google openly tells its users about its quest to find, review, and report child pornographic material on its platforms through its Transparency Report and Terms of Service. (Doc. 70-18; Doc. 70-20). According to Google's Transparency Report, its "teams work around the clock to identify, remove, and report this . . . content, using a combination of industry leading automated detection tools and specifically trained reviewers. We also receive reports from third parties and our users, which complement our ongoing work. We report [child pornography] to the National Center for Missing and Exploited Children, NMEC, . . . [who] may send those reports to law enforcement agencies around the world." (Doc. 70-20). Under Google's Terms of Services (Doc. 70-18), a user agrees to follow the laws and not abuse or harm others. Users are also advised that Google employs automated

systems to check for child pornography sent, received, and stored on its platform.

And Yahoo and Google are not all words without action. They both told their users that they follow through on their internal procedures. For example, in 2021, Yahoo reported 5,498 accounts to NCMEC for trafficking in child pornography on its platforms and filed 341 supplemental reports with NCMEC. Also in 2021, Google submitted over 850,000 CyberTipline reports to NCMEC. (Doc. 70-20; Doc. 70-21).

Because of the Terms of Service and Transparency Reports, Yahoo and Google warned Defendant he risked being reported to law enforcement or NCMEC if either discovered that he sent, received, or distributed apparent child pornography. Even if Defendant believed that his emails and photos were private, society is not prepared to recognize that belief as reasonable given the Terms of Service and Transparency Reports. In the end, Defendant lost any expectation of privacy in the files once he hit send. *See United States v. Odoni*, 782 F.3d 1226, 1238 (11th Cir. 2015) ("An individual does not have a reasonable expectation of privacy in an object to the extent the object has been searched by a private party." (citation omitted)). Without a reasonable expectation of privacy, TFO Lee did not violate Defendant's Fourth Amendment rights when she viewed the files, and any privacy was waived by Yahoo's and Google's prior searches.

C. Good-faith exception

Even if Defendant had a reasonable expectation of privacy and the private search doctrine did not apply, the Court still denies the Motion under the good-faith exception. To discourage police from violating the Fourth Amendment, courts have created the remedy of excluding "improperly obtained evidence at trial." *Herring v. United States*, 555 U.S. 135, 139 (2009). But "exclusion 'has always been our last resort, not our first impulse.'" *Id.* at 140 (citation omitted). The exclusionary rule's "sole purpose . . . is to deter future Fourth Amendment violations." *Davis v. United States*, 564 U.S. 229, 236-37 (2011) (citations omitted).

Courts must thus engage in a "rigorous weighing of [exclusion's] costs and deterrence benefits" to determine whether it is needed. *Id.* at 238. And the good-faith exception comes into that analysis. Under the exception, courts do not exclude evidence when law enforcement acts, as here, in "objectively reasonable reliance upon a statute authorizing" the search. *Illinois v. Krull*, 480 U.S. 340, 349 (1987) ("The application of the exclusionary rule to suppress evidence obtained by an officer acting in objectively reasonable reliance on a statute would have as little deterrent effect on the officer's actions as would

the exclusion of evidence when an officer acts in objectively reasonable reliance on a warrant.").

TFO Lee acted in objectively reasonable reliance on Yahoo's and Google's statutory reporting requirements to view the files here. *See* 18 U.S.C. § 2258A; *see also United States v. Ackerman*, 804 F. App'x 900, 905 (10th Cir. 2020) (finding the good-faith exception applied when NCMEC searched the defendant's email in good faith under § 2258A). Electronic service providers like Yahoo and Google must report to NCMEC's CyberTipline after it obtains "actual knowledge" of any apparent child pornography. 18 U.S.C. § 2258A(a)(1)-(2). They can even be fined if they do not do so. *Id.* § 2258A(c). NCMEC too has statutory obligations. It must maintain the CyberTipline and forward every report it receives to law enforcement. *Id.* § 2258A(a)(1)(B) & (c). Congress has also let NCMEC receive and review the illicit material without breaking the law. *Id.* § 2258A(c).

Under this statutory scheme, TFO Lee acted in reasonable reliance on Yahoo's, Google's, and NCMEC's legal obligations to view the files she received. *See generally United States v. Leon*, 468 U.S. 897, 918 (1984) (stating the exclusion of evidence is an "extreme sanction" that "should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion will further the purposes of the exclusionary rule"). The Court thus denies Defendant's Motion on the good-faith exception too.

Accordingly, it is now

ORDERED:

Defendant Richard Brillhart's Motion to Suppress (Doc. 56) is **DENIED.**

DONE AND ORDERED in Fort Myers, Florida on May 7, 2023.

SHERI POLSTER CHAPPELL
UNITED STATES DISTRICT JUDGE

Copies: Counsel of Record

UNITED STATES CONSTITUTION, AMENDMENT IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

28 U.S.C. § 1254(1)

Cases in the courts of appeals may be reviewed by the Supreme Court by the following methods:

(1) By writ of certiorari granted upon the petition of any party to any civil or criminal case, before or after rendition of judgment or decree;

28 U.S.C. § 1257(a)

(a) Final judgments or decrees rendered by the highest court of a State in which a decision could be had, may be reviewed by the Supreme Court by writ of certiorari where the validity of a treaty or statute of the United States is drawn in question or where the validity of a statute of any State is drawn in question on the ground of its being repugnant to the Constitution, treaties, or laws of the United States, or where any title, right, privilege, or immunity is specially set up or claimed under the Constitution or the treaties or statutes of, or any commission held or authority exercised under, the United States.

A. Yes, Google would provide the product or infrastructure it was stored in when submitting a NCMEC report.
Q. And did Google also provide two files to NCMEC along with the -- as part of the CyberTip?
A. Yes, the CyberTip report reflects that two files were attached to that report.
Q. In making the CyberTip report, did Google also provide the filename, the hash value for the file?
A. Google would provide just the standard course of production that we would for the image and provide the categorization of the image as well with the hash.
Q. Okay. And when you say categorization, what is the categorization that is seen for one of the files that was submitted with this particular CyberTip?
A. B1.
Q. And what is the categorization of B1 signify?
A. Pubescent minor sex act.
Q. And the categorization that is listed with the file B1, that would be a categorization that was given by Google to the attachment?
A. Yes, in line with industry classification.
Q. And in this particular first file, does it indicate whether or not the reporting ESP, in this case, Google, viewed the entire contents of the uploaded file?
A. Yes, one of the files was labeled as ESP, yes.

Q. So when it indicates yes, based on your knowledge and training and experience from Google, does that mean an actual employee of Google looked at the file?

A. Yes, it indicated that a Google reviewer had reviewed the file immediately or concurrently when sending the report to NCMEC.

Q. Can you please read this highlighted portion from the CyberTip that's in Government's Exhibit No. 3A?

A. "With respect to the portion of this CyberTip containing the heading was filed reviewed by company, when Google responds yes, it means the entire contents of the file reported reviewed by a person concurrently to or immediately preceding the sending of the CyberTip. When Google responds no, it means that while the contents of the 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 that it contained apparent child pornography. In some instances, Google will not provide an answer to this question, but will provide a description in the additional information field to explain the review conducted by a person at Google concurrently to or immediately preceding the sending of the CyberTip."

Q. And is that consistent with the policy that Google follows in making these CyberTips?

A. Yes.

Q. Did Google provide information as to the second file?
A. Yes.
Q. Did it provide the filename and the hash value for the file?
A. Yes.
Q. And was it as to whether they reviewed the entire content?
A. Yes.
Q. And what was the response?
A. So it means that the file's hash matched a hash of a file that had already been previously reviewed by a Google reviewer that was contained in the CSAM repository that Google has.
Q. Okay. But --
A. CSAM repository of hashes.
Q. But, at some point, a file matched an exact same digital fingerprint had been viewed by an employee at Google?
A. It means that the hash or very similar to the hash matched a hash that was included in the CSAM hash repository, and for a hash to be assigned for an image to go into that CSAM repository, a Google reviewer would have to have reviewed that image. So it just means that the file -- not viewed means that a Google reviewer did not review the file concurrently or immediately before sending the NCMEC report.
Q. Which was not the circumstance with the first file;

being submitted without review?
A. One of those being a report submitted because the hash matches a previously reviewed hash.
Q. Now, let's see. And in fact, go back to your declaration, that at least is the case here. I'm sorry, for purposes of the record, 10. Government's Exhibit 10.
It says here on the bottom of the page this CyberTip line report reflects that two files were attached to the report and Google indicated that a Google reviewer had reviewed one of the files immediately before submitting the report, while it did not review the other immediately before submitting the report. So one was looked at, one was not?
A. So that term the file not viewed means only, and it's listed in the declaration, that a Google reviewer did not review that file concurrently with or immediately preceding the report and it means that the file's hash matched the hash's in Google's repository of apparent CSAM. So the underlying image for that hash still would have been reviewed by a Google reviewer before that hash was even added to Google's repository of hashes.
Q. And how do you know that?
A. That's in Google's normal course of business.
Q. And but as we sit here today, you don't know who reviewed the one that's being reported right now; correct?
A. The CyberTip?

time to one another?
A. I received like the first couple together and then like a second batch like a month or so later.
Q. Okay. So within several weeks?
A. Yes.
Q. And did you review the suspect information?
A. Yes.
Q. Did you review the information provided by Google regarding how many files they uploaded that's on page 6 --
A. Yes.
Q. -- of Government's Exhibit No. --
How many files did they indicate that they uploaded in this particular report?
A. Two.
Q. And did you have an occasion to review what was provided on each file?
A. Yes.
Q. And on the first file, does it indicate whether the ESP viewed the contents of the uploaded file in its entirety?
A. Yes.
Q. And what was the response?
A. Yes, they did.
Q. And did they provide a categorization of the file?
A. Yes.
Q. And what did they provide?

A. B1.
Q. And what does B1 signify?
A. A prepubescent -- or a pubescent minor in a sex act.
Q. And does it provide source information as to each of those two files as to the date and time of the upload?
A. Yes.
Q. And did you have an occasion to review that material?
A. Yes.
Q. In looking at what was provided, did the source information of the upload occur on the same date and close to the same time?
A. Yes.
Q. From the same -- involving the same email address?
A. Yes.
Q. Now, looking at the second file, did the ESP indicate whether or not they looked at the file in its entire contents?
A. No.
Q. They indicated no, they had not?
A. Yeah, no, they had not looked at it.
Q. Okay. And have you received Google reports previously?
A. Yes.
Q. And are you familiar with their NCMEC reports?
A. Yes.
Q. Okay. And on this particular report, on page 1 of

the report, was there information, company information provided?

A. Yes.

Q. And did you have an occasion to read what the company information was --

A. Yes.

Q. -- that was provided?

A. Yes.

Q. And in so doing, did it provide any explanation as to how Google answers those questions as yes or no?

A. Yes.

Q. And in this instance, looking at what's contained on Government's Exhibit No. 3A that's blown up on the screen, what does Google indicate when it responds no?

A. When Google responds no, it means that while the contents of the file were not reviewed concurrently to making the report, historically, a person had reviewed a file whose hash, or digital footprint, matched the hash of the reported image and determined it contained apparent child pornography.

Q. I believe it was digital fingerprint.

A. Yes.

Q. I think you said footprint. I just want to make sure.

A. Oh, sorry, fingerprint.

Q. And based on your training and experience, are you

familiar with hash values or hash matches?
A. Yes.
Q. And, essentially, what is a hash match?
A. Almost like your fingerprint for a photo. If it's -- the photo's changed, the hash value will change. So there's a system where these values are stored, and when a photo matches it, it's able to match with it. It's identical.
Q. Okay. So looking -- were you aware of this information in terms of when Google responds no?
A. Yes.
Q. And did you also have an occasion to review section B that was contained in the report?
A. Yes.
Q. That is on page 8.
Did NCMEC provide any information regarding the files?
A. Yes, both of them were categorized as apparent child pornography.
Q. Okay. So NCMEC provided a categorization, but did you also review section C that's contained on page 13 of the report?
A. Yes.
Q. And did NCMEC indicate whether or not any staff members had reviewed the files?
A. They were not viewed by NCMEC.

Q. Okay. After reviewing this particular report, what action, if any, did you take?
A. I reviewed the files.
Q. Okay. Why did you review the files?
A. Because one of them had been viewed by the electronic service provider and the other one was a hash match to something that was known in the system.
Q. And had been -- and was it a file that was reported by Google?
A. Yes.
Q. And based on the CyberTip report that was made and the information that was contained within it, did you have reason to believe that there would be child pornography in those files?
A. Yes.
Q. Did you have an occasion to receive and review a CyberTip that has been admitted into evidence as Government's Exhibit No. 3B?
A. Yes.
MS. VIACAVA: At this time, the government would publish Government's Exhibit No. 3B.
Q. Did you review the contents of this particular report?
A. Yes.
Q. And in so doing, did it provide information as to the

A. They did not review it.
Q. After receiving this report, did you take any additional action?
A. Yes, I viewed the file.
Q. And why did you view the file?
A. Because it had the categorization of B1 and it was categorized as apparent child pornography.
Q. And did you also consider whether or not Google had accessed the file?
A. Yes, and Google, the electronic service provider, indicated they viewed the file.
Q. And in this case, it was to an extent that they felt necessary to determine it was child pornography?
A. Yes.
Q. And based on the categorization, based on the information provided, did you have reason to believe that the attachment contained child pornography?
A. Yes.
Q. And with these CyberTips, as you testified regarding the Google -- or the Yahoo, with these Google CyberTips, did you also have an occasion to provide descriptions of the files, attachments that you viewed to Agent Randall?
A. Yes.
Q. And to your knowledge, were those descriptions included as part of a search warrant?

A. Yes.
Q. And to your knowledge, were those descriptions included in an affidavit for several search warrants in this particular case?
A. Yes.
MS. VIACAVA: At this time, the government would publish Government's Exhibit No. 4A that's been admitted into evidence.
Q. Government's Exhibit No. 4A, was this a search warrant for the email accounts for Yahoo?
A. Yes.
Q. And these are the email accounts referenced in the CyberTips?
A. Yes.
Q. And are they included in the body of the application?
A. Yes.
MS. VIACAVA: May I approach the witness, Your Honor?
THE COURT: Yes, you may.
MS. VIACAVA: So, at this time, the government would publish page 19 of Government's Exhibit No. 4A., 19 of the actual affidavit.
BY MS. VIACAVA:
Q. In looking at -- have you had an occasion to look at all four of these search warrants involved in this case?
A. Yes.

Q. And looking at them, are the affidavits similar?
A. Yes.
Q. In terms of providing descriptions that were contained in the NCMEC reports?
A. Yes.
Q. And looking at this particular page, when it describes Task Force Officer O'Brien, that would be you; correct?
A. Yes.
Q. At the time, that was the name you were utilizing?
A. Yes.
Q. Okay. And you're the individual that reviewed the files and provided the descriptions?
A. Yes.
Q. And you've had an occasion to review all those descriptions to ascertain that they are the descriptions you provided to Special Agent Randall?
A. Yes.
MS. VIACAVA: At this time, the government would publish Government's Exhibit No. 4B that's been admitted into evidence.
Q. Government's Exhibit No. 4B, what was this affidavit -- or what was this search warrant for?
A. The Google email accounts.
Q. And the email accounts referenced are the email