In the

United States Court of Appeals

For the Seventh Circuit

No. 25-2740

UNITED STATES OF AMERICA,

Plaintiff-Appellant,

v.

PETER J. BRAUN,

Defendant-Appellee.

Appeal from the United States District Court for the
Eastern District of Wisconsin.
No. 2:24-cr-00164 — **Lynn Adelman**, *Judge*.

ARGUED MAY 12, 2026 — DECIDED AUGUST 20, 2026

Before BRENNAN, *Chief Judge*, and KIRSCH and LEE, *Circuit Judges*.

LEE, *Circuit Judge*. In September 2020, both Microsoft and Google each alerted the National Center for Missing and Exploited Children ("NCMEC") that images of child sexual

abuse material ("CSAM")[1] had been uploaded from a single IP address to their servers. No one at Microsoft, Google, or NCMEC viewed the images, but the entities flagged the images based on hash values that matched "Apparent Child Pornography."

NCMEC sent the four reports to the Wisconsin Department of Justice to investigate. As part of the investigation, Special Agent Aaron Koehler connected the IP address to Peter Braun's house, viewed the hash-matched images without a warrant, conducted his own investigation, and applied for a state warrant to search Braun's house.

Based on the evidence collected as well as additional information, Braun was charged with four counts of producing CSAM in violation of 18 U.S.C. § 2251(a). Braun moved to suppress the evidence obtained from the search of his home. The district court granted the motion to suppress, holding, in pertinent part, that Agent Koehler required a warrant to view the images, and without his descriptions of the images, the warrant failed to establish probable cause. The government has appealed under 18 U.S.C. § 3731.

---

[1] Federal criminal law defines "child pornography" as the "visual depiction" of a minor "engaging in sexually explicit conduct." 18 U.S.C. § 2256(8); *see also United States v. Williams*, 553 U.S. 285, 288 (2008) (child pornography generally "consists of sexually explicit visual portrayals that feature children."). "[T]he term 'child sexual abuse material' more 'accurately reflects what is depicted—the sexual abuse and exploitation of children.'" *United States v. Tucker*, 60 F.4th 879, 887 (4th Cir. 2023) (citation modified). We use the term "CSAM" interchangeably with the term "child pornography" to "reflect more accurately the abusive and exploitative nature of [the act]." *United States v. Kuehner*, 126 F.4th 319, 322 n.1 (4th Cir. 2025).

We reverse. Based on this record, we conclude that, even without Agent Koehler's descriptions of the images he viewed, his warrant affidavit provided sufficient information to establish probable cause for the search.

I. Background

Under 18 U.S.C. § 2258A(a)(1), an electronic service provider must report any CSAM to the CyberTipline of NCMEC. On September 8 and 9, 2020, NCMEC received three reports, commonly referred to as "CyberTips,"[2] from Microsoft and one report from Google about images uploaded to Skype and Gmail respectively, which were flagged as potentially containing CSAM.

Microsoft, Google, and NCMEC did not open or view the files. Instead, each entity reported that the images matched hash values of known or previously identified CSAM.[3]

---

[2] *See, e.g.*, *United States v. Osterman*, 119 F.4th 1090, 1093 (7th Cir. 2024).

[3] The Tenth Circuit has recently described hash-matching as follows:

> A "hash value" is a short string of characters generated from a much larger string of data (say, an electronic image) using an algorithm …. Hash values have been used to fight child pornography distribution, by comparing the hash values of suspect files against a list of the hash values of known child pornography images currently in circulation. This process allows potential child pornography images to be identified rapidly, without the need to involve human investigators at every stage.

United States v. Rosenschein, 136 F.4th 1247, 1253 n.1 (10th Cir. 2025) (citation modified).

Google's CyberTip also indicated that at least one image contained the file name "pedomom-and-son." Dkt. 22-4 at 4.[4]

NCMEC geolocated the IP (internet protocol) address to Lomira, Wisconsin, and forwarded the reports to the Wisconsin Department of Justice. The Wisconsin Department of Justice Division of Criminal Investigation reviewed the CyberTip reports and subpoenaed information that traced the IP address to Peter Braun's home.

In January 2021, Agent Koehler viewed the images without a warrant and conducted surveillance on Peter Braun's house. Agent Koehler also received information from the Lomira Police Department indicating that, in 2015, Braun's son had told his teacher that he had observed Braun communicating online with very young girls.

Agent Koehler obtained a state warrant to search Braun's house. In the supporting affidavit, Koehler included information from the CyberTip reports, described the images that he viewed, detailed Braun's identifying information, and included the 2015 report about Braun's online chats with young girls. Based on the evidence collected and after further investigation, the government charged Braun with four counts of producing child pornography.

Braun moved to suppress the evidence obtained from the search, and the motion was referred to the magistrate judge. The magistrate judge recommended denying the motion, and Braun objected.

---

[4] "Dkt." refers to the docket number in the district court record.

The district court rejected the magistrate judge's recommendation and granted the motion to suppress on three grounds. First, the court held that Agent Koehler needed a warrant to view the images provided in the CyberTips reports. Second, the court determined that, without the agent's descriptions of the images, the warrant failed to establish probable cause. Third, the court found that the good-faith exception to the exclusionary rule did not apply.

The government then filed this interlocutory appeal. It argues that the district court erred because, even without Agent Koehler's descriptions of the images, the warrant contained information sufficient to establish probable cause.

II. Discussion

When a district court grants a motion to suppress, "we review the district court's legal conclusions de novo and its factual findings for clear error." *United States v. Leal*, 1 F.4th 545, 548 (7th Cir. 2021). On appeal, the government argues that Agent Koehler's affidavit established probable cause even after excising the descriptions of the hash-matched images. As a threshold matter, we must first determine whether the issue was properly preserved for appellate review.

A. Preservation for Appeal

Braun argues that the government waived its argument by failing to develop it before the district court. In his view, the government made only "perfunctory reference to the agent's 'other investigative steps' and his receipt of the 2015 report." *See United States v. Dunkel*, 927 F.2d 955, 956 (7th Cir. 1991). And, indeed, the main thrust of the government's argument contesting the ruling below is that "[t]he warrant also

described SA Koehler's other investigative steps, as described above." Dkt. 27 at 13.

As Braun sees it, this argument is new. The government, he contends, "did not explain *which* specific steps it was referring to, or *how* they added up to probable cause." The district court seemed to agree. "The government develop[ed] no argument," the court stated, "that Koehler's additional investigation, e.g., the 2015 report that defendant's son saw him chatting with young girls online, suffices to establish probable cause." *United States v. Braun*, 798 F. Supp. 3d 916, 926 (E.D. Wis. 2025).[5]

Doubtless, the government may waive or forfeit arguments in a criminal case. *See United States v. Jones*, 713 F.3d 336, 351 (7th Cir. 2013); *United States v. Martinez*, 122 F.3d 421, 423 (7th Cir. 1997) ("The government thereby waived the waiver argument, or at the least forfeited it."). We rely on "the parties to frame the issues for decision and assign to courts the role of neutral arbiter of matters the parties present." *United States v. Sineneng-Smith*, 590 U.S. 371, 375 (2020) (quoting *Greenlaw v. United States*, 554 U.S. 237, 243 (2008)). As such, we presume that parties represented by competent counsel "know what is best for them" and accordingly hold them "responsible for advancing the facts and argument entitling them

[5] To the extent this statement is construed as a finding of waiver, we owe no deference to the district court's determination. We "review the factual determinations upon which a district court predicates a finding of waiver for clear error and the legal question of whether the conduct amounts to waiver de novo." *e360 Insight v. The Spamhaus Project*, 500 F.3d 594, 599 (7th Cir. 2007) (citation omitted).

to relief." *Id.* at 375–76 (quoting *Castro v. United States*, 540 U.S. 375, 386 (2003) (Scalia, J., concurring in part)).

At the same time, "parties are not limited to the precise arguments they made below." *Yee v. City of Escondido*, 503 U.S. 519, 534 (1992) (collecting cases); *see also United States v. Wanjiku*, 919 F.3d 472, 486 (7th Cir. 2019) (finding government's arguments not waived because "the government's argument on appeal is simply a new twist on the arguments it preserved below"); *cf. Hernandez v. Cook Cnty. Sheriff's Off.*, 634 F.3d 906, 913 (7th Cir. 2011) ("While arguments made for the first time in a reply brief are generally treated as waived, it does not necessarily follow that arguments that are better developed in a reply brief are waived.").

The government posits that it properly preserved the argument for review because it summarized the information in the affidavit, provided the legal standard for probable cause, and argued that "the warrant contained sufficient probable cause excluding the challenged conduct." Dkt. 27 at 7. Based on the record before us, we agree.

The government's response to Braun's motion to suppress contains enough references to Agent Koehler's "other investigative steps" to preserve the government's probable cause argument, although by a hair's breadth. We must keep in mind that, when assessing probable cause in the context of a warrant, the record is limited to the supporting affidavit. *See United States v. Orozco*, 576 F.3d 745, 748 (7th Cir. 2009) (noting that courts review the determination of probable cause by looking only at the "strength" of the affidavit) (quotation omitted). And the government presented numerous facts before the district court that were contained in Agent Koehler's affidavit.

For example, the government informed the court that Microsoft and Google had "determined that the images contained CSAM, and they therefore alerted NCMEC." Dkt. 27 at 3. It stated that one of the images contained a "file name of 'pedomom-and-son.jpg,'" which "is a common type of name used to identify files that contain child pornography." *Id.* at 3–4. The government also explained the significance of the file name, stating that "[t]hose seeking child pornography often use such a title to conduct a word search of files that would contain child pornography." *Id.* at 4. Finally, the government pointed to the 2015 investigation report, which "alleged that [Braun] had been observed by his son chatting/interacting online with very young girls." *Id.* at 5–6. Certainly, the government could have been more articulate in presenting its argument, but it directed the district court to the affidavit's facts that supported probable cause even in the absence of Agent Koehler's descriptions.

In addition to the relevant facts, the government pointed to the applicable legal standard. "To find probable cause," the government informed the court, "the magistrate judge need only find that there is a 'fair probability' that the search will reveal 'evidence of a crime.'" *Id.* at 13 (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)). The government then applied this standard to the facts to argue that "the warrant contained sufficient probable cause excluding the challenged content." *Id.* at 7.

Although the government could have (and should have) done more to explicate its argument, what it did here was just enough. *See United States v. Roque-Espinoza*, 338 F.3d 724, 727 (7th Cir. 2003) (finding that a defendant did not forfeit his claim, which was "[a]t worst … underdeveloped" but still

"indicate[d]" the nature of his argument); *cf. United States v. Marrocco*, 578 F.3d 627, 637 n.13 (7th Cir. 2009) (finding that the government preserved an "inevitable discovery" argument, despite not invoking that precise term, by arguing, in part, that "other facts gave the officers independent probable cause" to search the defendant's belongings).

B. Probable Cause

Turning to the merits, under the Fourth Amendment, "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation." U.S. Const. amend. IV. The standard is familiar by now. "Probable cause … is not a high bar." *Kaley v. United States*, 571 U.S. 320, 338 (2014). It "exists when, based on the totality of the circumstances, there is a 'fair probability that contraband or evidence of a crime will be found in a particular place.'" *United States v. Douglas*, 164 F.4th 1017, 1021 (7th Cir. 2026) (quoting *United States v. Calligan*, 8 F.4th 499, 504 (7th Cir. 2021)). Our probable cause examination "does not take each fact in isolation; it depends on the totality of the circumstances." *Rainsberger v. Benner*, 913 F.3d 640, 648 (7th Cir. 2019) (citing *District of Columbia v. Wesby*, 583 U.S. 48, 60–61 (2018)).

The government does not challenge the district court's holding that Agent Koehler's viewing of the images constituted an unlawful search. Thus, for purposes of our analysis, we presume that the descriptions were illegally acquired. Rather, the government argues that the district court erred in concluding that the search warrant failed to establish probable cause even in the absence of the descriptions.

If a judicial officer secures a warrant by relying on illegally acquired information, any evidence discovered pursuant to

that warrant will be inadmissible. *United States v. Scott*, 731 F.3d 659, 664 (7th Cir. 2013) (citing *United States v. Oakley*, 944 F.2d 384, 386 (7th Cir. 1991)). Whether to suppress such evidence requires a two-part inquiry. *Id.* First, we ask "whether the illegally obtained evidence affected the judge's decision to issue the warrant." *Id.* Put another way, evidence will not be suppressed where the "untainted information, considered by itself, establishes probable cause for the warrant to issue." *United States v. Gray*, 410 F.3d 338, 344 (7th Cir. 2005) (quoting *Oakley*, 944 F.2d at 386). Second, we ask "whether the decision to seek the warrant was prompted by information unlawfully obtained." *Scott*, 731 F.3d at 664 (citation modified).

1. Other Supporting Information

The government points to three pieces of information that, it believes, are sufficient to establish probable cause when considered with the rest of the affidavit even absent the descriptions of the images. First, it contends that the sources of the information, Microsoft and Google, have proven to be reliable informants in similar CSAM cases. Second, the government points to the telltale name on one of the files. Finally, the government references the information Agent Koehler obtained about Braun's prior activities with minors.

a. Reliability of Informants

"[A] search warrant need not be based on first-hand observations." *United States v. Hollingsworth,* 495 F.3d 795, 805 (7th Cir. 2007). Rather, an affidavit in support of a search warrant may be based on information from reliable sources. *See Woods v. City of Chicago,* 234 F.3d 979, 996 (7th Cir. 2000); *Gates*, 462 U.S. at 233 (suggesting that a tip might be made more reliable if it came from an informant "known for the unusual

reliability of his predictions" or from "an unquestionably honest citizen").

Here, the CSAM information Microsoft, Google, and NCMEC provided to the government is akin to tips a typical informant might provide to law enforcement. In the latter context, we evaluate the credibility of an informant by assessing the particular circumstances including "the level of detail, the extent of firsthand observation, the degree of corroboration, [and] the time between the events reported and the warrant application." *United States v. Glover*, 755 F.3d 811, 816 (7th Cir. 2014).[6] We also consider the informant's "past reliability," "reputation for honesty," and "potential motive." *Cherry*, 920 F.3d at 1133 (citing *Gates*, 462 U.S. at 234–35). In weighing these factors, we do not take any one of them as "determinative, and a deficiency in one factor may be compensated for by a strong showing in another or by some other indication of reliability." *United States v. Mullins*, 803 F.3d 858, 863 (7th Cir. 2015) (internal quotation marks omitted).

Agent Koehler's affidavit relayed that Microsoft and Google had provided NCMEC with four separate reports indicating that images of CSAM were uploaded from a single IP address to their platforms; NCMEC then conveyed these tips to the Wisconsin Department of Justice. The affidavit also noted that the applicable federal statute "created a mechanism" by which such internet service providers could report suspected CSAM activities to NCMEC, which in turn had

---

[6] Of course, "[a]nonymous tips … require more corroboration[.]" *United States v. Cherry*, 920 F.3d 1126, 1134 (7th Cir. 2019). But Microsoft, Google, and NCMEC are well-known institutional sources of information regarding CSAM use and distribution.

formed a partnership with law enforcement to review and act on such information. Agent Koehler also confirmed that he considered the information NCMEC and the internet service providers provided to be reliable because it was provided pursuant to federal law. Moreover, he added, similar information the internet service providers had provided in the past "was found to be accurate and reliable."

The government concedes that a CyberTip report alone is not sufficient to establish probable cause to search the location of an implicated IP address. Here, however, Agent Koehler also described his experience with the CyberTip process, the roles that NCMEC and the internet service providers play, and the reliability of their information based on his own experience. Such indicia of reliability lent credence to the accuracy of the CyberTip reports. *See United States v. Landreneau*, 967 F.3d 443, 452 (5th Cir. 2020) ("The tip did not come from an unidentified or questionable source: Google, pursuant to a federal statute, see 18 U.S.C. § 2258A, alerted NCMEC, and in turn local law enforcement, based on Google's actual knowledge that a Gmail user had uploaded child pornography images to an email.") (footnote omitted).

Furthermore, the CyberTip reports contained appreciable amounts of detail, which further bolstered their trustworthiness. The reports referred to "Apparent Child Pornography," matched the images to those involving a sex act with a prepubescent minor, and provided the IP address associated with the incident. What is more, the information was relatively fresh; only about six months had elapsed from the dates of the reports to the warrant application. *Compare* Dkt. 22-1, 22-2, 22-3, 22-4, *with* Dkt. 22-5 ¶ 31, and *id.* at 26; *see United States v. Newsom*, 402 F.3d 780, 783 (7th Cir. 2005) ("Information a year

old is not necessarily stale as a matter of law, especially where child pornography is concerned.") (citing *United States v. Lacy*, 119 F.3d 742, 745 (9th Cir. 1997)).

Additionally, Agent Koehler did more than simply attach the CyberTip reports to the court. He performed his own investigation, linked the IP address to Braun, analyzed the file names, and corroborated the behavior with a prior report of Braun's inappropriate interactions with minors, all of which supported the reliability of the information in the CyberTip reports. *See United States v. Walker*, 237 F.3d 845, 850 (7th Cir. 2001) (stating that the purpose of corroborating information is to establish a source's reliability, not to confirm all the information the source provided).

All told, the information in Agent Koehler's affidavit would have indicated to the court that Microsoft, Google, and NCMEC were reliable sources of information and that the CyberTip reports provided accurate information regarding the distribution of suspected CSAM.

b. File Name

The affidavit also recounted that one of the files identified in the CyberTip reports bore the moniker "pedomom-and-son.jpg." According to the government, the file name reflected terminology commonly associated with child pornography and strongly suggested that the image depicted a woman engaged in a sex act with her minor son. Such naming conventions are typical of CSAM files because, as the government argued before the district court, "[t]hose seeking child pornography often use such a title to conduct a word search of files that would contain child pornography." Dkt. 27 at 4.

We see no reason to disagree with the government's reasoning. The file name "pedomom-and-son" strongly suggests sexualized content involving a minor child. And it makes it more likely than not that the reports from Microsoft, Google, and NCMEC involved CSAM, supporting probable cause for the search. *See United States v. Borowy*, 595 F.3d 1045, 1049 (9th Cir. 2010) (per curiam) (holding that file names that are "explicitly suggestive of child pornography" may support probable cause); *United States v. Loera*, 923 F.3d 907, 929 (10th Cir. 2019)) (noting that a file labeled "Spycam 9yr Undress" "would have been sufficient to establish probable cause to support a warrant to search all of the electronic devices belonging to [defendant]"); *United States v. Haymond*, 672 F.3d 948, 950 (10th Cir. 2012) (noting that a file name's title "8yo" is an acronym for "'8 year old' which is associated with child pornography"); *cf. United States v. Stabile*, 633 F.3d 219, 242 (3d Cir. 2011) (finding probable cause to search a file "once [the detective] saw the lurid file names" under the plain view doctrine); *United States v. Breton*, 740 F.3d 1, 14 (1st Cir. 2014) ("The presence of files with names indicative of child pornography—even absent further proof of what, if anything, those files contained—tends to make it more probable that [the defendant] knowingly was involved with child pornography.").

c. 2015 Investigation

The government also points to a 2015 investigation into allegations that Braun was engaging with young children online. According to Agent Koehler's affidavit, he obtained a December 9, 2015, report from the Village of Lomira Police Department that "detailed information passed on to law enforcement by a teacher of the (then) 15-year-old son of Peter Braun … which alleged that Peter Braun had been observed

by his son chatting/interacting online with very young girls around the time the report was made." Dkt. 22-5 ¶ 39.

Of course, Braun is correct that "the fact of an … investigation alone is probative of nothing." *United States v. Clark*, 668 F.3d 934, 941 (7th Cir. 2012). But, when considered within the totality of the other evidence, this fact tends to support the trustworthiness of the CyberTip reports. In Braun's view, though, the age of the report makes the information stale and less helpful to the government. And, to be sure, "[r]ecency of the information provided to the issuing judge is one factor bearing on the question of probable cause." *United States v. Carroll*, 750 F.3d 700, 703 (7th Cir. 2014) (citing *United States v. Pappas,* 592 F.3d 799, 803 (7th Cir. 2010)). This is because "probable cause measures the likelihood of uncovering evidence of a crime *at the time of* the search." *Edmond v. United States*, 899 F.3d 446, 454 (7th Cir. 2018) (emphasis in original). But "more recent information supporting probable cause can freshen information that might otherwise be stale." *United States v. Bradford*, 905 F.3d 497, 504 (7th Cir. 2018); *see Newsom*, 402 F.3d at 783. Here, the recent CyberTip reports provided that freshening information.

Perhaps any one of these three factors alone might not be sufficient to establish probable cause for the search of Braun's residence. But, when considered together with the other information in the affidavit, we agree with the government that they are enough even without the descriptions to create a fair probability that evidence of CSAM would be found at Braun's home.

2. Decision to Seek Warrant

Establishing probable cause absent the tainted information, however, is just the first step of the analysis. We also must determine whether "the decision to seek the warrant was prompted by information unlawfully obtained." *Scott*, 731 F.3d at 664. But the two inquiries overlap to some degree. As we have observed, "[t]he answer to the first part of the inquiry is relevant to the second—once an officer has probable cause to believe a piece of property contains evidence of a crime, it is hard to see how an additional illegal search would alter the officer's desire to examine the property." *United States v. Bell*, 925 F.3d 362, 371 (7th Cir. 2019).

It is clear from this record that Agent Koehler would have decided to seek the warrant regardless of whether he actually viewed the images. As described above, he received four CyberTip reports from trusted sources who had previously provided him with reliable information in previous CSAM investigations. He noticed the peculiar name on one of the files that further supported the reports. And he later learned that Braun may have had a history of engaging with young children online.

On this record, we conclude that Agent Koehler had all the information he needed to secure a warrant to search Braun's home even without viewing the files themselves. *Scott*, 731 F.3d at 666 (finding that agent's "decision to seek the warrant was [not] prompted by information unlawfully obtained" because "other facts [in the affidavit] were sufficient to create probable cause"). That he would have proceeded to seek a warrant to search Braun's home based on this information is a short logical leap.

* * *

For the foregoing reasons, the judgment is REVERSED.

BRENNAN, *Chief Judge*. I am pleased to join the majority opinion in full. I write separately about two of the district court's rulings not discussed on appeal. Each is troubling, and our reversal on different grounds should not be read as endorsing the district court's reasoning or conclusions on those rulings.

I

The first issue involves hash-value matching. Electronic service providers, like Google and Microsoft, assist law enforcement by identifying child sexual abuse material (CSAM). Understandably, providers do not want to ask their employees to examine CSAM every time a flagged photo is shared on their platform. Thus, providers use a tool called hash-value matching. A "hash value is a string of characters that together represent a file's unique, algorithmically generated 'digital fingerprint.'" *United States v. Brillhart*, 181 F.4th 1181, 1185 (11th Cir. 2026). Providers have a repository of previously determined CSAM, and if a flagged photo has a hash value that matches the value of a photo in the repository, the providers relay the information to the National Center for Missing and Exploited Children (NCMEC). Then, law enforcement will view the images to confirm they are CSAM. That is what happened here: Google and Microsoft hash-value matched Braun's photographs (but did not visually inspect them) and forwarded them to NCMEC, which alerted Special Agent Aaron Koehler, who viewed the images.

Agent Koehler did not need a warrant to view these photos. Under the private-search doctrine, authorities may replicate a private party's search as long as their search does not exceed the scope of the initial private search. So, for example, if employees of a freight-carrier inspect a package and find a

"tube containing plastic bags and, ultimately, white powder," a DEA agent may also manually inspect the package. *United States v. Jacobsen*, 466 U.S. 109, 118 (1984). By contrast, when a private person opens a mistakenly-delivered package containing videotapes and reads descriptive labels on those tapes, the scope of that private search would be exceeded if the police watch those tapes. *Walter v. United States*, 447 U.S. 649, 656 (1980) (plurality opinion).

If an internet service provider has matched the hash value of a CSAM photograph, and an officer then views the photograph, he has not exceeded the scope of the provider's search. Matching hash values is functionally the same as a human comparing two pictures. "A hash value is a string of characters that together constitute a file's unique digital signature or fingerprint, such that if two files have the same hash value, they're the same file." *Brillhart*, 181 F.4th at 1191 (citation modified). Whether an officer's search exceeds the scope of the private search hinges on whether there is "virtual certainty" that authorities will find "nothing else of significance." *Jacobsen*, 466 U.S. at 119. Hash-value matching, therefore, is a suitable replacement for human comparison. It was virtually certain Agent Koehler would find nothing but the identified CSAM because the photos' hash values matched photos already confirmed as CSAM by human review.

That conclusion is consistent with several circuits. *See Brillhart*, 181 F.4th at 1191; *United States v. Reddick*, 900 F.3d 636, 640 (5th Cir. 2018); *United States v. Miller*, 982 F.3d 412, 429–30 (6th Cir. 2020). Instead, the district court here ruled that an agent's viewing of CSAM images exceeds the scope of the provider's private search and thus needed a warrant. In doing so, it sided with other circuits. *See United States v.*

Lowers, 170 F.4th 134, 156 (4th Cir. 2026); *United States v. Maher*, 120 F.4th 297, 314 (2d Cir. 2024); *United States v. Wilson*, 13 F.4th 961, 971 (9th Cir. 2021). In my view, respectfully, the first set of decisions is more persuasive than the latter set of decisions.

The district court's ruling too quickly dismissed the fact that hash-value matching is nearly perfect. We said as much in *United States v. Owens*: "if the hash value of two files matches up, then the chances are 'astronomically small' that the two files are different." 18 F.4th 928, 932 n.1 (7th Cir. 2021). As the Sixth Circuit observed, the Federal Judicial Center explained that the chances "that any two data sets will have the same [hash value], no matter how similar they appear, is less than one in one billion." *Miller*, 982 F.3d at 430. One government manual put the odds at 1 in 9,223,372,036,854,775,808. *See id.*

Next, the district court's statement that "the Supreme Court has never suggested that the police may dispense with a warrant just because they are sure what they will find"[1] is difficult to square with *Jacobsen*'s instruction that law enforcement may recreate a private search as long as it is a "virtual certainty" law enforcement will find "nothing else of significance." 466 U.S. at 119. If a photograph's hash values match those of a confirmed CSAM photo, it is virtually impossible that a police officer will find anything but confirmed CSAM when he views the image. So, the district court's concern that law enforcement might find photographs embarrassing and invasive—but legal—verges on the hypothetical.

---

[1] Dkt. 59 at 13.

The district court also noted that an agent's viewing of CSAM is analogous to the facts in *Walter*. There, a fractured Court held that if a private party reads a descriptive label on a videotape, authorities exceed the scope of that private search by playing the videotape. 447 U.S. at 656–57. Yet hash values are not labels. Instead, they are akin to fingerprints or DNA. Rather than describe the photos, the technology opened and inspected the files, "revealing that they had the same content as files that Google had already found to be child pornography." *Miller*, 982 F.3d at 431.

As the Eleventh Circuit thoughtfully explained in *Brillhart*, a hash value, not the photograph, "*is* the content," because a hash value is 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." 181 F.4th at 1194. Put differently, matching hash values confirms two photos as identical. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 541 (2005) ("If the two identical files are inputted, however, the hash function will generate identical output."). As noted above, providers have a repository of photos which humans have previously reviewed and determined to be CSAM. *See Brillhart*, 181 F.4th at 1191. So, a hash-value match to a photo in the repository confirms that photo as CSAM. Even more, that the original photo in the repository could be mistakenly deemed illegal does not matter under the private search doctrine because the private actor's search voids any original expectation of privacy. *Jacobsen*, 466 U.S. at 114–15, 119; *Miller*, 982 F.3d at 431.

Consider a familiar example: if a computer reads a published opinion and identifies it as "389 U.S. 347 (1967)," that is functionally the same as designating the case "*Katz v. United*

States." If an agent reads the case and confirms it is *Katz*, he has not exceeded the scope of what the computer has conveyed. The district court failed to address these points, despite its conclusion that a police officer "clearly" expands a private search by viewing a hash-matched CSAM photo.[2]

The touchstone of the Fourth Amendment is reasonableness. *Lange v. California*, 594 U.S. 295, 301 (2021). Google and Microsoft understandably do not wish to repeatedly expose their employees to thousands of CSAM images. Here, Braun's photographs included CSAM of minors engaging in sex acts with household objects and animals, and a photo of a mother and young child engaging in a sex act. Internet service providers developed a tool to replace human review, which effectively guarantees that a flagged photograph is CSAM. The accuracy and technology behind hash-value matching protects a user's reasonable expectation of privacy in his images while also helping officers address these crimes.

II

The second matter is Braun's release pending appeal. When the government appeals, and the defendant seeks release pending that appeal, 18 U.S.C. § 3143(c) instructs courts to apply the pretrial detention standards of 18 U.S.C. § 3142. Detention is determined by considering several factors, among them "the nature of the charged offense, the defendant's history and characteristics, and the risk to the public."

---

[2] A related question is whether Braun lost an expectation of privacy by agreeing to Google's and Microsoft's terms of service. A future panel of this court may have to reconcile *Chatrie v. United States*, 146 S. Ct. 2193, 2212–15 (2026), and *United States v. Blocker*, 174 F.4th 587, 590–92 (7th Cir. 2026).

United States v. Wilks, 15 F.4th 842, 846 (7th Cir. 2021) (citing § 3142(g)).

Here, the district court incorrectly suppressed the evidence obtained from the warrant. Then, it ordered Braun released from custody during this appeal.

On my review of this record, Braun was and is a danger to the community. For his acts, which he admitted to, he faced 120 years in prison. In his home, police found 81 compact discs. When law enforcement viewed the CDs, they discovered that Braun had induced minors as young as nine years old to engage in disturbing sex acts involving household objects, bestiality, and younger relatives. In one video, a minor is being sexually assaulted by her grandfather while Braun watches.

For many reasons, Braun is a continued threat to the people of the Eastern District of Wisconsin. He has a history of deception: police interviewed four victims, who explained that Braun had used a picture of his son as a façade to pose as a minor. He has at least a dozen victims, one of which he attempted to meet at a Wisconsin ice cream parlor. One of his victims wrote a letter, which the government read to the court at the bond hearing, stating, "Releasing him would not only be a betrayal to his victims, but it would—but it would also put more innocent lives at risk."

Braun is likely to continue his behavior. He admitted to watching and producing child pornography for the past 20 years, showing no signs he could stop. The government pointed out that Braun may have unfettered internet access through his employer. He is also familiar with the dark web and computer technology. What is more, Braun is connected

to a woman who lives in the Philippines. She has a minor son, and the government offered evidence that Braun was sending her incestual CSAM for her to recreate over webcam for money.

The district court ordered Braun's release, reasoning in part that "he's been in jail for a long time," and "there's never been any direct assault … any face-to-face assault."[3] That Braun had not directly sexually assaulted a child does not vitiate the seriousness of his crimes—manipulating more than a dozen children to produce horrific CSAM. In a future case like this, courts should ensure that a defendant like Braun does not put the community at risk.

* * *

The panel here correctly chooses not to discuss these topics, as we are confined to the government's arguments and litigation choices. These omissions should not be taken as approval of the district court's decisions on these serious doctrinal and safety questions.

[3] The court imposed other conditions of release, such as GPS monitoring, a curfew, residence at a specified address, and a prohibition on possessing any device with internet access.