UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA
Plaintiff,

v. **Case No. 24-CR-164**

PETER BRAUN
Defendant.

DECISION AND ORDER

Defendant Peter Braun, charged with production of child pornography, moved to suppress evidence obtained by law enforcement during the execution of a search warrant. The magistrate judge handling pre-trial proceedings in this case issued a recommendation that the motion be denied. Defendant objects, requiring me to review the matter de novo. Fed. R. Crim. P. 59(b).

I. FACTS AND BACKGROUND

Microsoft and Google use "hash matching" technology to detect suspected child pornography on their platforms. As the Tenth Circuit recently explained:

> A "hash value" is a short string of characters generated from a much larger string of data (say, an electronic image) using an algorithm—and calculated in a way that makes it highly unlikely another set of data will produce the same value. 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) (internal citations and quote marks omitted). Federal law requires an electronic service provider ("ESP"), such as

Microsoft or Google, to report to the National Center for Missing and Exploited Children ("NCMEC") any apparent child pornography of which it is aware. 18 U.S.C. § 2258A(a)(1). ESPs report such material using the NCMEC's CyberTipline; the NCMEC, in turn, notifies the appropriate local law enforcement agency. See United States v. Bebris, 4 F.4th 551, 553 (7th Cir. 2021) (discussing this process). Sometimes an ESP employee will visually examine the suspected child pornography file prior to notifying the NCMEC; other times, the ESP relies on matching hash values.

In September 2020, the NCMEC received four CyberTipline reports (three from Microsoft, one from Google) indicating images of suspected child pornography had been uploaded to their platforms from a particular IP address. (R. 22 at 1; R. 39 at 2-3.) The reports all indicated the ESP had not viewed the contents of the uploaded files. (R. 22 at 3; R. 22-1 at 4; R. 22-2 at 4; R. 22-3 at 4; R. 22-4 at 4; R. 27 at 3; R. 39 at 2-3.) While the ESPs made four reports, just two images were involved. (R. 22-5 at 17 ¶ 34, 18 ¶ 36; R. 27 at 1; R. 37-1 at 3-4.) ESPs have created a classification system for such images, under which the letter "A" means the image involves a prepubescent minor, the letter "B" a pubescent minor, the number "1" a sex act, and the number "2" lascivious exhibition. (E.g., R. 22-2 at 5.) Here, one of the images was classified A1, the other A2. (R. 22-1 at 4; R. 22-2 at 4.)

The NCMEC placed the IP address in Lomira, Wisconsin and forwarded the reports to the Wisconsin Department of Justice, Division of Criminal Investigation ("DCI"). (R. 22 at 3-4; R. 27 at 4; R. 39 at 3.) The DCI issued an administrative subpoena for subscriber information for the IP address, determining it listed to defendant. (R. 22 at 4; R. 27 at 5; R. 39 at 3.)

In January 2021, DCI Special Agent Aaron Koehler viewed the images from the reports and determined them to be child pornography. (R. 22 at 4; R. 37-1 at 3-4; R. 39 at 3.) He then

conducted surveillance of defendant's residence and received further information from the Lomira Police Department, specifically, a December 2015 report indicating a teacher of defendant's then 15-year-old son passed on information that the son had seen defendant chatting/interacting online with very young girls around the time the report was made. (R. 22-5 at 19-20 ¶ 39.)

In March 2021, Koehler applied for a warrant to search defendant's residence. (R. 22 at 4; R. 22-5 at 1, 19-20; R. 39 at 3-4.) The warrant affidavit noted the CyberTipline reports (R. 22-5 at 3 ¶ 6, 17 ¶¶ 31-33), described the two images (R. 22-5 at 17-18 ¶ 34-36), and included the 2015 report about defendant chatting online with young girls (R. 22-5 at 20 ¶ 39). Koehler averred that he believed the information provided by Microsoft and Google to be reliable and correct because it was provided as part of their official duties, and information provided by these parties in the past was found to be accurate and reliable. (R. 22-5 at 21 ¶ 43.) However, he did not discuss hash matching, in general or regarding these particular files. The application was reviewed and approved by a state prosecutor. (R. 22-5 at 21 ¶ 44.)

A Wisconsin state court judge issued the warrant (R. 22-5 at 27-34), and during execution law enforcement recovered child pornography, including the images referenced in the CyberTipline reports. (R. 27 at 6; R. 39 at 4.) State authorities prosecuted defendant for possession of child pornography, and he was sentenced to 3 years in prison. (R. 22 at 5; R. 27 at 6; R. 39 at 4.) Law enforcement also recovered various compact discs (CDs) containing suspected child pornography, which, later investigation revealed, defendant had allegedly recorded from his online interactions with minor girls; this material forms the basis for the instant charges. (R. 22 at 5-6; R. 27 at 6-7; R. 39 at 4.)

II. DISCUSSION

Defendant argues that Koehler violated the Fourth Amendment when he viewed the files reported by the NCMEC without first obtaining a warrant.[1] As indicated, the CDs forming the basis for the instant indictment were seized later pursuant to a search warrant. However, "evidence discovered pursuant to a warrant will be inadmissible if the warrant was secured from a judicial officer through the use of illegally acquired information." United States v. Shelton, 997 F.3d 749, 770 (7th Cir. 2021). A search warrant that has been obtained, in part, with evidence which is tainted will still support a search if the untainted information, considered by itself, establishes probable cause. Id.

Defendant's challenge to Koehler's viewing of the images requires consideration of the so-called "private search doctrine." (R. 22 at 6, 8.) Under that doctrine, police may repeat a search conducted by a private party so long as they do not exceed the scope of the earlier

[1]Defendant contends that he had a reasonable expectation of privacy in the files. (R. 22 at 7-8.) The government notes that after matching the hash values each ESP shut down defendant's account, consistent with its terms and conditions. (R. 27 at 3, 12.) However, the government develops no argument that this action, or the ESP's terms of service permitting such action, defeated defendant's expectation of privacy. See United States v. Berkowitz, 927 F.2d 1376, 1384 (7th Cir. 1991) ("We repeatedly have made clear that perfunctory and undeveloped arguments, and arguments that are unsupported by pertinent authority, are waived (even where those arguments raise constitutional issues)."). The government did seek to develop a different argument: that Koehler did not view defendant's copy of the images; instead, he viewed identical (hash-matched) images provided by the NCMEC. (See R. 27 at 12.) The government argued the point was potentially dispositive, as defendant had no privacy interest in images already in law enforcement databases. (R. 46 at 2.) On initial review of the objections, I noted that Koehler's report, which defendant presented to the magistrate judge, was equivocal on this point and did not permit the court to determine which version of the images Koehler viewed. (R. 54 at 7.) I accordingly scheduled an evidentiary hearing. (R. 56.) Prior to the hearing, the government filed a supplement indicating that its previous representation that Koehler viewed images from a law enforcement database was based on a mis-communication; based on subsequent conversations with Koehler, the government clarified that he viewed only images that were contained in the NCMEC CyberTipline reports. (R. 57 at 1.) I accordingly canceled the hearing. (R. 58.)

private search. See Bebris, 4 F.4th at 560 ("[A]uthorities typically may repeat a private search already conducted by a third party but may not expand on it—a legal principle that has been described as the private search doctrine."). The doctrine can be traced to two Supreme Court cases: United States v. Jacobsen, 466 U.S. 109 (1984) and Walter v. United States, 447 U.S. 649 (1980).

In Walter, boxes containing pornographic films were mistakenly delivered to the wrong business. 447 U.S. at 651 (plurality opinion). Employees of the business opened the boxes and saw on the films' labels "suggestive drawings" and "explicit descriptions" of the films' contents. Id. at 652. The company contacted the FBI, which took possession of the boxes, and an FBI agent, acting without a warrant, viewed the films using a projector. Id. A fractured Court concluded that the FBI's warrantless viewing of the films violated the Fourth Amendment. In the plurality opinion announcing the Court's judgment, Justice Stevens stated that there was nothing wrongful about the government's acquisition of the boxes or its examination of their contents to the extent that they had already been examined by a private party. Id. at 656. However, the private party had not actually viewed the films, making the FBI's projection a "significant expansion" of the previous search. "That separate search was not supported by any exigency, or by a warrant even though one could have easily been obtained." Id. at 657.

Justice Stevens rejected the government's argument that because the packages had been opened by a private party, thereby exposing the descriptive labels on the boxes, the defendants no longer had any reasonable expectation of privacy in the films. Id. at 658. While the mis-delivery partially frustrated their expectation that no one except the intended recipient would either open the boxes or project the films, the private search "merely frustrated that expectation in part. It did not simply strip the remaining unfrustrated portion of that expectation

of all Fourth Amendment protection. Since the additional search conducted by the FBI—the screening of the films—was not supported by any justification, it violated that Amendment." Id. at 659.

In Jacobsen, Federal Express employees opened a damaged package, discovering a tube constructed of duct tape, cut open the tube, and found four plastic bags filled with white powder. Federal Express notified the DEA and put the items back into the box. Upon arrival, a DEA agent reopened the box, removed the tube from the box, the plastic bags from the tube and a small amount of white powder from one of the bags, then conducted a field test on the powder, which reacted positively for cocaine. 466 U.S. at 111-12. The Supreme Court held that the private search doctrine supported the agent's warrantless removal of the tube from the box and the plastic bags from the tube, as these actions merely duplicated the search previously conducted by Federal Express employees and caused no additional invasion of privacy. Id. at 115; see id. at 119 ("[T]here was a virtual certainty that nothing else of significance was in the package and that a manual inspection of the tube and its contents would not tell him anything more than he already had been told."). The field test did effect an additional intrusion, but the Court ruled that no warrant was required because the test disclosed only whether or not the suspicious white powder was cocaine and no other arguably private fact. Id. at 122-23.

Courts have applied the private search doctrine in a variety of child pornography prosecutions. In cases where a private party, such as an ESP employee, has visually examined the suspected child pornography file before passing it on to authorities, courts have held that the private search doctrine permits law enforcement to (also) view the image without obtaining a warrant. See United States v. Maher, 120 F.4th 297, 313 n.13 (2nd Cir. 2024) (collecting cases); United States v. Jeffery, No. 23-4264, 2024 U.S. App. LEXIS 29787, at *9-10 (4th Cir.

Nov. 22, 2024) (affirming the district court's factual finding that Microsoft conducted an eyes-on review before police did); see also Rosenschein, 136 F.4th at 1254 (rejecting the argument than an ESP acts as a government agent in this context); Bebris, 4 F.4th at 562 (same).[2] Courts have also held that police may view without a warrant images the defendant uploads for sharing with strangers online. Rosenschein, 136 F.4th at 1257 (collecting cases finding no reasonable expectation of privacy in such images), 1259 (finding that a detective did not need a warrant to view such uploads).

However, courts have differed over the specific question presented in this case: whether the private search doctrine authorizes law enforcement to conduct a warrantless examination of the contents of a digital file where the ESP has not visually inspected the contents of that file but instead relied on hash matching in making a CyberTipline report. The Fifth and Sixth Circuits have held the doctrine applies in this context, United States v. Miller, 982 F.3d 412 (6th Cir. 2020); United States v. Reddick, 900 F.3d 636 (5th Cir. 2018), while the Second and Ninth Circuits have come to the opposite conclusion, Maher, 120 F.4th at 320; United States v. Wilson, 13 F.4th 961 (9th Cir. 2021); see also United States v. Holmes, 121 F.4th 727 (9th Cir. 2024).

In Reddick, after the defendant uploaded the subject files to a Microsoft platform, an automated program reviewed the hash values of those files and compared them against an existing database of known child pornography hash values. The Fifth Circuit reasoned that, "whatever expectation of privacy [the defendant] might have had in the hash values of his files

[2]The Tenth Circuit has held that the NCMEC is a governmental entity or agent. United States v. Ackerman, 831 F.3d 1292, 1296-1304 (10th Cir. 2016). Because the NCMEC did not view the images at issue in the present case, I need not address its status.

was frustrated by Microsoft's private search." 982 F.3d at 639. Accordingly, when a detective opened the files, there was no significant expansion of the search that had been conducted previously by a private party. "His visual review of the suspect images—a step which merely dispelled any residual doubt about the contents of the files—was akin to the government agents' decision to conduct chemical tests on the white powder in Jacobsen." Id.; see also id. at 640 ("The government effectively learned nothing from [the detective's] viewing of the files that it had not already learned from the private search.").

In Miller, the Sixth Circuit declined to rely on Reddick's determination "that the detective's viewing of the images was like the DEA agent's testing of the powder in Jacobsen." 982 F.3d at 429. The Jacobsen Court recognized that this testing "exceeded the scope" of the Federal Express employees' search, upholding the test for a reason unrelated to the private search doctrine. Specifically, that "binary test" revealed only whether or not the white powder was cocaine (a contraband substance); if the test came back negative, it would not disclose what the substance actually was (e.g., sugar or talcum powder). The Sixth Circuit acknowledged that this logic does not cover an officer's actions in viewing a file attached to a CyberTipline report. If such a file portrays something other than child pornography, e.g., an embarrassing picture of the sender, an additional invasion of privacy will have occurred. Id. Instead of comparing an officer's viewing of the files to the agent's field test, the court compared the ESP's search of the files to the Federal Express employees' search of the box. The court then concluded that, given the high reliability of hash matching, which Miller had not challenged, it was "virtually certain" that viewing the files would reveal the same images previously determined to be child pornography. Id. at 429-30. Continuing in a more pragmatic vein, the court stated:

> [T]he information on which the district court relied suggests that a computer's virtual search of a single file creates more certainty about the file's contents than a person's manual search of the file. Most people who view images do not use a magnifying glass to undertake a pixel-by-pixel inspection. Common hash algorithms, by contrast, catalogue every pixel. Suppose a private party gets only a quick view of a picture before concluding that it is child pornography and handing the picture to the police. Under Jacobsen, that inspection would likely trigger the private-search doctrine and allow the police to reexamine the picture more thoroughly, despite the risk of a flaw in the person's recollection. What sense would it make to treat a more accurate search of a file differently?

Id. at 430-31 (cleaned up).

In Wilson, the Ninth Circuit held that an agent's viewing of previously uninspected files attached to a CyberTipline report was more like the FBI's projection of the films in Walter than the DEA's search of the box in Jacobsen. 13 F.4th at 972-73. The court reasoned that the CyberTip functioned like a label, while the agent's viewing of the file (like the projection of the film) permitted him to learn exactly what the image showed. Id. at 973. The court further noted that Fourth Amendment rights are personal. "Even if Wilson's email attachments were precise duplicates of different files a Google employee had earlier reviewed and categorized as child pornography, both Walter and Jacobsen—and general Fourth Amendment principles—instruct that we must specifically focus on the extent of Google's private search of Wilson's effects, not of other individuals' belongings[.]" Id. at 975. The court then reasoned that, while Wilson did not have an expectation of privacy in other individuals' files, he did have an expectation of privacy in his files, even if others had identical files. Id. at 975.

> If, for example, police officers search someone else's house and find documents evidencing wrongdoing along with notes indicating that I have identical documents in my house, they cannot, without a warrant or some distinct exception to the warrant requirement, seize my copies. I would retain a personal expectation of privacy in them, and in my connection to them, even if law enforcement had a strong basis for anticipating what my copies would contain. A violation of a third party's privacy has no bearing on my reasonable expectation of privacy in my own documents.

Id.

The Ninth Circuit rejected Reddick because it conflated Jacobsen's first holding regarding the private search exception to the Fourth Amendment with its second holding regarding whether the field test constituted a search under the Fourth Amendment. Id. at 978. The court also rejected Miller's focus on the assumed reliability of hash matching technology. Id. at 979. Unlike Miller, Wilson did challenge the "accuracy and reliability" of the hashing technology. The Ninth Circuit further noted that, "contrary to Miller's assertion, the government bears the burden to prove its warrantless search was permissible." Id. The court then concluded:

> Our analysis, however, relies only contingently on the adequacy of the record with regard to the hash match technology. In our view, the critical factors in the private search analysis, both unacknowledged in Miller, include the personal nature of Fourth Amendment rights and the breadth of essential information Agent Thompson obtained by opening the attachment, information—and a privacy invasion—well beyond what Google communicated to NCMEC. . . . The reliability of Google's proprietary technology, in our estimation, is pertinent to whether probable cause could be shown to obtain a warrant, not to whether the private search doctrine precludes the need for the warrant.

Id.; see also Holmes, 121 F.4th at 733 (following Wilson).

Finally, in Maher, the Second Circuit agreed with the Ninth Circuit's application of the private search doctrine in this context. The Second Circuit rejected Reddick, noting that the Fourth Amendment does not "permit law enforcement officials to conduct warrantless searches of unopened property to confirm a private party's report—however strong—that the property contains contraband." 120 F.4th at 315. The ESP's report that Maher's unopened file contained an image whose hash value matched that of an image previously determined to depict child pornography may have provided authorities with probable cause to obtain a warrant, but it "did not authorize them to conduct an unwarranted search of the unopened Maher file to confirm

that belief." Id. The court further noted that, unlike the field test in Jacobsen, visual inspection of a computer file would reveal more than a binary result; it would "reveal particulars, ranging from the innocuous to the embarrassing, that the account holder reasonably expected were private." Id. at 316.

The Second Circuit also disagreed with Miller's reasoning that the high reliability of hash matching technology created a "virtual certainty" that the warrantless search would reveal the same evidence uncovered in the private search. Id. "[E]ven if the government in this case had offered evidence that Google's hash matching technology made it virtually certain that the images contained in two hash matched files were identical, the match did not permit the government to go further than Google had and to examine visually the contents of the Maher file without a warrant." Id. at 317 (footnote omitted). The court concluded:

> Insofar as Google searched the Maher file for a hash value that matched the hash value previously assigned to an image identified by a Google employee or contractor as depicting child pornography, the private search doctrine likely would have permitted police to rely on that computer match to demonstrate probable cause to support warrants for their own searches of Maher's Google accounts and residence. It might also have permitted the government—with sufficient foundation—to offer evidence of the match at trial. But here, the police understandably wanted to obtain evidence of more than a hash match. They wanted evidence of the particulars depicted in the matched Maher file image. Because no one at Google had ever opened or visually examined the contents of the Maher file, and because such a visual examination would reveal more information than Google knew at the time it reported the Maher file to the NCMEC, such a visual examination by the police did not fall within the private search doctrine's exception to the warrant requirement.
>
> In sum, we here conclude that the private search doctrine does not authorize government authorities to conduct a warrantless human visual examination of the contents of an unopened file attached to an email based on Google's computer hash value match of an image in that file to another image previously identified by a Google employee or contractor as child pornography. The former search does not duplicate the latter but rather exceeds its scope, thereby allowing authorities to learn more than had been revealed by the private search. In so holding, we suggest no constitutional limitation on Google's own ability, as a

> private actor, to search for and remove child pornography on its platform. Nor do we limit government authorities from using a private party's reliable hash matches between an identified image of child pornography and an unviewed file image to demonstrate probable cause for a warrant to conduct more expansive searches. But as the Ninth Circuit has explained, the reliability of a company's hash matching technology is pertinent to whether probable cause could be shown to obtain a warrant, not to whether the private search doctrine precludes the need for the warrant.

Id. at 319-20 (internal citations and quote marks omitted).

The Second and Ninth Circuits have the better of the argument.[3] By viewing an image the ESP has not examined, a police officer clearly expands on the previous private search. Contrary to the Fifth Circuit's position, viewing the image cannot be compared to a field test, which reveals only whether or not a substance is contraband. The inspecting officer will learn precisely what the images depicts, not just whether it meets the legal definition of child pornography. And if the image does not meet that definition, the sender could be exposed to further embarrassment and invasion of privacy. In Miller the Sixth Circuit acknowledged this flaw in the Fifth Circuit's analysis but, deferring to the district court's factual finding, which Miller did not contest with evidence, found hash matching so reliable as to make it virtually certain a visual inspection will confirm the presence of child pornography. But this argument ignores that the government bears the burden of justifying a warrantless search. See Walton v. Nehls, 135 F.4th 1070, 1076 (7th Cir. 2025) ("[I]n the Fourth Amendment context, the Supreme Court has long held that warrantless searches are presumptively unreasonable. Under that presumption, the government bears the burden of showing that a warrantless search was

[3]The magistrate judge seemed sympathetic to the Sixth Circuit's approach, although he reached no conclusion on the merits. (R. 39 at 10: "Assuming Koehler viewed Braun's copy of the images, doing so was still likely not a 'search' because it was virtually certain that the files contained child pornography, in which Braun has no legitimate privacy interest.".)

nevertheless constitutional.") (cleaned up). More importantly, the Supreme Court has never suggested that the police may dispense with a warrant just because they are sure what they will find:

> [N]o amount of probable cause can justify a warrantless search or seizure absent exigent circumstances. Incontrovertible testimony of the senses that an incriminating object is on premises belonging to a criminal suspect may establish the fullest possible measure of probable cause. But even where the object is contraband, this Court has repeatedly stated and enforced the basic rule that the police may not enter and make a warrantless seizure.

Horton v. California, 496 U.S. 128, 137 n.7 (1990) (internal quote marks omitted).

The government argues that, even excising Koehler's description of the images, the warrant application established probable cause. (R. 27 at 13.) The government notes that Microsoft, Google, and the NCMEC each found hash values that matched previously identified images of child pornography. The application also described SA Koehler's other investigative steps. (R. 27 at 13.)

The problem with this argument is that the warrant affidavit says nothing about the reliability of hash matching, either in general or as used in this particular case, as the magistrate judge noted. (R. 39 at 10-11; see also R. 37 at 6-7.) Accordingly, while I have no reason to quarrel with the proposition that hash values can establish probable cause (see R. 27 at 13-14), that cannot save the search warrant here. See United States v. Koerth, 312 F.3d 862, 871 (7th Cir. 2002) (limiting review to the four corners of the warrant application). The government develops no argument 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.

In the objection briefing, the government repeats its argument that the warrant was

supported by probable cause, even without the description of the images, given the reliability of hash matching. (R. 46 at 3.) However, the government does not address the absence of any information about hash matching in the affidavit.

The magistrate judge ultimately recommended denial of defendant's motion based on the "good faith" exception to the exclusionary rule. (R. 39 at 11.) The good faith exception follows from the purpose of the exclusionary rule: to deter official misconduct. Accordingly,

> To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system. As laid out in our cases, the exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence.

Herring v. United States, 555 U.S. 135, 144 (2009). Under the exception, exclusion of evidence is not required when the police conduct a search in "objectively reasonable reliance" on, e.g., a warrant later held invalid, United States v. Leon, 468 U.S. 897, 922 (1984); on a subsequently invalidated statute, Illinois v. Krull, 480 U.S. 340, 349-50 (1987); or, as is pertinent here, on binding judicial precedent later overruled, Davis v. United States, 564 U.S. 229, 239-40 (2011); see id. at 249-50 ("We therefore hold that when the police conduct a search in objectively reasonable reliance on binding appellate precedent, the exclusionary rule does not apply.").

As discussed above, four circuits have address this issue; the Seventh Circuit is not one of them. At the time Koehler viewed the files in early 2021, two circuits, the Fifth and Sixth, supported his actions (albeit on different grounds). The Ninth's Circuit's decision in Wilson came later in 2021 and the Second Circuit's decision in Maher in 2024.[4]

[4]In Ackerman, decided in 2016, the Tenth Circuit referenced the scenario at issue in this case but did not rule on it. See 831 F.3d at 1306-07 ("Interesting questions, to be sure, but

The magistrate judge reasoned that, while the Seventh Circuit has not addressed the precise issue presented here, at the time Koehler viewed the files the Supreme Court had held in Jacobsen that an officer could perform a test on a suspicious item provided by a private party to confirm whether it was contraband; two circuits had held that police may view uninspected images turned over by an ESP based on hash matching; and no circuit had (yet) found that viewing such images required a warrant. (R. 39 at 12-13.) And, despite agreeing the officer violated the Fourth Amendment by viewing the file, the Second Circuit in Maher declined suppression under the good faith exception. (R. 39 at 13, citing 120 F.4th at 321-22.) But see Holmes, 121 F.4th at 737 (declining to apply good faith).

In order to resolve defendant's objection to the magistrate judge's recommendation, I must assess the scope of the exception recognized in Davis. Does it require "binding appellate precedent" authorizing the particular police practice at issue, the specific holding of Davis, or

---

ones we don't have to resolve in this case. We don't because the 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 but three others as well.")."[F]ederal law, not state law, controls the admissibility of evidence in a federal prosecution, even if the evidence was seized by state officials and would not be admissible in state court." United States v. Rainone, 816 F.3d 490, 496 (7th Cir. 2016). Nevertheless, because Koehler is a state law enforcement officer, I have also reviewed Wisconsin appellate decisions. In State v. Gasper, 414 Wis. 2d 532 (Ct. App. 2024), review granted, 2025 Wisc. LEXIS 129 (Wis. Mar. 13, 2025), the Wisconsin court of appeals (district two) held that the Fourth Amendment was not implicated by a similar search because, based on the ESP's terms of service, the account holder had no reasonable expectation of privacy in files containing child pornography. As discussed above, the government has not developed such an argument in the present case. Earlier this year, the court of appeals (district four) issued an opinion disagreeing with Gasper's analysis (though not its result) and certifying issues to the state supreme court, including whether a law enforcement officer is required to obtain a warrant before opening and viewing any files that the ESP sent to the NCMEC, which then sent the files to law enforcement. State v. Sharak, No. 2024AP469-CR, 2025 Wisc. App. LEXIS 42, at *2 (Wis. Ct. App. Jan. 16, 2025), petition granted, 2025 Wisc. LEXIS 130 (Wis. Mar. 13, 2025). Sharak and Gasper were argued on September 2, 2025. It appears no Wisconsin appellate decision had previously addressed this specific issue.

does it incorporate the Supreme Court's more general good faith test, that evidence should not be suppressed where the police acted with a good faith belief in the lawfulness of their conduct that was "objectively reasonable"? See United States v. Katzin, 769 F.3d 163, 173 (3rd Cir. 2014) (en banc) (discussing the issue).[5]

The Second Circuit applied the broader version of the good faith rule in Maher. See 120 F.4th at 322 (citing Davis's "binding appellate precedent" language, but then noting that the rule "can also apply where a relevant legal deficiency was not previously established in precedent, such that the agent's failure to recognize that deficiency cannot vitiate good faith") (cleaned up, emphasis added). The Ninth Circuit, conversely, has "taken a narrow view of when precedent specifically authorizes an action." Holmes, 121 F.4th at 737.

In United States v. Matthew Martin, a case involving the warrantless attachment and use of a GPS device, the Seventh Circuit endorsed the narrow view:

> Davis expanded the good-faith rationale . . . only to "a search [conducted] in objectively reasonable reliance on binding appellate precedent," finding that this

---

[5]Many of the cases discussing good faith involve the warrantless installation or monitoring of GPS tracking devices prior to the Supreme Court's decisions in United States v. Jones, 565 U.S. 400 (2012) (holding that installation of a GPS device on the defendant's vehicle and use of that device to monitor the vehicle's movements constituted a Fourth Amendment search), and Carpenter v. United States, 585 U.S. 296 (2018) (holding that tracking a person with cell-site data is a search). Most circuits, including the Seventh, had approved these practices. See, e.g., United States v. Garcia, 474 F.3d 994 (7th Cir. 2007). In Katzin, the majority applied both variants of the good faith rule, first holding that, while no Third Circuit case had endorsed such tracking, the agents could have reasonably relied on, as "binding precedent," the Supreme Court's previous decisions in United States v. Knotts, 460 U.S. 276 (1983) and United States v. Karo, 468 U.S. 705 (1984), both of which involved "beepers." 769 F.3d at 173-74. Katzin also concluded, under the second variant of the good faith rule, that the agents could have relied on the "nearly uniform consensus across the federal courts of appeals that addressed the issue that the installation and subsequent use of a GPS or GPS-like device was not a search, or, at most, was a search but did not require a warrant." Id. at 180 (collecting cases, including Garcia). See also United States v. Richard Martin, 807 F.3d 842 (7th Cir. 2015) (holding that good faith applied to post-Garcia GPS tracking).

> set of searches are not subject to the exclusionary rule. See Davis, 131 S. Ct. at 2434 (emphasis added). As Justice Sotomayor pointed out in her opinion concurring in the judgment, Davis "d[id] not present the markedly different question whether the exclusionary rule applies when the law governing the constitutionality of a particular search is unsettled." 131 S. Ct. at 2435. The Supreme Court may decide to expand Davis in the coming years, but until it does so, we are bound to continue applying the traditional remedy of exclusion when the government seeks to introduce evidence that is the "fruit" of an unconstitutional search. We reject the government's invitation to allow police officers to rely on a diffuse notion of the weight of authority around the country, especially where that amorphous opinion turns out to be incorrect in the Supreme Court's eyes. Here, as Martin points out in his supplemental brief, there was no binding appellate precedent in the Eighth Circuit at the time that Iowa law enforcement officials attached the GPS device to Martin's car.

712 F.3d 1080, 1082 (7th Cir. 2013); see also United States v. Berrios, 990 F.3d 528, 532 (7th Cir. 2021) ("We acknowledged the distinction between established law and unsettled law in our decisions in United States v. Martin, 712 F.3d 1080 (7th Cir. 2013), and United States v. Jenkins, 850 F.3d 912 (7th Cir. 2017), where we declined to apply Davis to 'mistaken efforts to extend controlling precedents.' 712 F.3d at 1082; 850 F.3d at 920."); United States v. Correa, No. 11 CR 0750, 2015 U.S. Dist. LEXIS 6978, at *8 (N.D. Ill. Jan. 21, 2015) ("The Seventh Circuit adopted Justice Sotomayor's limiting principle in United States v. Martin, 712 F.3d 1080, 1082 (7th Cir. 2013)."). However, the quoted discussion above could be deemed dicta, as the Matthew Martin court went on to deny suppression on other grounds. 712 F.3d at 1082 ("We need not definitively resolve this point . . . because [the] evidence he seeks to suppress had little to do with the fact that a GPS device had been used[.]").

In United States v. Brown, 744 F.3d 474, 477-78 (7th Cir. 2014), also a GPS monitoring case, the Seventh Circuit declined to suppress evidence gathered in 2006, before the court had issued its decision in Garcia, holding that Knotts and Karo were "binding appellate precedent" for purposes of Davis. The court continued:

> There is legitimate debate about whether precedent from Circuit A could be deemed "binding" (for the purpose of Davis) when the search occurs in Circuit B, where the issue remains unresolved. Still, police and the FBI (or the lawyers advising them) often rely on precedent from one circuit when another has yet to address a question. One can doubt that much deterrence is to be had from telling the police that they are not entitled to rely on decisions issued by several circuits, just because the circuit covering the state in which an investigation is ongoing lacks its own precedent. If the question were whether police who installed a GPS locator, in reliance on Circuit A's precedent, could be ordered to pay damages when, years later, Circuit B disagreed with Circuit A, the answer would be no. It's hard to see why the exclusionary rule should be handled differently. But that's a question for another day.

Id. at 478. This discussion, too, is dicta. See United States v. Diggs, 385 F. Supp. 3d 648, 659 (N.D. Ill. 2019) (citing Brown and Matthew Martin, and noting the "Seventh Circuit has not definitively resolved whether decisions from other circuits can be 'binding appellate precedent' for purposes of the Davis good-faith exception").

Most recently, in United States v. Walker, 143 F.4th 889, 900 (7th Cir. 2025), the Seventh Circuit declined to apply good faith to a protective sweep during which police looked between a mattress and box spring, finding a gun, despite what the government called an "abundance of nonbinding cases holding that where officers have reason to believe other persons are present, they may conduct a protective sweep that includes checking under mattresses." The court explained:

> We note that the government does not cite any Seventh Circuit case holding that the good-faith exception applies when an officer's conduct is in line with non-binding caselaw. But even assuming an "abundance" of non-binding caselaw warrants applying the good-faith exception, there was no such abundance of non-binding caselaw to support the search here.

Id.[6]

[6]While several courts had upheld such searches where the police had reason to believe a person could be hiding under the bed, other courts had declined to find reasonable searches underneath mattresses where the police lacked such belief. Id. at 898-99.

The magistrate judge applied the broader version of good faith in this case:

> Where the law is unsettled, the police conduct generally must be "'deliberate, reckless, or grossly negligent' [in order] to warrant application of the exclusionary rule." United States v. [Richard] Martin, 807 F.3d 842, 847 (7th Cir. 2015) (quoting Davis, 564 U.S. at 238). "But when the police act with an objectively 'reasonable good-faith belief' that their conduct is lawful, … or when their conduct involves only simple, 'isolated' negligence, … the 'deterrence rationale loses much of its force,' and exclusion cannot 'pay its way[.]'" Davis, 564 U.S. at 238 (citations omitted) (quoting United States v. Leon, 468 U.S. 897, 909, 908 n.6 (1984), and Herring v. United States, 555 U.S. 135, 137 (2009)).

(R. 39 at 11-12; see also R. 39 at 12, stating that Koehler's conduct was not "reckless or grossly negligent".)

In his objections, defendant argues this application vastly expands the good faith doctrine. He further notes that the law in Richard Martin was not "unsettled," as the Seventh Circuit had (at that time) approved of warrantless GPS tracking. Defendant concludes that good faith should apply only if binding authority explicitly authorizes the warrantless search at issue. (R. 44 at 4.)

The government counters that it was objectively reasonable for Koehler to conclude that the Supreme Court's binding precedent in Jacobsen permitted him to view the images, consistent with the views of the Fifth and Sixth Circuits, particularly since no circuit had (at that time) held otherwise. (R. 46 at 4-5.) The government further contends that Koehler's decision to consult a state prosecutor and then seek a warrant provides additional evidence of good faith. (R. 27 at 16; R. 46 at 5-6.)

The government fails to demonstrate that the good faith exception applies here. See Walker, 143 F.4th at 900 ("The government fails to carry its burden of showing that officers acted in objective good faith when lifting the mattress in Walker Jr.'s bedroom.") (citing United States v. Matthews, 12 F.4th 647, 653 (7th Cir. 2021)). Applying a strict interpretation of Davis,

the government points to no binding appellate precedent specifically authorizing this particular police practice. As noted, the Seventh Circuit has not addressed the issue. Nor can the Supreme Court's private search cases be considered the applicable binding appellate precedent. While it is true two circuits, the Fifth and Sixth, extended Jacobsen to this context, it is important to note that they did not rely on the same reasoning, as discussed above. More importantly, Walter is the more analogous Supreme Court precedent, as also discussed.

Even under the more general test, good faith does not apply. Perhaps in some cases an officer could rely on an unbroken string of out-of-circuit decisions, but here there was no such consensus. While the Fifth and Sixth Circuits supported the search, they relied on different theories, as discussed above. Further, dicta in the Tenth Circuit's decision in Ackerman suggested a contrary result:

> Yes, AOL ran a search that suggested a hash value match between one attachment to Mr. Ackerman's email and an image AOL employees had previously identified as child pornography. But AOL never opened the email itself. Only NCMEC did that, and in at least this way exceeded rather than repeated AOL's private search.

831 F.3d at 1305-06 (Gorsuch, J.).[7] At the very least, Ackerman shows the issue was unsettled.

As the government notes, courts have held that an officer's decision to seek a warrant creates a presumption that he acted in good faith. See, e.g., United States v. Yarber, 915 F.3d 1103, 1106 (7th Cir. 2019); United States v. Orozco, 576 F.3d 745, 750 (7th Cir. 2009). However, these are cases in which the reviewing court determined a warrant application failed to establish probable cause; they do not involve the scenario here, where a warrant is obtained based in part on illegally obtained evidence. See United States v. Oakley, 944 F.2d 384, 386

[7]Recall that in Ackerman the court held the NCMEC qualified as a government entity to which the Fourth Amendment applied.

(7th Cir. 1991) ("[E]vidence discovered pursuant to a warrant will be inadmissible if the warrant was secured from a judicial officer through the use of illegally acquired information."). It may be objectively reasonable for an officer to rely on the opinion of a reviewing prosecutor or the determination of the issuing court that probable cause exists. However, it cannot be presumed that the prosecutor or the court will have passed on the legality of antecedent police actions used to gather evidence for the warrant application.

Finally, there are good reasons for declining to extend Davis to this context. One could argue that no official misconduct will be deterred when unbroken precedent authorizes the search. But when the law is unsettled, officers should be encouraged to err on the side of obtaining a warrant, particularly where, as here, there is no exigency. As defendant notes (R. 37 at 8-9), it would have been easy for Koehler to obtain a warrant before viewing the images, but he decided not to do so. See United States v. Banks, 60 F.4th 386, 391 (7th Cir. 2023) (declining to apply good faith based on a previous Seventh Circuit decision upholding a similar search on different legal grounds, and stressing that the police could have avoided suppression by taking the "small but necessary step" of obtaining a search warrant).

III. CONCLUSION

THEREFORE, IT IS ORDERED that defendant's motion to suppress (R. 20) is granted.

IT IS FURTHER ORDERED that this matter is scheduled for telephonic status on **Monday, September 15, 2025, at 10:30 a.m.**

Dated at Milwaukee, Wisconsin, this 3rd day of September, 2025.

/s/ Lynn Adelman
LYNN ADELMAN
District Judge