UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
NORTHERN DIVISION
COVINGTON

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	Criminal Case No. 16-47-ART-CJS
	)	
v.	)	
	)	**REPORT AND RECOMMENDATION**
WILLIAM MILLER,	)	
	)	
Defendant.	)	

*** *** *** ***

This matter is before the Court on the Defendant's Motion to Suppress. (R. 27). The Government has filed its Response, to which Defendant filed a Reply. (R. 33; R.37). The Motions have been referred to the undersigned for preparation of a Report and Recommendation pursuant to 28 U.S.C. § 636(b)(1)(B). (*See* R. 6). While Defendant requested an evidentiary hearing in his Motion filing, he withdrew that request in his Reply and instead requested the Court set the matter for oral argument. (*See* R. 27, at 11; R. 37, at 1). The Court heard oral argument on the Motion (*see* R. 38; R. 39), and the matter is now ripe for consideration. For the reasons set forth below, it will be recommended that Defendant's Motion to Suppress be **denied**.

I. Factual Background

On July 9, 2015, an individual using Google email (Gmail) account miller694u@gmail.com uploaded two images of apparent child pornography to an email, which may or may not have been sent. (R. 33-2, at 3-4). Google was alerted to these images through use of its proprietary "hashing" technology. (R. 33-1, at 1-2, 4-10 ¶¶ 4-8, 10-13). A representative from Google explains:

> 4. . . . [S]ince 2008, Google has been using its own proprietary hashing technology to tag confirmed child sexual abuse images. Each offending

> image, after it is viewed by at least one Google employee, is given a digital fingerprint ("hash") that our computers can automatically recognize and is added to our repository of hashes of apparent child pornography as defined in 18 U.S.C. § 2256. Comparing these hashes to hashes of content uploaded to our services allows us to identify duplicate images of apparent child pornography to prevent them from continuing to circulate on our products.
>
> 5. We also rely on users who flag suspicious content they encounter so we can review it and help expand our database of illegal images. No hash is added to our repository without the corresponding image first having been visually confirmed by a Google employee to be apparent child pornography.
>
> . . .
>
> 7. When Google's product abuse detection system encounters a hash that matches a hash of a known child sexual abuse image, in some cases Google automatically reports the user to [the National Center for Missing and Exploited Children] NCMEC without re-viewing the image. In other cases, Google undertakes a manual, human review, to confirm that the image contains apparent child pornography before reporting it to NCMEC.
>
> 8. When Google discovers apparent child pornography, Google files a report with . . . NCMEC in the form of a CyberTip. . . .

(R. 33-1, at 1 ¶¶ 4-8).[1]

Here, the parties do not dispute that Google's product abuse detection system hit on two images attached to an email in Defendant's Gmail account that matched hash values in Google's repository of hashes of apparent child pornography. (R. 27, at 1-2; R. 33, at 1-3; R. 33-1, at 2, ¶¶ 10, 11; R. 37, at 2-3). In response, Google submitted an "automatic report" to NCMEC–which Google is required to do by law, via a CyberTipline report.[2] (R. 33-1, at 1-2 ¶¶ 7, 8, 10; R. 33-2, at 3).

[1]In his Motion to Suppress Defendant stated he believed NCMEC provided Google with the hash values to use in its searching process. However, during oral argument counsel withdrew this statement, acknowledging the Affidavit of the Google executive explained that was not the case in this circumstance. (*See* R. 33-1, at ¶ 9).

[2]Google's Senior Manager of Law Enforcement and Information Security stated that "[w]hen Google's product abuse detection system encounters a hash that matches a hash of a known child sexual abuse image, in some cases Google automatically reports the user to NCMEC without a manual re-review of the image. (R. 33-1, at 1-2, ¶ 7). Here, the report states it is an "automatic report." (R. 33-2, at 3).

Google's employees did not manually view the content of the email or the images prior to submitting the report to NCMEC. (R. 33-1, at ¶¶ 10-11). The CyberTipline report did not contain the content of the email or header information, but did include the email address used, the IP address associated with the email in question, classification of the images,[3] the file names listed with the images and the two uploaded image files. (R. 33-1, at ¶¶ 10-11; R. 33-2, at 1-5; R. 33-6, at 4 ¶ 14). In addition, on or about the time it submitted the CyberTipline report, Google disabled the associated Gmail account. (R. 33-1, at ¶¶ 10-11).

When NCMEC received the CyberTipline report, its staff did not open or view the two uploaded files contained in the report. (R. 33-6, at 4 ¶ 15). Instead, a member of NCMEC's staff queried publicly-available sources related to the "miller694u@gmail.com" email address and located publicly-available social network profiles associated with that account. (*Id*.). NCMEC also verified the IP address reported by Google and learned it appeared to be associated with a Time Warner Cable account having a potential geographic location of Fort Mitchell, Kentucky. (*Id*. at ¶ 16). NCMEC, either by automated processes or its staff, provided the information in Sections B and C of the CyberTipline report and specifically noted in the report: "[p]lease be advised that NCMEC has not opened or viewed any uploaded files submitted with this report and has no information concerning the content of the uploaded files other than information provided in the report by the ESP [electronic service provider]." (*Id*. at ¶¶ 16-17; R. 33-2, at 8). NCMEC made the CyberTipline report available to Kentucky State Police and the Kenton County Police Department. (R. 33-6, at ¶¶ 16, 17).

---

[3]The CyberTipline report noted the images had been classified as A1 under the industry classification system, which indicates that the content of the associated image contained a depiction of a prepubescent minor engaged in a sexual act. (R. 33-1, at 2 ¶ 10; R. 33-2, at 4).

On August 13, 2015, Detective Aaron Schihl of the Kenton County Police Department received this CyberTipline report from NCMEC. (R 33-3, at 1). Detective Schihl opened the attachments and viewed the images, which he confirmed to be child pornography. (*Id*. at 1-2). Detective Schihl requested a grand jury subpoena for the subscriber information for the Time Warner Cable account associated with the IP address provided in the report. (*Id*. at 1). Time Warner responded to the request, identifying Tania Miller of 2271 Mercury Street, Fort Mitchell, Kentucky, 41017 as the subscriber for the requested IP address and provided contact information for the account. (*Id*.). Detective Schihl sought and obtained a search warrant for the contents of the miller694u@gmail.com account. (R. 33-3). In his Affidavit, Detective Schihl states he received a CyberTipline report, he provides the information learned regarding the IP and email addresses, and he describes the images based on his review of them. (R. 33-3, at 1-2). After review of the contents of the Gmail account, Detective Schihl obtained a search warrant for Defendant's home, followed by a search warrant for the electronic devices seized from Defendant's home. (R. 33-4; R. 33-5). The fruits of these three searches yielded additional evidence of the receipt, possession, and distribution of child pornography. (*See* R. 33-3; R. 33-4; R. 33-5). Defendant seeks to suppress all evidence obtained in this case.

II. Analysis

The Fourth Amendment provides in relevant part that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV. Fourth Amendment protections attach when a "search" occurs. A "search" occurs when the government infringes on an expectation of privacy that society is prepared to consider reasonable, *see United States v. Jacobsen*, 466 U.S. 109, 115 (1984), or where

the government physically intrudes on a constitutionally protected area for the purpose of obtaining information, *see United States v. Jones*, 565 U.S. 400, 407-08 (2012). Fourth Amendment protections do not apply to a private search. *Jacobsen*, 466 U.S. at 113. Nor do they apply if the government merely replicates a prior private search. *Id*. at 115.

In the pending Motion, Defendant challenges two warrantless searches as having violated his Fourth Amendment rights against unreasonable searches and seizures. He first contends that Google's use of its hashing technology to search his email account without a warrant constituted a search implicating the Fourth Amendment because Google acted as a state actor in conducting the search. Defendant also challenges Detective Schihl's actions of opening and viewing the attachments to his email, which he argues no one had previously opened and viewed, without first obtaining a warrant. For the reasons discussed below, Defendant's challenges to these searches fail.

A. Google is not a government actor

Defendant challenges Google's conduct of searching his email account for child pornography by utilizing hashing technology and then seizing two images attached to an unsent email. (R. 27, at 3-7). The Sixth Circuit has held that a person has a reasonable expectation of privacy in the content of his emails. *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010). The Fourth Amendment, however, applies only to government action and does not constrain private parties "not acting as an agent of the Government or with the participation or knowledge of any governmental official." *Jacobsen*, 466 U.S. at 113 (quoting *Walter v. United States*, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting)). Defendant argues that because of Google's nexus with NCMEC, an entity Defendant argues qualifies as a state actor, Google is also a state actor for purposes of the Fourth Amendment. (R. 27, at 5-6).

Defendant acknowledges that the Sixth Circuit has yet to consider whether NCMEC is a state actor. However, he notes that the Tenth Circuit has recently considered the issue and found that it is. *See United States v. Ackerman*, 831 F.3d 1292, 1296 (10th Cir. 2016) (finding NCMEC to be a governmental entity and an agent of the government). For purposes of this Motion, the Court will assume without deciding that NCMEC is a governmental entity or an agent of the Government such that the Fourth Amendment applies to its searches.

In his Motion, Defendant argues Google's conduct of searching his email account implicates the Fourth Amendment because there is a sufficiently close nexus between NCMEC and Google's search such that Google's conduct is fairly treated as that of NCMEC. (R. 27, at 5-6) (citing *Lansing v. City of Memphis*, 202 F.3d 821, 830 (6th Cir. 2000)). He also argues that Google is a government actor because it is a willful participant in NCMEC's policy of searching for and finding child pornography. (*Id*.).

To support his argument, Defendant points to statutory reporting requirements that require Google to report child pornography to NCMEC and preserve the suspected file or be subject to significant monetary penalties for failing to adhere to the reporting requirements. (R. 27, at 6) (citing 18 U.S.C. § 2258A). Defendant also argues that while Google is not statutorily required to search its products for child pornography, it presumably does so because of its relationship with NCMEC. Specifically, Defendant explains that Google and NCMEC are "entwined based on shared governmental policies and their combined actions reflect a joint effort and commitment to work together" to combat child pornography. (*Id.* at 7).

As the parties acknowledge, the Sixth Circuit has not yet addressed the issue of whether ESPs, such as Google, act as an agent of the government when they scan files on their network for

child pornography and, pursuant to the reporting requirement contained in 18 U.S.C. § 2258A, report findings of apparent child pornography to NCMEC. However, the cases that have considered the issue have uniformly held that such conduct does not transform an ESP into a government actor. *See United States v. Stevenson*, 727 F.3d 826, 831 (8th Cir. 2013) ("A reporting requirement, standing alone, does not transform an [i]nternet service provider into a government agent whenever it chooses to scan files sent on its network for child pornography."); *United States v. Cameron,* 699 F.3d 621, 638 (1st Cir. 2012) (finding Yahoo! was not acting as an agent of the government in conducting a search of defendant's account and reporting its findings to NCMEC, stating "if Yahoo! chose to implement a policy of searching for child pornography, it presumably did so for its own interests."); *United States v. Richardson*, 607 F.3d 357, 366 (4th Cir. 2010) (holding that AOL's scanning of email communications for child pornography and reporting discoveries to NCMEC did not trigger the Fourth Amendment's warrant requirement because no law enforcement officer or agency asked the provider to search or scan the defendant's emails); *United States v. Stratton*, No. 15-40084, 2017 WL 169041, at **4-5 (D. Kan. Jan. 7, 2017) (finding Sony was not acting as government agent when it monitored its users' accounts for child pornography because it was acting to protect its own interest in providing a safe online gaming community); *United States v. Miller*, No. 8:15-cr-172, 2015 WL 5824024, at *4 (D. Neb. Oct. 6, 2015) ("Google did not become a state actor by providing the reports required by law."); *United States v. Keith*, 980 F. Supp. 2d 33, 44 (D. Mass. 2013) (finding AOL, motivated by its own wholly private interests in monitoring emails for child pornography, was not acting as a government agent in searching its network for child pornography and reporting any findings to NCMEC). In fact, defense counsel stated during oral argument that

his research revealed no authority, either in this circuit or elsewhere, where an ESP has been held to be a government actor in a similar circumstance.

While Defendant argues Google is a state actor because of its nexus relationship to NCMEC, the Sixth Circuit has explained the appropriate considerations when determining whether a private party is acting as an agent of the government in conducting a search such that the Fourth Amendment is implicated:

> [A] private party's search is attributable to the government only "if the private party acted as an instrument or agent of the Government." *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 614, 109 S. Ct. 1402, 103 L. Ed.2d 639 (1989); *see, e.g., United States v. Clutter*, 914 F.2d 775, 778 (6th Cir. 1990). That "necessarily turns on the degree of the Government's participation in the private party's activities." *Skinner*, 489 U.S. at 614, 109 S. Ct. 1402. In the context of a search, the defendant must demonstrate two facts: (1) Law enforcement "instigated, encouraged or participated in the search" and (2) the individual "engaged in the search with the intent of assisting the police in their investigative efforts." *United States v. Hardin*, 539 F.3d 404, 419 (6th Cir. 2008) (quoting *United States v. Lambert*, 771 F.2d 83, 89 (6th Cir. 1985)).

United States v. Shepherd, 646 F. App'x 385, 388 (6th Cir. 2016); *see also United States v. Bowers*, 594 F.3d 522, 525-26 (6th Cir. 2010) ("in determining whether a private party is acting as an agent of the government such that the Fourth Amendment applies" the Sixth Circuit uses a two-factor analysis: "(1) the government's knowledge or acquiescence to the search, and (2) the intent of the party performing the search.") (quoting *Hardin*, 539 F.3d at 418) (internal quotations omitted). "If 'the intent of the private party conducting the search is entirely independent of the government's intent to collect evidence for use in a criminal prosecution,' then 'the private party is not an agent of the government.'" *Bowers*, 594 F.3d at 526 (quoting *Hardin*, 539 F.3d at 418 (internal quotation marks and emphasis omitted)).

Defendant's argument that Google's reporting obligations under 18 U.S.C. § 2258A render Google an agent of NCMEC is not persuasive. As Defendant acknowledges, § 2258A does not require Google to search for child pornography. In fact, the statute specifically states that it does not impose such a requirement: "[n]othing in this section shall be construed to require an electronic communication service provider . . . to – (1) monitor any user, subscriber, or customer of that provider; (2) monitor the content of any communication of any person described in paragraph (1); or (3) affirmatively seek facts or circumstances described in sections (a) and (b)." 18 U.S.C. § 2258A(f). Instead, the statute merely requires that when an ESP discovers apparent child pornography, it comply with its reporting requirements. Thus, Defendant's pointing to the statute does not establish that Google conducted its search because of any directive or encouragement by the government.

Further, while the Sixth Circuit has not addressed the specific issue at hand, several other circuit courts have considered the issue and have consistently held that the reporting requirement set forth in 18 U.S.C. § 2258A, or its predecessor statute, "does not transform an [i]nternet service provider into a government agent whenever it chooses to scan files sent on its network for child pornography." *Stevenson*, 727 F.3d at 829-30; *see also Cameron*, 699 F.3d at 637-38 (rejecting argument that statutory reporting obligations demonstrated government control over Yahoo!, stating "the statute did not impose any obligation to *search* for child pornography, merely an obligation to *report* child pornography of which Yahoo! became aware") (emphasis original); *Richardson*, 607 F.3d at 367 (distinguishing the reporting scheme in *Skinner*, noting nothing in the statute requires the electronic communication services to actively seek evidence of child pornography nor prescribes the procedures for doing so). These persuasive authorities support the conclusion in this case that

Google's obligation to report known facts or circumstances of apparent child pornography to NCMEC does not transform Google's voluntary decision to use its own proprietary hashing technology to search its products for child pornography into conduct of a government actor where the statute does not impose a duty to conduct a search.

Nor does the Court find merit in Defendant's argument that Google's willful participation in NCMEC's policy of searching for and finding child pornography demonstrates Google was acting as a government actor. The question of whether Google served as an agent of the government in performing its search of Defendant's email account for hash value matches "necessarily turns on the degree of the Government's participation in [Google's] activities." *Shepherd*, 646 F. App'x at 388 (quoting *Skinner*, 489 U.S. at 614).

Here, Defendant has not presented any evidence that NCMEC or law enforcement "instigated, encouraged or participated in the search" of Defendant's Gmail account. *Shepherd*, 646 F. App'x at 388. Defendant does not contend that NCMEC or law enforcement asked Google to perform the search of his emails or that either had any role in instigating or participating in the search. Even assuming NCMEC may have been aware that Google routinely monitors its platforms for illegal usage, and submits reports of any illegal activity found, there is no evidence that NCMEC or law enforcement compelled or encouraged Google to routinely monitor its platforms. Nor does Defendant present evidence to suggest that NCMEC or law enforcement were aware of the existence of Defendant or the miller694u@gmail.com account prior to Google's search in this case. *Cameron,* 699 F.3d at 638 (finding no evidence that the government instigated the search, participated in the search, or coerced the ESP to conduct the search at issue).

In fact, the Affidavit of Cathy A. McGoff, Google's Senior Manager of Law Enforcement and Information Security, provides that Google has no records to suggest, prior to submitting the CyberTipline report, that Google was aware of any law enforcement investigation pertaining to the user associated with the report. (R. 33-1, at 2 ¶ 12). Thus, evidence in the record does not establish that NCMEC or law enforcement "instigated, encouraged or participated" in Google's search.

Nor is there evidence that Google "engaged in the search with the intent of assisting the [government] in their investigative efforts." *Shepherd*, 646 F. App'x at 388. Other than referencing the statute requiring Google to report (but not search for) discoveries of child pornography to NCMEC, the only other evidence Defendant points to as suggesting a relationship between Google, NCMEC and/or law enforcement are website citations to a number of articles on Google's website and blog. (R. 27, at 6 n.3). In these articles, Google expresses its commitment to protecting children online, discusses its goal of finding, removing and reporting child pornography on its products, and discusses its involvement/collaboration with other "tech industry companies" and NCMEC to combat child pornography by participating in various coalitions and programs. (*Id.*). While Defendant argues this evidence demonstrates Google is collaborating with NCMEC and has "made itself a willful participant in NCMEC's policy of searching out and finding child pornography," these articles only establish that Google and NCMEC have a shared goal of eradicating the online sharing of child pornography. "Sharing a goal with the Government is insufficient to transform [an ESP] from a private actor into a Government agent." *United States v. Stevenson*, No. 3:12-cr-5, 2012 WL 12895560, at *3 (S.D. Iowa June 20, 2012), *affirmed,* 727 F.3d 825 (8th Cir. 2013).

Here, as in *Stevenson*, Defendant has offered no evidence that the Government, through NCMEC or law enforcement, participated in or encouraged Google's search of Defendant's email

account. In fact, there is no evidence that NCMEC or law enforcement were even aware of the search of Defendant's emails prior to their receipt of the CyberTipline report. Nor is there evidence Google performed the search for the purpose of assisting the Government in its investigative efforts. Instead, the Government provided the Affidavit of Ms. McGoff that explains Google's reasons for its decision to monitor its platform for child pornography:

> 3. Google has a strong business interest in enforcing our terms of service and ensuring that our products are free of illegal content, and in particular, child sexual abuse material. We independently and voluntarily take steps to monitor and safeguard our platform. If our product is associated with being a haven for abusive content and conduct, users will stop using our services. Ridding our products and services of child abuse images is critically important to protecting our users, our product, our brand, and our business interests.
>
> 4. Based on these private, non-government interests, since 2008, Google has been using its own proprietary hashing technology to tag confirmed child sexual abuse images. Each offending image, after it is viewed by at least one Google employee, is given a digital fingerprint ("hash") that our computers can automatically recognize and is added to our repository of hashes of apparent child pornography as defined in 18 U.S.C. § 2256. Comparing these hashes to hashes of content uploaded to our services allows us to identify duplicate images of apparent child pornography to prevent them from continuing to circulate on our products.

(R. 33-1, at 1 ¶¶ 3-4). This evidence demonstrates Google's actions in this case were motivated by business interests that are separate from a desire to assist law enforcement. (*Id.*). Other courts have found such evidence sufficient to demonstrate the ESP operated its file-scanning programs independently of the government, and thus were held not to have acted as agents of the government in operating their scanning programs. *Stevenson*, 727 F.3d at 830-31; *Cameron,* 699 F.3d at 638 (stating that the fact child pornography is a government interest does not mean that an ESP "cannot voluntarily choose to have the same interest").

Thus, the evidence before the Court in the present case demonstrates that Google was not acting as an agent of NCMEC or law enforcement, but as a private entity pursuing its own business interests. Therefore, Google's use of its hashing technology to search Defendant's email account did not implicate the Fourth Amendment.

B. Detective Schihl's actions did not exceed Google's private search

Defendant also argues that even if Google's search and seizure was not government action, Detective Schihl exceeded Google's private search by opening and viewing the email attachments and thereby violated his Fourth Amendment rights. This raises questions about the private search doctrine and the application of the doctrine to the circumstances here.

The private search doctrine permits a government agent to verify the illegality of evidence discovered during a private search provided the agent stays within the scope of the private search. *United States v. Lichtenberger*, 786 F.3d 478, 481-83 (6th Cir. 2015) (citing *Jacobsen*, 466 U.S. at 119-20). A government agent's invasion of a defendant's privacy "must be tested by the degree to which [the agent] exceeded the scope of the private search." *Jacobsen*, 466 U.S. at 115 (citing *Walter*, 447 U.S. 649); *Lichtenberger,* 786 F.3d at 482. The Supreme Court has explained that "[o]nce frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information." *Jacobsen*, 466 U.S. at 117.

The private search doctrine originates from the Supreme Court's decision in *Jacobsen*, 466 U.S. at 109. In *Jacobsen*, Federal Express ("FedEx") employees discovered a damaged package and proceeded to examine its contents, which was consistent with company policy involving insurance claims. *Jacobsen,* 466 U.S. at 111. The container itself was made of cardboard packaging, but inside of it were crumpled newspapers concealing a 10-inch tube made of silver duct tape. *Id.* The

employees proceeded to cut open the tube, and discovered four zip-lock bags filled with an unidentified white powder. *Id.* FedEx notified the Drug Enforcement Agency ("DEA") of their discovery, and placed the tube and its contents back in the cardboard container. *Id.* Upon arrival, a DEA agent discovered the partially opened container, and observed a slit in the duct tape tube. He then removed the zip-lock bags, took a sample from each, and field-tested it. The test positively identified the substance as cocaine. *Id.* at 112.

The Supreme Court analyzed whether the DEA agent's after-occurring warrantless search had exceeded the scope of the FedEx employees' initial private search of the package. The Court found that the agent's removal of the cocaine from the package remained within the scope of the private search because "there was a virtual certainty that nothing else of significance was in the package and that a manual inspection of the tube and its contents would not tell him anything more than he already had been told." *Id.* at 119. As for the chemical test, the Court held that the field test "could disclose only one fact previously unknown to the agent–whether or not a suspicious white powder was cocaine." *Id.* at 122. The Court concluded that no search occurred because the defendant did not have a legitimate expectation of privacy in whether the powder was contraband and the test could not disclose any other arguable private fact. *Id*. at 123-24.

Here, Defendant argues Detective Schihl exceeded Google's private search when he opened and viewed the email attachments because Google had not conducted a manual review of the two attached images before submitting them to NCMEC. (R. 33-1, at 2 ¶ 11). Instead, Google reported the attachments to NCMEC because its hashing technology indicated they were images that matched hash values of images its employees had previously viewed and found to be apparent child pornography. (R. 33-1, at 2 ¶¶ 4, 7, 10-11). NCMEC, without opening the attachments or otherwise

viewing the images, forwarded the CyberTipline report to law enforcement.[4] (R. 33-6, at 4 ¶15). It is undisputed that Detective Schihl was the first person to manually open and view the attachments to Defendant's email. (R. 33-3, at 2; R. 33-6, at 4 ¶ 15). Thus, Defendant argues that because Google did not manually open and view the attachments, Detective Schihl opened and viewed unopened virtual containers, i.e., the attachments, thereby exceeding the scope of Google's search.

The Sixth Circuit has explained that "[u]nder the private search doctrine, the critical measures of whether a governmental search exceeds the scope of the private search that preceded it are how much information the government stands to gain when it re-examines the evidence and, relatedly, how certain it is regarding what it will find." *Lichtenberger*, 786 F.3d at 485-86 (citing *Jacobsen*, 466 U.S. at 119-20). Thus, to determine whether the Fourth Amendment is implicated by Detective Schihl's opening and viewing of the attachments sent via the CyberTipline report, the Court must determine whether Detective Schihl was virtually certain that his "inspection of the [attachments] . . . would not tell [him] anything more than he already had been told [by Google via the CyberTipline report]." *Lichtenberger*, 786 F.3d at 488 (citing *Jacobsen*, 466 U.S. at 119).

Defendant looks to the Tenth Circuit's *Ackerman* decision to support his argument that Detective Schihl's conduct was unconstitutional. *Ackerman*, 831 F.3d at 1292. Defendant contends the facts here are analogous to those the *Ackerman* court found exceeded the ESP's private search. (R. 27, at 8). In *Ackerman*, the defendant sent an email containing child pornography. *Id*. at 1294.

---

[4]Defendant finds of import that the CyberTipline report noted that NCMEC had "no information concerning the content of the uploaded files other than information provided in the report by [Google]," and that NCMEC classified the files as "Child Pornography (Unconfirmed-Files Not Reviewed by NCMEC). (R. 27, at 10) (quoting R. 33-2, at 8). However, the fact that NCMEC did not review the image files reported by Google does not affect the Court's determination of whether Officer Schihl's actions fell within the scope of Google's private search.

But before the email reached its intended recipient, AOL's automated filter identified the email as containing one image that matched the hash value of an image an AOL employee had previously viewed and deemed to be child pornography. *Id*. AOL automatically stopped the email's delivery and without manually viewing the email or its attachments, it reported the email to NCMEC and provided the email and its four attachments (not just the one attachment containing the image AOL's filter found matched the hash value of a known image of child pornography). *Id*.

A NCMEC analyst opened the email, viewed each of the four attached images and confirmed all four images appeared to be child pornography. *Id*. In reaching its decision that NCMEC, a governmental entity or agent, had exceeded AOL's private search, the *Ackerman* court found of import that NCMEC opened and viewed information beyond the one image that was the target of AOL's hash value match. *Id*. at 1306. Notably, the *Ackerman* court asked, but left unresolved the following questions:

> What if NCMEC hadn't opened Mr. Ackerman's email but had somehow directly accessed (only) the (one) attached image with the matching hash value? Could the government have argued that, in that case, NCMEC's actions didn't risk exposing any private information beyond what AOL had already reported to it? Or might even that have risked exposing new and protected information, maybe because the hash value match could have proven mistaken (unlikely if not impossible) or because the AOL employee who identified the original image as child pornography was mistaken in his assessment (unlikely if maybe more possible)?

Id. at 1306 (citing Salgado, Fourth Amendment Search and the Power of the Hash, 119 Harv. L. Rev. F. 38, 38-40 (2005)). The court left these questions unresolved because it found the undisputed facts indicated that NCMEC exceeded AOL's private search when it opened the email as well as all four images, rather than solely viewing the one attachment that was the target of AOL's private search. The Court found that NCMEC's conduct of opening the email and viewing the three attachments that

had not been identified by AOL as having a hash value match "was enough to risk exposing private, noncontraband information that AOL had not previously examined." *Ackerman*, 831 F.3d 1306-07.

The facts of this case are distinguishable from *Ackerman*. Most significantly, there is no evidence or allegation that Google sent anything to NCMEC other than the files of the two images having a hash value match to two images Google's employees had previously identified as being apparent child pornography. (R. 33-1, at 2 ¶¶ 10, 11; R. 33-2, at 4-5). Thus, the reasoning of the *Ackerman* court in finding the search exceeded the scope of AOL's private search is not applicable. Instead, the issue is whether Detective Schihl's opening and viewing of the two attachments that Google's private search detected as matching the hash values of images previously identified as apparent child pornography risked exposing any private information beyond what Google had reported.

Defendant contends the answer to this inquiry is yes, and argues the circumstances at hand are similar to those in *Walter v. United States*, 447 U.S. 649 (1980). In *Walter*, a private mail carrier mistakenly delivered 12 packages containing 871 boxes of 8-millimeter film to the wrong address. *Id*. at 651. Employees of the company that received the packages opened them, finding the boxes of film. The boxes contained drawings and descriptions that alluded to the obscene content of the films. *Id.* at 652. One employee attempted to view portions of at least one film by holding it up to the light, but was unsuccessful. *Id.* Soon after, the employees contacted the FBI, and an agent picked up the packages. *Id.* The FBI agents–without obtaining a warrant–proceeded to screen the films through a projector. *Id.*

The Supreme Court did not issue a majority opinion in *Walter*.[5] Justice Stevens, joined by Justice Stewart, announced the judgment of the Court, and found that "the Government may not exceed the scope of the private search unless it has the right to make an independent search." *Id*. at 657. Justice Stevens found that despite the descriptive nature of the labels on the films' packaging, the private party had not actually viewed the films and "prior to the [g]overnment screening one could only draw inferences about what was on the films." *Id.* at 656-57. He thus concluded that the viewing of the films was a "significant expansion" of the private search, requiring it be characterized as a separate search. *Id.* at 657-59.

Here, Defendant Miller contends the hash values of the images Google located in its search are analogous to the descriptive labels on the films in *Walter.* Detective Schihl's conduct of opening and viewing the attachments, argues Miller, is akin to the FBI agents' unconstitutional conduct in *Walter* of viewing the films without a warrant. (R. 37, at 4). Defendant points to a decision of the United States District Court in the District of Massachusetts as supporting the comparison of the facts at hand to those in *Walter*. *See United States v. Keith*, 980 F. Supp. 2d 33 (D. Mass. 2013).

---

[5]While a majority opinion did not issue, five Justices agreed that the warrantless projection of the films constituted a search that infringed the defendant's Fourth Amendment interests. Justices Stevens and Stewart found that the officers had violated the Fourth Amendment because they exceeded the scope of the private search. *Walter*, 447 U.S. at 653-60. However, Justice White, with whom Justice Brennan joined, wrote separately stating that even if there had been a private screening of the films, the agents still needed a warrant because the private search would not have exposed the content of the films to plain view. Justice Marshall concurred in the judgment without discussion.

Justices Blackmun, with whom Chief Justice Burger, Justice Powell and Justice Rehnquist joined, dissented in the judgment, but agreed the legality of the government's actions must be tested by the scope of the private search that preceded them. *See Jacobsen*, 466 U.S. at 115-16 (discussing the various opinions in *Walter*). Justice Blackmun explained that because the private search in *Walter* exposed the labels describing the nature of the films, there was no remaining expectation of privacy in the contents of the films. He found the subsequent viewing of the films by the agents did not "change the nature of the search," and therefore their viewing did not constitute an additional search subject to the warrant requirement. *Walter*, 447 U.S. at 663-64.

In *Keith*, AOL was alerted to an email on its system containing a file that had a positive hash value match to an image AOL had previously determined to be child pornography. *Keith,* 980 F. Supp. 2d at 37. Much like Google, AOL maintains a database of hash values that is "essentially a catalog of files that have previously been identified as containing child pornography." *Id.* at 36. Upon detecting a hash value match in defendant's email, AOL forwarded the file (unopened) to NCMEC via the CyberTipline. *Id.* A NCMEC analyst opened and inspected the file and determined it contained child pornography. The file was then forwarded to local law enforcement. *Id.*

The defendant in *Keith* moved to suppress this evidence, arguing that by opening and viewing the image NCMEC exceeded AOL's private search.[6] *Id*. The district court agreed, finding that the hash value provided by AOL, much like the labels on the films in *Walter*, likely would have furnished the requisite probable cause for a warrant, but did not justify viewing the contents without a warrant. The court also distinguished *Jacobsen*, 466 U.S. at 109, stating it is "indisputable that AOL forwarded the suspect file only because its hash value matched a stored hash value, not because some AOL employee had opened the file and viewed the contents." *Keith*, 980 F. Supp. 2d at 42-43. The court found *Walter*, not *Jacobsen*, was the better analog to the facts of its case. *Id*. at 43. The court further stated:

> In this regard it is worth noting that matching the hash value of a file to a stored hash value is not the virtual equivalent of viewing the contents of the file. What the match says is that the two files are identical; it does not itself convey any information about the contents of the file. It does say that the suspect file is identical to a file that someone, sometime, identified as containing child pornography, but the provenance

[6]Defendant also argued that both AOL and NCMEC were acting as government agents under the circumstances, and thus their searches violated his Fourth Amendment rights. *Keith*, 980 F. Supp. 2d at 39. The district court dismissed the notion that AOL had a sufficient enough connection with the government to be treated as a government actor, but held NCMEC to be an agent of the government and subject to Fourth Amendment constraints. *Id*. at 40-42.

> of that designation is unknown. So a match alone indicts a file as contraband but cannot alone convict it. That is surely why a CyberTipline analyst opens the file to view it, because the actual viewing of the contents provides information additional to the information provided by the hash match. This is unlike what the Court found the case to be in *Jacobsen*, where the subsequent DEA search provided no more information than had already been exposed by the initial FedEx search. *Jacobsen* is inapposite.

Id. Thus, the court found that by opening the previously unopened email image file, NCMEC exceeded the scope of the private search. *Id*.

Defendant Miller's reliance upon the *Keith* court's rejection of *Jacobsen* and acceptance of *Walters* to the circumstances in that case raises additional questions for this Court. In applying the Supreme Court's holding in *Jacobsen*, the Sixth Circuit has explained that the relevant inquiry for determining if government action exceeds the scope of a private search is to determine how much information the government stood to gain when it conducted the search and, relatedly, how certain it was regarding what it would find. *Lichtenberger,* 786 F.3d at 485-86 ("We have held a government search permissible–that is, properly limited in scope–in instances involving physical containers and spaces on the grounds that the officers in question had near-certainty regarding what they would find and little chance to see much other than contraband");[7] *Bowers*, 594 F.3d at 526 ("based on [defendant's roommate's] statements that the album contained child pornography, the agents were justified in opening the album to view the potentially incriminating evidence. . . . In doing so, the agents 'learn[ed] nothing that had not previously been learned during the private search' and 'infringed no legitimate expectation of privacy.'") (quoting *Jacobsen*, 466 U.S. at 120);

[7]The *Lichtenberger* court further explained that when the item searched is an electronic device, the privacy interests at stake are increased because of the amount of information that is stored in such devices. *Lichtenberger,* 786 F.3d at 488. The court found that given the amount of data that can be stored in a laptop, "'there was absolutely no virtual certainty that the search of [defendant's] laptop would have' revealed only what Officer Huston had already been told." *Id*.

United States v. Richards, 301 F. App'x 480, 483 (6th Cir. 2008) ("the government's confirmation of prior knowledge learned by the private individuals does not constitute exceeding the scope of a private search.").

Importantly, Defendant Miller does not question the reliability of hashing technology, and it appears well established that it is, in fact, reliable. *Ackerman* contains language, albeit *in dicta,* indicating the reliability of hash value matching, stating it is "unlikely if not impossible" that a hash value match could have proven a mistake. *Ackerman,* 831 F.3d at 1306 (citing Salgado, Fourth Amendment Search and the Power of the Hash, 119 Harv. L. Rev. F. 38, 45-46 (2005)). In *Ackerman*, the court explained hash values as "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. Some consider a hash value as a sort of digital fingerprint." *Id*. at 1294.

In addition, other courts, including our own, have found hash values to be highly reliable–akin to the reliability of DNA. *See United States v. Dunning*, No. 7:15-04-DCR, 2015 WL 5999818, at *3 (E.D. Ky. Oct. 15, 2015) (noting in a probable cause analysis that "as Magistrate Judge Atkins observed, hash values 'boast a reliability and accuracy akin to DNA: 99.99%.'") (citing *United States v. Wellman*, 663 F.3d 224, 226 n.2 (4th Cir. 2011) (also citing the 99.99% probability statistic); *see also United States v. Cartier*, 543 F.3d 442, 446 (8th Cir. 2008)). The Federal Judicial Center, in a guide for federal judges, has defined "hash value" as follows:

> hash value: A unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. The most commonly used algorithms, known as MD5 and SHA, will generate numerical values so distinctive that the chance that any two data sets will have the same hash value, no matter how similar they appear, is less

> than one in one billion. "Hashing" is used to guarantee the authenticity of an original data set and can be used as a digital equivalent of the Bates stamp used in paper document production.

Barbara J. Rothstein et al., Managing Discovery of Electronic Information: A Pocket Guide for Judges 24 (Federal Judicial Center 2007).

Even the court in *Keith* acknowledges the reliability of hashing technology, explaining:

> A hash value is an alphanumeric sequence that is unique to a specific digital file. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Consequently, once a file has been "hashed," a suspect copy can be determined to be identical to the original file if it has the same hash value as the original, and not to be identical if it has a different hash value.

Keith, 980 F. Supp. 2d at 36-37.

Given the function of the hash value, the *Keith* court's analogy of the hash value to the labels at issue in *Walter* seems misplaced. A label, such as those in *Walter,* is not mathematically derived, nor is it intended to have unique identification features that permit one to know with near certainty that a container containing the exact label will have identical contents to that of another containing the same label. Further, the content in labeled containers can be removed or altered without changing the label. A hash value, on the other hand, is derived from an algorithm and is a unique identifier that confirms that two digital files are the same or different (often discussed as being similar to a digital fingerprint or DNA). *See supra*. In addition, changes to the contents of a digital file will change the hash value. Thus, a label, such as those at issue in *Walter*, is not only created differently than a hash value, but serves an entirely different purpose.

Instead of merely describing what may be in the attachments, Google's search of the attachments using hashing technology revealed they contained images that were duplicates of images

a Google employee had previously identified as apparent child pornography. (R. 33-1, at 1 ¶ 4). Accordingly, when Detective Schihl opened and viewed the two images Google identified as matching the hash values of images it previously identified as apparent child pornography, he was virtually certain to view an exact duplicate of the original image and was merely confirming what Google had told him–that the attachments contained apparent child pornography. The virtual certainty that Detective Schihl would see only images of apparent child pornography is what distinguishes this case from *Walter*.

Similarly, *Lichtenberger* is also distinguishable on this basis. *Lichtenberger*, 786 F.3d 478 (6th Cir. 2015). In *Lichtenberger,* Defendant's girlfriend, without his permission, hacked into his laptop and found a number of images of child pornography. The girlfriend called the police and told them of the child pornography images she found. An officer came to the home and directed the girlfriend to access the laptop and open the files. She testified that she showed the officer a few pictures from the computer files she had found, but she was not sure if they were the same images she had seen in her original search. *Id.* at 481. The Sixth Circuit held the police officer's warrantless search of defendant's laptop computer exceeded the scope of defendant's girlfriend's search because it was not virtually certain that the officer's review would be limited to the images the girlfriend had previously viewed.[8] *Id.* at 485-88. Specifically, the court noted:

---

[8]*Bowers* also supports the Court's finding. *Bowers*, 594 F.3d at 524-26. In *Bowers*, the boyfriend of defendant's roommate discovered a photo album containing what he believed to be child pornography in the defendant's bedroom. *Bowers*, 594 F.3d at 524. When the summoned authorities arrived at the defendant's home, his roommate directed them to the dining room table where they had placed the album. The agents opened the album to view the potentially incriminating evidence. *Id*. at 524-25. The Sixth Circuit upheld the search of the photo album by agents because the roommate had already described the contents of the album. *Id*. at 526. The agents therefore knew the album contained child pornography, "learn[ed] nothing that had not previously been learned during the private search," and "infringed no legitimate expectation of privacy." *Id*. (quoting *Jacobsen*, 466 U.S. at 120) (internal quotation marks omitted).

> Considering the extent of information that can be stored on a laptop computer–a device with even greater capacity than the cell phones at issue in *Riley [v. California* __ U.S. __, 134 S. Ct. 2473 (2014)]–the "virtual certainty" threshold in *Jacobsen* requires more than was present here. When Office Huston arrived, he asked Holmes to show him what she had found. While the government emphasizes that she showed Officer Huston only a handful of photographs, Holmes admitted during testimony that she could not recall if these were among the same photographs she had seen earlier because there were hundreds of photographs in the folders she had accessed. And Officer Holmes himself admitted that he may have asked Holmes to open files other than those she had previously opened. As a result, not only was there no virtual certainty that Officer Huston's review was limited to the photographs from Holmes's earlier search, there was a very real possibility Officer Huston exceeded the scope of Holmes's search and that he could have discovered something else on Lichtenberger's laptop that was private, legal, and unrelated to the allegations prompting the search–precisely the sort of discovery the *Jacobsen* Court sought to avoid in articulating its beyond-the-scope test.
>
> All the photographs Holmes showed Officer Huston contained images of child pornography, but there was no virtual certainty that would be the case. The same folders–labeled with numbers, not words–could have contained, for example, explicit photos of Lichtenberger himself: legal, unrelated to the crime alleged, and the most private sort of images. Other documents, such as bank statements or personal communications, could also have been discovered among the photographs. So, too, could internet search histories containing anything from Lichtenberger's medical history to his choice of restaurant. The reality of modern data storage is that the possibilities are expansive.

Lichtenberger, 786 F.3d at 488-89.

Here, on the other hand, Defendant Miller does not dispute that only the two images Google's private search identified as matching previously tagged images of apparent child pornography were attached to the CyberTipline report. Thus, there was little to no possibility that Detective Schihl's review of the two image files would reveal other information beyond what the private search revealed–the two image files contained images of apparent child pornography.

Further, Defendant's argument that the "virtual certainty" language in *Jacobsen* is not applicable because Detective Schihl did not "re-examine" the attachments but rather opened "an

unopened virtual container" is not persuasive. (R. 37, at 2-6). The evidence establishes that Google used its digital or virtual eye to search the contents of Defendant's email account looking for images it had previously viewed and tagged as apparent child pornography. Once it located two images within Defendant's email account having hash values that matched images it had previously viewed and tagged as apparent child pornography, it knew from its electronic viewing or examination of the attachments that they contained apparent contraband. Accordingly, because hashing technology identifies files that are exact matches to images containing the same hash value, Google's private search of the attachments, using its digital or virtual eye, frustrated Defendant's expectation of privacy in those attachments. Simply put, Google's private search "compromised the integrity of the [attachments]." *Jacobsen*, 466 U.S. at 120 n.17. Therefore, contrary to Defendant's argument, the principles articulated in *Jacobsen* apply to determine whether Detective Schihl's actions exceeded the scope of Google's private search.

As discussed above, Detective Schihl's opening and viewing of the images Google's private search identified as having hash values that matched that of known images of apparent child pornography was virtually certain to reveal only the images Google previously viewed and tagged. As in *Jacobsen*, there was a virtual certainty that nothing else of significance except suspected contraband, i.e. apparent child pornography, would be found in the attachments, and a manual inspection of the attachments would reveal nothing more than what Google's private search revealed–the attachments contained apparent child pornography.[9] Therefore, Detective Schihl's

[9]As the Government notes, while the possibility exists that Google erred in its original determination that these images constituted child pornography, that possibility is no greater than any other circumstance where a private person reports apparent child pornography. *Cf. Bowers*, 594 F.3d at 526 ("based on the [roommate's] statements that the album contained child pornography, the agents were justified in opening the album to view the potentially incriminating evidence. . . . In doing so, the agents 'learn[ed] nothing that

opening and viewing of the attachments to confirm Google's report of apparent child pornography falls within the private search doctrine, and no Fourth Amendment violation occurred. *See Jacobsen*, 466 U.S. at 115; *Lichtenberger*, 786 F.3d at 485-86; *Bowers*, 594 F.3d at 524-26.[10]

III. Conclusion and Recommendation

Google's use of its hashing technology to search Defendant's email account does not implicate the Fourth Amendment because it was a private search. Further, Detective Schihl's actions of opening the email attachments did not exceed the scope of Google's private search because it was virtually certain his actions would reveal nothing more than already reported by Google–that the images were apparent child pornography.

Accordingly, **IT IS RECOMMENDED** that Defendant's Motion to Suppress (R. 27) be **DENIED.**

---

had not previously been learned during the private search' and 'infringed no legitimate expectation of privacy.'") (quoting *Jacobsen*, 466 U.S. at 120).

[10]Defendant also briefly argues in Reply that while the Government suggests Detective Schihl's opening of the two email attachments was not a physical trespass, his conduct does, in fact, constitute a search under the traditional trespass test. (R. 37, at 9) (citing *Ackerman*, 831 F.3d at 1308) (citing *United States v. Jones*, 565 U.S. 400 (2012)). Defendant specifically references the finding in *Ackerman* that NCMEC's opening of the email and its attachments in that case constituted a search under both the reasonable expectation of privacy test discussed by the Supreme Court in *Jacobsen*, *Walter* and *Katz v. United States*, 389 U.S. 347 (1967) and the traditional trespass test discussed in *Jones*. However, *Jones* and *Ackerman* are distinguishable from this case. *Jones* did not involve the application of the private search doctrine; and *Ackerman* involved a finding that the Government exceeded the scope of AOL's private search by opening the email and all four attachments, not just the one attachment with the hash value match. As discussed above, the Fourth Amendment only prohibits governmental action; it is inapplicable "to a search or 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." *Jacobsen*, 466 U.S. at 113 (quoting *Walter*, 447 U.S. at 662) (Blackmun, J., dissenting). Given the Court's finding that the private search doctrine is applicable to the case at bar and the lack of any appreciable development of a trespass argument by Defendant, this argument will not be considered further.

Specific objections to this Report and Recommendation must be filed within **fourteen (14) days** of the date of service or further appeal is waived. 28 U.S.C. § 636(b)(1)(C); Fed. R. Crim. P. 59(b)(2); *Thomas v. Arn*, 728 F.2d 813, 815 (6th Cir. 1984), *aff'd*, 474 U.S. 140 (1985); *United States v. Walters*, 638 F.2d 947 (6th Cir. 1981).

Dated this 19th day of May, 2017.

Signed By:
Candace J. Smith
United States Magistrate Judge

J:\DATA\Orders\criminal cov\2016\16-47-ART-CJS mtn to suppress R&R.wpd