UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
NORTHERN DIVISION
AT COVINGTON

CRIMINAL ACTION NO. 16-47-DLB-CJS

UNITED STATES OF AMERICA **PLAINTIFF**

vs. **MEMORANDUM ORDER ADOPTING REPORT AND RECOMMENDATION**

WILLIAM MILLER **DEFENDANT**

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

I. Introduction

This matter concerns the role of electronic service providers (ESPs) in identifying and reporting images of child pornography sent using their services and the constitutionality of law enforcement's subsequent review of those images. Defendant's Motion to Suppress two images of apparent child pornography attached to an email in his Google account is before the Court on the Report and Recommendation (R&R) of Magistrate Judge Candace J. Smith, who recommends that the Court deny the Motion. (Doc. # 41). Defendant has filed objections to the R&R (Doc. # 44), and the R&R and objections are now ripe for the Court's review. For the reasons that follow, the objections are **overruled**, and the motion to suppress is **denied**.

II. Factual Background

On July 9, 2015, someone using the Google email (Gmail) account miller694u@gmail.com uploaded two images as attachments to an email. (Doc. # 33-2 at 3-4). Google's product abuse detection system recognized those images as apparent child

pornography using its proprietary "hashing" technology. (Doc. # 33-1 at ¶¶ 4-8, 10-13). Hashing is "the process of taking an input data string [from an electronic image, for example] and using a mathematical function to generate a (usually smaller) output string." Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38, 38-39 (2005). The output string, called the hash value, is a "digital fingerprint" shared by any duplicate of the input data string. (Doc. # 33-1 at ¶ 4). Hashing is not unique to images of child pornography–the process can be used to derive hash values for many different kinds of data sets, "including the contents of a DVD, USB drive, or an entire hard drive." Salgado, *supra*, at 39. Importantly, hash values are uniquely associated with the input data, meaning that "if an unknown file has a hash value identical to that of another known file, then you know that the first file is the same as the second." *Id.* at 39-40; *see also* Doc. # 33-1 at ¶ 4.

Google has been using its proprietary hashing technology since 2008 to identify "confirmed child sexual abuse images." (Doc. # 33-1 at ¶¶ 4-8). After an image of child sexual abuse is viewed "by at least one Google employee," the image "is given a digital fingerprint ('hash')" and is "added to [Google's] repository of hashes of apparent child pornography as defined in 18 U.S.C. § 2256." *Id.* at ¶ 4. Although the company also receives tips from users who "flag suspicious content," Google confirms that "[n]o hash is added to [its] repository without the corresponding image first having been visually confirmed by a Google employee to be apparent child pornography." *Id.* at ¶ 5.

When Google "encounters a hash that matches a hash of a known child sexual abuse image," it does one of two things. *Id.* at ¶ 5. In some cases, Google does not view the image again, but instead automatically reports the user to the National Center for

Missing and Exploited Children (NCMEC), a non-profit organization authorized by Congress to "operate a cyber tipline to provide [ESPs] an effective means of reporting . . . child pornography." *Id.*; 42 U.S.C. § 5773(b)(1)(P). "In other cases, Google undertakes a manual, human review, to confirm that the image contains apparent child pornography before reporting it to NCMEC." *Id.* Google is required by law to report apparent child pornography to NCMEC through the CyberTipline when it becomes aware of it. 18 U.S.C. § 2258A.

In this case, when Google's product abuse detection system identified two images in miller694u@gmail.com's email account as having hash values matching hash values contained in Google's repository of apparent child pornography, Google "submitted an 'automatic report' to NCMEC" in compliance with its reporting obligations. (Doc. # 41 at 2 n.2). A Google employee did not re-view the images or the content of the email before submitting the report to NCMEC. (Doc. # 33-1 at ¶ 11). However, Google did provide NCMEC with "the email address used, the IP address associated with the email in question, classification of the images ['A1' under the industry classification system, meaning the image contained a depiction of a prepubescent minor engaged in a sexual act], the file names listed with the images and the two uploaded image files." (Doc. # 41 at 3).

Upon receiving the images, NCMEC's staff "did not open or view the two uploaded files contained in the report." *Id.* Instead, NCMEC "located publicly available social network profiles" associated with the email account, verified the IP address reported by Google, and learned it to be associated with a Time Warner Cable account having a

potential geographic location of Fort Mitchell, Kentucky." *Id.* That information was sent to the Kentucky State Police and the Kenton County Police Department. *Id.*

Detective Aaron Schihl of the KCPD received NCMEC's CyberTipline report on August 13, 2015. *Id.* at 4. "Detective Schihl opened the attachments and viewed the images, which he confirmed to be child pornography." *Id.* He sought a grand jury subpoena for the subscriber information for the Time Warner account and then sought and obtained a search warrant for the contents of the miller694u@gmail.com account. *Id.* Detective Schihl then obtained search warrants for Defendant's home and the electronic devices seized from his home, which yielded additional evidence of "receipt, possession, and distribution of child pornography." *Id.*

Now, Defendant seeks to suppress all evidence obtained by Detective Schihl, arguing that both Google's initial search and Detective Schihl's subsequent search violated the Fourth Amendment. In her R&R, Magistrate Judge Smith concluded that Google's initial review of the files did not implicate the Fourth Amendment because Google is a private actor, not a government agent. She also concluded that Detective Schihl's actions in viewing the images did not implicate the Fourth Amendment because his actions did not exceed the scope of the prior private search by Google.

In his objections, which the Court reviews *de novo*, Defendant makes three specific arguments. First, he argues that Google is a government actor because of its "close relationship and collaborative crime fighting efforts" with NCMEC, which the R&R assumes without deciding is a government actor. (Doc. # 44 at 2). As a result, Defendant argues, the fruits of Google's warrantless search should be suppressed. Second, Defendant argues that, even if Google is not a government actor, Detective Schihl's subsequent

review of the images exceeded Google's private search, meaning that the detective violated the Fourth Amendment because Defendant had a reasonable interest in the privacy of his email attachments. Finally, Defendant argues that Detective Schihl's actions were a search pursuant to traditional trespass doctrine because the email attachments were sealed virtual containers.

For the reasons set forth herein, the Court finds that Defendant's arguments are unavailing, **overrules** his objections, and **adopts** Magistrate Judge Smith's R&R as the Opinion of the Court.

III. Analysis

A. Google is not a government actor.

Defendant's first objection is to Magistrate Judge Smith's conclusion that Google is not a government actor. (Doc. # 44 at 2-4). Whether Google is a government actor is significant because the Fourth Amendment protects individuals from "unreasonable searches and seizures" by the government, not private entities. U.S. Const. amend. IV. Indeed, the Fourth Amendment "is wholly inapplicable" to searches and seizures by "a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official." *United States v. Jacobsen*, 466 U.S. 109, 113-14 (1984) (internal quotation marks omitted).

The Sixth Circuit uses a two-part test to determine whether a private entity is a government agent for the purposes of the Fourth Amendment. "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)). If the defendant cannot show both of these facts, the private actor is not a government agent. Here, Magistrate Judge Smith correctly concluded that Google is not a government agent when it voluntarily scans email attachments for apparent child pornography and sends reports to NCMEC.

The Sixth Circuit has not yet determined whether NCMEC itself is a government agent. (Doc. # 41 at 6). The Tenth Circuit recently concluded that it is, which means that NCMEC's actions implicate the Fourth Amendment to the extent they constitute "searches" or "seizures." *United States v. Ackerman*, 831 F.2d 1292, 1294-1304 (10th Cir. 2016 (Gorsuch, J.) (concluding that NCMEC is a government entity and a government agent). Magistrate Judge Smith assumed without deciding that NCMEC acted as a government agent in this case (Doc. # 41 at 6), and the Court sees no reason to disturb that assumption. However, that assumption does not extend to ESPs (like Google) that voluntarily scan emails for child pornography and report apparent child pornography to NCMEC.[1] In fact, every court to have addressed the question (including the First, Fourth, and Eighth Circuits) has determined that, in situations like this one, the ESP is not a government agent. (Doc. # 41 at 6-8 (collecting cases)).

Defendant argues that Google's "close and collaborative relationship" with NCMEC, a government agent, makes Google a government agent too. (Doc. # 44 at 2-3). According to Defendant, a statutory scheme that involves "mandatory reporting

[1] In *Ackerman*, the Tenth Circuit concluded that NCMEC exceeded the scope of the ESP's search in any event, so the status of the ESP was not at issue in that case. *Ackerman*, 831 F.2d at 1306-07.

requirements and penalties for failure to report" and a "requirement to preserve evidence" ties Google to NCMEC and makes it a government agent for purposes of the Fourth Amendment. (Doc. # 41 at 2); 18 U.S.C. §§ 2258A(a), (e), (f).

The statutory reporting requirements are not sufficient to transform Google into a government agent under this test. The Supreme Court's leading Fourth Amendment agency case, *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602 (1989), held that a regulatory scheme evidenced the government's "encouragement, endorsement, and participation" of a search when it "removed all legal barriers" for breath, blood, and urine testing of railroad operators, "mandated that the railroads not bargain away the authority to perform [such] tests," required employers to remove employees who refused to submit to the tests from service, and conferred the right to receive the results of the test on the government. *Skinner*, 489 U.S. at 615-16. The Court held that the regulatory scheme rendered otherwise private railroads agents of the government because it belied the idea that "tests conducted by private railroads . . . will be primarily the result of private initiative." *Id.*

Here, by contrast, there is ample evidence that Google's scanning is still the result of its private initiative, not government pressure. Unlike the regulations at issue in *Skinner*, the statutory scheme for reporting child pornography does not purport to authorize or remove "legal barriers" to ESP email scanning, or "prescribe consequences for [an ESP's] users should they refuse to submit" to the scanning. *United States v. Stevenson*, 727 F.3d 826, 829-30 (8th Cir. 2013). In fact, the statute explicitly disclaims a scanning or monitoring requirement, 18 U.S.C. § 2258A(f), and mandates only reporting of apparent images of child pornography that the ESPs are aware of, § 2258A(a). The penalties for failure to

report do not compel ESPs to monitor their subscribers as a practical matter, either–in fact, "the converse is just as likely to be true," because ESPs "might just as well take steps to avoid discovering reportable information" to avoid penalties for failure to report. *United States v. Richardson*, 607 F.3d 357, 367 (4th Cir. 2010). Unlike the regulatory scheme at issue in *Skinner*, nothing prevents the ESPs from doing just that, and there is no evidence that NCMEC imposes obligations on Google that the statutory scheme does not. As a result, the statutory reporting requirements do not transform Google into a government agent.

Defendant also argues that Google and NCMEC's collaborative relationship "supports a finding that NCMEC has intimate knowledge of Google's searching activities, and encourages them." (Doc. # 44 at 3). Defendant explains that Google and NCMEC share hash values (though he acknowledges that they did not do so in this case, *id.* at 3 n.3), that NCMEC gives Google awards for its collaboration, and that Google makes public statements about its collaboration with and support for NCMEC. *Id.* at 3. But acknowledgment of Google's voluntary activities is not the same as government participation in or encouragement of the search activities themselves. Whether Google has made itself a "willful participant" (Doc. # 27 at 6) in NCMEC's child-protective policies is not dispositive where, as here, Defendant has not met the second prong of the test–that Google's intention in searching is to provide the government with evidence for its criminal investigations.

Defendant failed to show that Google monitors image attachments for apparent child pornography with the intent of assisting police investigative efforts. Instead, Google presented evidence that it scans email attachments and uses its proprietary hashing

technology for its own business purposes. Google explains that it "independently and voluntarily take[s] steps to monitor and safeguard [its] platform" because if it "is associated with being a haven for abusive content and conduct, users will stop using [Google's] services." (Doc. # 33-1 at ¶ 3). In particular, "[r]idding [its] products and services of child abuse images is critically important to protecting [Google's] users, product, brand, and business interests." *Id.*

Other than reflecting a general societal consensus that images of child pornography are harmful, Google's business interests are "entirely independent of the government's intent to collect evidence for use in a criminal prosecution." *United States v. Bowers*, 594 F.3d 522, 526 (6th Cir. 2010) (internal quotation marks omitted). Even without a statutory obligation to report its findings to NCMEC, it seems likely that Google would screen its platform for images of child pornography because doing so is good business practice.

For all those reasons, the Court agrees with Magistrate Judge Smith that the evidence does not compel a finding that the government participates in Google's activities to such a degree that Google's search is the government's search. Defendant's objection is **overruled**.

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

Because Google's actions are not attributable to the government, Detective Schihl's subsequent review of the images will not violate the Fourth Amendment if that review does not exceed the scope of the prior private search. *Jacobsen*, 466 U.S. at 115. "Under 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." *United States v. Lichtenberger*, 786 F.3d 478, 485-86 (6th Cir. 2015) (citing *Jacobsen*, 466 U.S. at 119-20). With respect to child pornography, the Sixth Circuit has held a government search permissible 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," "learned nothing that had not previously been learned during the private search," and "infringed no legitimate expectation of privacy." *Id.* (internal quotation marks omitted).

1. This case is not like *Walter* because the images have been previously viewed by Google and the hash value is not a mere label.

Defendant's core objection is that Detective Schihl's actions are broader in scope and different in type from the actions taken by Google because Detective Schihl opened Defendant's email attachments to view the images, while Google merely looked at the hash values. (Doc. # 44 at 6). That distinction, Defendant argues, makes *Walter v. United States*, 447 U.S. 649 (1980) the proper analog to this case, and Defendant cites *United States v. Keith*, 980 F. Supp. 2d 33 (D. Mass. 2013), in support.

The Court disagrees. Defendant's argument is based on two flawed premises contradicted by the evidence and case law. The first flawed premise is that the images attached to his emails are akin to a sealed container that has never been opened. The second flawed premise is that the hash values associated with those images are analogous to the labels in *Walter*.

In *Walter*, the Supreme Court found a Fourth Amendment violation where private individuals mistakenly received shipments of films in boxes with labels that alluded to the obscene content of the films. *Walter*, 447 U.S. at 651. One individual held the film up to

the light, but could not see anything. *Id.* at 652. None of the private individuals watched the films. *Id.* Instead, they called the FBI, who watched the films without a warrant. *Id.* Two justices wrote that watching the film exceeded the scope of the prior search, two justices concurred in the result but wrote that watching the film would exceed the scope of the prior search even if the private individuals had held their own private screening because the private screening would not have exposed the film to plain view, and one justice concurred in the judgment without discussion. *Walter*, 447 U.S. at 658-62. Even the dissenting justices agreed that "[t]he additional invasions of respondents' privacy by the Government agent must be tested by the degree to which they exceeded the scope of the private search." *Jacobsen*, 466 U.S. at 115.

Defendant's argument that the images in this case are akin to the films in *Walter* that were not viewed in the private search is inconsistent with the evidence. Google's practice is to register hash values for images that Google has already physically viewed. (Doc. # 33-1 at ¶¶ 4-5). There is no evidence that Google departed from that practice in this case (and Defendant has abandoned his argument to the contrary (Doc. # 44 at 2 n.1)). After viewing the images at issue here, Google used its hashing technology and included the hash value in its registry. When Defendant attached the images to his email, Google noted a match in the hash values, conveyed that information to NCMEC, and NCMEC passed the information and the images along to Detective Schihl. (Doc. # 33-1 at ¶¶ 11). The argument that Detective Schihl, like the FBI agents in *Walter*, viewed the images when the private searchers did not is therefore not supported by the facts.[2]

---

[2] To the extent that Defendant's argument relies on a distinction between the file previously viewed by Google and the file Defendant attached to his email, that is a distinction without a

Contrary to Defendant's suggestion, the hash value is not a label like what was written on the boxes in *Walter*. A hash value, unlike a label, has no inherent meaning–it gains meaning only when it matches with a hash value in the child pornography repository and therefore reminds Google that it has seen this image before. Indeed, a closer analog to the *Walter* case would be if Google had flagged the images in Defendant's email as apparent child pornography *merely because of their file names*, without having ever looked at the images to verify their content. If that were the situation, Detective Schihl's subsequent examination of the files would present a different, and much more difficult, question of scope.

For the same reasons outlined above, the Court departs from the district court's analysis in *United States v. Keith*, 980 F. Supp. 2d 33 (D. Mass. 2013). That court found 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." *Id.* at 43. "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 of that designation is unknown.*" *Id.* (emphasis added). Based on the evidence before the *Keith* Court, it was not clear *who* performed the initial private search—the court noted it was "possible that the hash value of a suspect file was initially generated by another provider and then shared with AOL." *Id.* at 37 n.2. The court also concluded from testimony at the evidentiary hearing that it is "indisputable that

---

difference. The two files were matched by hash values—a digital fingerprint. (Doc. # 33-1 at ¶ 4). Defendant does not challenge the reliability of hashing, and as the R&R notes, "it appears well established that it is, in fact, reliable." (*See* Doc. # 41 at 21).

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." *Id.* at 42-43; *see also id.* at 37 ("[n]othing is known about how the file came to be originally hashed and added to the flat file database, except that it was AOL's practice to hash and add to the database either the hash value of any file that was identified by one of its graphic file analysts as containing child pornography or a hash value similarly generated by a different ESP or ISP and shared with AOL").

Here, by contrast, the evidence indicates that Google itself had already viewed the images and identified them as apparent child pornography to Detective Schihl before he ever conducted his search. (*See* Doc. # 33-1 at ¶¶ 4-5 ("[n]o hash is added to [Google's] repository without the corresponding image first having been visually confirmed by a Google employee to be apparent child pornography")). Defendant's efforts to analogize this case with searches violative of the Fourth Amendment in *Walter* and *Keith* fail because this case is distinguishable on a key point—the evidence shows that Google previously viewed the images at issue and tagged them as apparent child pornography.

Detective Schihl also avoids the pitfall the Tenth Circuit identified in *Ackerman*, where NCMEC (acting as a government agent) viewed images that the ESP had not even hashed. As Magistrate Judge Smith explains, in *Ackerman*, AOL's email filter identified one image out of four attachments to an email that matched the hash value of an image AOL had previously deemed to be child pornography. *Ackerman*, 831 F.3d at 1294. Like Google did here, AOL sent a report to NCMEC. *Id.* But unlike here, NCMEC viewed more than just the image matching AOL's hash values—it also viewed the contents of the email and the other three attachments, which AOL had never examined. *Id*. The *Ackerman*

Court determined that by "opening the email itself" and the three additional attachments, NCMEC "exceeded rather than repeated" AOL's private search. *Id.* at 1306. The Tenth Circuit did not need to address the constitutionality of the situation presented here, where the government looks only at the material that had previously been examined. *Id.* at 1306.

2. *Jacobsen* and *Bowers* support the conclusion that Detective Schihl's search did not exceed the scope of Google's.

Contrary to Defendant's argument, the scope of Detective Schihl's search in this case is more like the narrowly drawn searches that the Supreme Court and Sixth Circuit upheld in *Jacobsen* and *Bowers*. *Jacobsen*, the case that marks the origin of the private search doctrine, began with FedEx employees examining the contents of a damaged package. *Jacobsen*, 466 U.S. at 111. Inside the cardboard container, they discovered a ten-inch tube made of duct tape which, when the employees cut it open, revealed four plastic bags filled with white powder. *Id.* FedEx called the DEA and put the tube and its contents back in the box. *Id.* The DEA agent inspected the partially open container, removed the plastic bags, and field-tested them for cocaine. *Id.* at 112. The Supreme Court held that the DEA agent's inspection of the plastic bags and testing of the powder remained within the scope of FedEx's prior 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 had already been told." *Id.* at 119. Moreover, the field test "could disclose only one fact previously unknown to the agent—whether or not a suspicious white powder was cocaine"—a fact in which the defendant had no legitimate expectation of privacy. *Id.* at 122-24.

The Sixth Circuit applied the logic of *Jacobsen*'s private search doctrine to depictions of child pornography in *Bowers*. *Bowers*, 594 F.3d at 526. In that case, a private search by the defendant's housemate uncovered a physical photo album that contained child pornography. *Bowers*, 594 F. 3d at 524. The housemate alerted the FBI, who later looked at the same photo album and confirmed that it likely contained child pornography. *Id*. The Sixth Circuit held that the FBI's actions did not exceed the scope of the housemate's private search and affirmed the denial of the motion to suppress because "the agents 'learn[ed] nothing that had not previously been learned during the private search' and 'infringed no legitimate expectation of privacy.'" *Id.* at 526 (quoting *Jacobsen*, 466 U.S. at 119-20). *See also 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" in a case where storage unit employee notified police of child pornography found in a suitcase in defendant's storage unit).

Defendant argues that the "virtual certainty" test of *Jacobsen* does not apply unless there has been a "previous search of the actual container in question." (Doc. # 44 at 6). As explained above, Google's practice of only hashing files its employees have viewed indicates that Google *did* previously view the images attached to Defendant's email. In this case, as in *Bowers*, a private party viewed the images, believed that they were child pornography, and alerted the authorities, who then viewed the same images. The difference between *Bowers* and this case is that the images here are made of pixels, not photo paper, and that Google identified the images as ones it had previously viewed by using hash values instead of human memory. Despite the relation to legitimate and "extensive privacy interests at stake in . . . modern electronic device[s]," *Lichtenberger*, 786

F.3d at 485, those differences do not require a different result in this case because the "virtual certainty" standard is met.

In *Lichtenberger*, the Sixth Circuit applied *Jacobsen* to an officer's search of a defendant's laptop for child pornography, holding that, in order for the government's search to be within the scope of the earlier private search, the government official "had to proceed with 'virtual certainty' that the 'inspection of the [laptop] and its contents would not tell [him] anything more than he had already been told'" by the defendant's girlfriend, the private searcher. *Lichtenberger*, 786 F.3d at 488. The court ruled that the officer did not have "virtual certainty" that what he viewed would be the same child pornography the girlfriend reported because it was not at all clear that she showed him the same images she had previously looked at. There was "a very real possibility," the court concluded, that the detective "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." *Id.* at 488-49.

There is no such possibility here. As discussed earlier, the digital fingerprints produced by hashing provide "virtual certainty" that the images will be the same as those seen on a prior search. And because Google's CyberTip report "did not include any email body text or header information associated with the reported content" (Doc. # 33-1 at ¶ 10), or any images that Google had not previously viewed, Detective Schihl had "little chance to see much other than contraband." *Lichtenberger*, 786 F.3d at 486. *Compare with Ackerman*, 831 F.3d at 1294 (NCMEC viewed email content and three attachments that the ESP had not viewed). That distinguishes this case from ones involving laptops and cell

phones where privacy interests are high because of the large amount of information on those devices. There was no likelihood here, as there was in *Lichtenberger* or similar cases, that the attachments would "contain 1) many kinds of data, 2) in vast amounts, and 3) corresponding to a long swath of time." *Lichtenberger*, 786 F.3d at 488. The key question for the test under *Jacobsen* is whether the government official "saw the exact same images" the private searcher saw. *Id.* at 490. In this case, the evidence reveals that Detective Schihl and Google saw the same images—no more and no less.

Finally, Defendant argues that applying *Jacobsen* to find that Defendant's Fourth Amendment rights were not violated is a dramatic expanse of doctrine that allows "modern technology utilized by the private party" to "frustrate a citizen's reasonable expectation of privacy in the contents of a citizen's sealed container." (Doc. # 44 at 6-7). This is not so. Google's hash-value matching—in the words of the R&R, its "virtual eye"—does not reveal anything about an image that Google does not already know from the regular eyes of its employees. Put another way, hashing is not a futuristic substitute for a private search—it is merely a sophisticated way of confirming that Google already conducted a private search. Google's use of hash values has no more effect on Defendant's reasonable expectation of privacy than Google's initial private search does (and because Google is not a government agent, the Fourth Amendment is "wholly inapplicable" to its searches, even "unreasonable one[s]," *Jacobsen*, 446 U.S. at 113-14).

For all those reasons, Defendant's objection that Detective Schihl's search exceeded the scope of Google's private search is **overruled**.

C. Traditional trespass analysis does not apply.

Defendant's last objection is that Detective Schihl's search "was illegal when viewed through the lens of the traditional trespass test." (Doc. # 44 at 7-8) (citing *Ackerman*, 831 F.3d at 1308 (citing *United States v. Jones*, 565 U.S. 400 (2012))). Defendant also argues that Google did not open the attachments, which he refers to as "sealed virtual containers." *Id.* Once again, Defendant's attempt to distinguish between the image uploaded to his email account and the image Google previously viewed is unavailing—these particular attachments are not "sealed virtual containers" because the matching hash values indicate that Google has previously viewed them. Moreover, as Magistrate Judge Smith explains in the R&R, the "traditional trespass" test does not apply when the government action is within the scope of a previous private search, because the Fourth Amendment does not apply to private individuals. (Doc. # 41 at 26 n.10). Therefore, this objection is overruled.

IV. Conclusion

Upon *de novo* consideration of the R&R and the objections thereto, the Court concludes that Magistrate Judge Smith's factual findings are clearly supported by the record. The Court further agrees with Magistrate Judge Smith's analysis and recommended disposition of Defendant's motion to suppress. Accordingly,

IT IS ORDERED as follows:

(1) Defendant's objections to the Magistrate Judge's Report and Recommendation are **overruled**;

(2) The Magistrate Judge's factual findings are **adopted** as the factual findings of the Court;

(3) The Magistrate Judge's analysis and conclusions of law are **adopted** as the Court's conclusions of law, as supplemented herein;

(4) Defendant's Motion to Suppress evidence (Doc. # 27) is **denied**; and

(5) The time period from January 31, 2017 through the date of this Order, totaling 143 days, is deemed excludable time from the Speedy Trial Act pursuant to 18 U.S.C. § 3161(h)(1)(F).

This 23rd day of June, 2017.

Signed By:
David L. Bunning DB
United States District Judge

K:\DATA\ORDERS\Covington Criminal\2016\16-47 Order Adopting R&R.wpd