UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
NORTHERN DIVISION
COVINGTON

CRIMINAL ACTION NO. 16-47-S-ART

UNITED STATES OF AMERICA **PLAINTIFF**

V. **UNITED STATES'S RESPONSE TO DEFENDANT'S MOTION TO SUPPRESS**

WILLIAM J. MILLER **DEFENDANT**

* * * * *

The United States submits the following response to the Defendant's motion to suppress [R. 27: Motion.] As set forth more fully below, the Defendant's motion should be denied.

I. Factual Background

On July 9, 2015, an individual using Google email (gmail) account miller694u@gmail.com uploaded two images of child pornography to an email. Google became aware of the images because "since 2008, Google has been using its own proprietary hashing technology to tag confirmed child sexual abuse images." *See* Exhibit 1 (Declaration of Cathy McGoff) at ¶4. The process used by Google is explained as follows:

> Each offending image, after it is viewed by at least one Google employee, is given a digital fingerprint ("hash") that [Google's] computers can automatically recognize and is added to [Google's] repository of hashes of apparent child pornography as defined in 18 USC § 2256. Comparing these hashes to hashes of content uploaded to [Google's] services allows

> [Google] to identify duplicate images of apparent child pornography to prevent them from continuing to circulate on [Google's] products.

Id. When the software identified the two images of child pornography, it triggered both an "Automatic Report" to the National Center for Missing and Exploited Children (NCMEC) CyberTipline,[1] which is required by law, as well as an automatic disabling of the gmail account. The Automatic Report sent by Google to NCMEC contained the following information: (1) the incident type (child pornography) and time; (2) the email address used; (3) the IP address for the computer used; and (4) the number of files uploaded, the file names, and a categorization that indicated that the images depicted a prepubescent minor engaging in a "sex act" or sexually explicit conduct. *See* Exhibit 2 (CyberTipline Report) at 1-4. Google did not review the contents of the email to which the images were attached, and advised NCMEC that "[t]he reported user uploaded the attached media to an email in Gmail, which may or may not have been sent." *Id*. at 2-3.

The classification of the report as "Automatic" meant that the images were scanned by Google's proprietary hashing technology (rather than reviewed by a Google employee concurrently with submitting the report) and found to contain hash values that matched images that had previously been identified by a Google employee as depicting child pornography. *See* Exhibit 1 at ¶¶7, 10. Google utilizes this technology because its "has a strong business interest in …ensuring [its] products are free of illegal content, and in particular, child sexual abuse material." *Id*. at ¶3. In a similar vein, Google "rel[ies]

[1] *See* Declaration of John Shehan, Vice President of Exploited Children Division at the National Center for Missing and Exploited Children, attached hereto as Exhibit 6, for a detailed explanation of NCMEC's corporate status, mission, and operation; as well as the creation and operation of the CyberTipline.

on users who flag suspicious content they encounter so [Google] can review it and help expand [its] database of illegal images." *Id*. at ¶5. Importantly, "[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." *Id*.

Once NCMEC received the report by Google, it undertook a series of steps, including geographically resolving the IP address via a publicly-available online search. That search revealed that Time Warner Cable was Internet Service Provider (ISP) for the computer involved, which was located in Ft. Mitchell, Kentucky. NCMEC also searched the email address that was used to upload the images, using Google, Facebook, MeetMe and other publicly-available websites. Importantly, NMCEC did not review the two images provided by Google; in fact, the CyberTipline report expressly states, "[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." *See* Exhibit 2 at 6. Rather, NCMEC simply forwarded the images – as part of the CyberTipline report – to the Kentucky Internet Crimes Against Children (ICAC) task force, which is headed by the Kentucky State Police (KSP). The CyberTipline report was made available to KSP via a virtual private network (VPN). The report was then mailed via certified mail by KSP to the Kenton County Police Department and ultimately reviewed by Detective Aaron Schihl.

On August 13, 2015, Detective Aaron Schihl reviewed the CyberTipline report, including the images provided by Google to NCMEC. On August 24, 2015, Schihl obtained – via subpoena – subscriber information from Time Warner Cable, including the

subscriber's name and address,[2] and confirmation that the internet service was still active. On October 22, 2015, Schihl obtained a search warrant for the contents of gmail account miller694u@gmail.com; the affidavit in support included the information contained in the CyberTipline report, the information provided by Time Warner Cable, and a description of what the images depicted, which Schihl indicated was based upon his review of the images themselves. *See* Exhibit 3 (Google search warrant). The results produced by Google included thousands of emails, which revealed evidence of distribution and receipt of child pornography by the Defendant.

Detective Schihl then obtained a search warrant for the Defendant's home, which was searched on October 29, 2015. *See* Exhibit 4 (Residence search warrant). Officers located several items of digital media, including an Acer laptop (which the Defendant acknowledged belonged to him and was primarily used by him), as well as a Toshiba external hard drive (which the Defendant admitted was purchased by him and contained child pornography). All of these admissions were made after the Defendant was advised of his *Miranda* rights, voluntarily waived those rights, and agreed to speak to agents.

Finally, Schihl obtained a search warrant for the electronic evidence seized from the Defendant's home. *See* Exhibit 5 (Media search warrant). Forensic examination of the laptop and hard drive, in particular, revealed Skype chat messages sent from "Bill Miller" and requesting "naked pics" of girls or young boys and offering to pay for sex

[2] The responsive information from Time Warner Cable revealed that the subscriber was Tania Miller and listed the Defendant's residence as the address.

online; thousands of videos and images of minors engaged in sex acts; and user-created folders labeled "Incest," "Teens," "Preteens," and the like.

II. Argument

a. Google is not a government actor

In his motion, the Defendant contends that "Google, as a state actor, searched [his email account] and seized specific email attachments," all without a warrant. [R. 27: Motion at 111.][3] According to the Defendant, Google is transformed into a state actor "[b]ecause NCMEC is a state actor and, Google … has a nexus relationship with NCMEC…." [*Id*. at 112.] The Defendant presumes that "[a]lthough Google is not required by law to search its email accounts for child pornography, [it does so] … based on Google's relationship with NCMEC." [*Id*. at 114.] That faulty premise leads to an equally untenable conclusion. *See* Exhibit 1 at ¶3 (explaining that Google "independently and voluntarily" takes steps to monitor and safeguard its platform to promote its own business interests).

Although the Sixth Circuit has not addressed whether electronic service providers (ESPs), like Google, act as government agents when they monitor their users' activities on their servers, or when they implement their own internal security measures against users engaging in illegal activity through their services, those courts that have addressed the question uniformly answer it in the negative. *See United States v. Stratton*, No. 15-40084-010-DDC, 2017 WL 169041, at *4 (D. Kansas Jan. 17, 2017) (holding that Sony

[3] All references are to the Page ID#.

was not a government agent when it searched images stored on the defendant's PS3); *United States v. Richardson*, 607 F.3d 357, 366 (4th Cir. 2010) (holding that AOL's scanning of email communications for child pornography 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. Stevenson*, 727 F.3d 826, 831 (8th Cir. 2013) ("AOL's decision on its own initiative to ferret out child pornography does not convert the company into an agent or instrument of the government for Fourth Amendment purposes.... AOL's voluntary efforts to achieve a goal that it shares with law enforcement do not, by themselves, transform the company into a government agent."); *United States v. Keith*, 980 F. Supp. 2d 33, 40 (D. Mass 2013) (AOL is not a government agent); *United States v. Ackerman*, No. 13–10176–01–EFM, 2014 WL 2968164, at *5-6 (D. Kan. July 1, 2014) (AOL is not a state actor), *rev'd on other grounds*, 831 F.3d 1292 (10th Cir. 2016); *United States v. Drivdahl*, No. CR–13–18–DLC, 2014 WL 896734, at *3-4 (D. Mont. Mar. 6, 2014) (Google is not a Government agent); *United States v. Cameron*, 699 F.3d 621, 637–38 (1st Cir. 2012) (Yahoo!, Inc., did not act as an agent in searching e-mails and sending reports to NCMEC); *United States v. DiTomasso*, 81 F. Supp. 3d 304 (S.D.N.Y. 2015) (chat service provider Omegle held not to be a Government agent and its search of defendant's chat messages held to be a pure private search beyond the reach of the Fourth Amendment); *United States v. Miller*, No. 8:15CR172, 2015 WL 5824024, at *4 (D. Neb. Oct. 6, 2015) (holding that Google is a "private, for profit entity" that "complied with its statutory duty to report violations of child pornography laws" and did not become a state actor by doing

so). Many of these courts have so held despite the relationship between NCMEC and ESPs that is relied upon by the Defendant. Therefore, contrary to the Defendant's claim, Google did not lose or forfeit its status a private party simply by complying with its legal obligation to report suspected criminal activity to NCMEC.

In short, the great weight of authority refutes the Defendant's claim that Google acted as a government agent in conducting a warrantless search of his email account. So, even if the Court assumes that a search occurred when Google reported the images, the Fourth Amendment is not implicated and no warrant was required. *See infra* pp. 7-8.

b. NCMEC acted solely as a clearinghouse in this case

NCMEC's involvement in this case was limited to compiling all the information it received from Google, conducting limited investigation using publicly-available resources, and transmitting the full report to law enforcement. In fact, the CyberTipline report expressly states: "[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." *See* Exhibit 2 at 6. Therefore, unlike in *Ackerman*, 831 F.3d 1292 (10th Cir. 2016) – upon which the Defendant relies – NCMEC did not conduct a "search" of any kind; as a result, the determination of NCMEC's status is irrelevant.

c. Detective Schihl's review of the images did not constitute a search

Detective Schihl's review of the two images contained in the CyberTipline report did not constitute a "search" subject to Fourth Amendment scrutiny. Outside the context of physical trespass, a "search" within the meaning of the Fourth Amendment occurs

when governmental action infringes "an expectation of privacy that society is prepared to consider reasonable." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). The Fourth Amendment is "wholly inapplicable" to a search or seizure conducted by a private party not acting as an agent of the government, and additional invasions of privacy by the government following a private search do not implicate the Fourth Amendment if they stay within the scope of the private search. *Id*. at 115. The reasonableness of a particular intrusion by the government is "appraised on the basis of the facts as they existed at the time that invasion occurred." *Id*.; *United States v. Lichtenberger*, 786 F.3d 478, 485 (6th Cir. 2015) (*quoting Jacobsen*). While, as a general matter, a person who uses a third-party email provider enjoys a reasonable expectation of privacy in the contents of his account, *United States v. Warshak*, 631 F.3d 266, 287-88 (6th Cir. 2010), there is no allegation that Detective Schihl reviewed, or asked Google to review, the contents of the Defendant's gmail account prior to obtaining a search warrant. Instead, the allegedly unconstitutional action by Detective Schihl is limited to his review of two images that Google had already identified as child pornography, separated from other materials in the account, and submitted to NCMEC.

Under these circumstances, the application of the private search doctrine insulates Detective Schihl's review of the images from Fourth Amendment scrutiny because Google had already identified the two images as child pornography, even going so far as categorizing the images as to their content and including this information in its CyberTipline submission. Detective Schihl's subsequent review of the images stayed within the scope of Google's private search because it was virtually certain to reveal

nothing more than that the images constituted child pornography, as reported by Google after its private search.

Alternatively, even if the Court finds that Detective Schihl's review of the images exceeded the scope of the search conducted by Google so as to render the private search doctrine inapplicable, the Defendant still cannot meet his burden of showing that, at the time of Detective Schihl's review of the two images submitted by Google: 1) he had an actual, subjective expectation of privacy in the images; and 2) society is prepared to recognize that expectation as objectively reasonable. *See, e.g.*, *Rawlings v. Kentucky*, 448 U.S. 98, 104-105 (1980). Any subjective expectation of privacy that the Defendant may have had was not one that society is prepared to recognize as objectively reasonable because Google had exercised its right to monitor its system, disabled the Defendant's account, and turned the images over to NCMEC. *See infra* pp. 16-20.

d. Detective Schihl's review stayed within the scope of the private search

When a private party conducts a search that frustrates an individual's reasonable expectation of privacy and delivers information to the government, the Fourth Amendment is "implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated." *Jacobsen*, 466 U.S. at 117. To determine whether "additional invasions" of privacy by a government actor are subject to Fourth Amendment scrutiny, they must be "tested by the degree to which they exceeded the scope of the private search." *Id*. at 115 (*citing Walter v. United States*, 447 U.S. 649 (1980)). As the Sixth Circuit has explained, a government search will be deemed to stay within the scope of the private search when "the officers in question had

near-certainty regarding what they would find and little chance to see much other than contraband." *Lichtenberger*, 786 F.3d at 486.

The Sixth Circuit has applied the private search doctrine in cases involving child pornography at least three times. *See Lichtenberger*, 786 F.3d at 485-86; *United States v. Bowers*, 594 F.3d 522 (6th Cir. 2010); *United States v. Richards*, F. App'x 480 (6th Cir. 2008). Law enforcement's conduct in this case – which included reviewing only two images that had already been isolated and turned over by the private searcher – is far more limited than the alleged intrusions considered by the Sixth Circuit in the prior cases. Those same facts also ameliorate the concerns about the significant privacy interests implicated in searches of "complex electronic devices" that informed the Sixth Circuit's holding in *Lichtenberger*. 786 F.3d at 487. In this case, it is clear that when Detective Schihl opened the two images contained in the CyberTipline report, he had a virtual certainty of finding child pornography already revealed during the private search, and little, if any, chance of observing anything other than material already revealed by the private search.

In *Lichtenberger*, a private searcher saw what she believed to be child pornography images on the defendant's laptop computer and called police. While the responding officer asked the private searcher to show him what she had found during her earlier search of the laptop, the private searcher testified 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." 786 F.3d at 488. Under those circumstances, and in light of the vast amount of private information stored on laptop

computers, the court in *Lichtenberger* concluded that the government exceeded the scope of the private search. *Id*. In so holding, the court noted that, while all of the images that the private searcher showed to the officer were child pornography, "there was no virtual certainty that would be the case." *Id*. Rather, "the same folders . . . could have contained . . . bank statements or personal communications" or "anything from Lichtenberger's medical history to his choice of restaurant." *Id*.

In the other two Sixth Circuit cases involving child pornography images and the private search doctrine, the court found that the government stayed within the scope of the private search notwithstanding the fact that law enforcement officers may have viewed individual images not seen during the private search. In *Bowers*, for example, two private individuals discovered a binder containing child pornography photos in the defendant's bedroom. 594 F.3d at 524. Agents were notified, saw the album on a kitchen table, "reviewed the album," and "confirmed that it likely contained child pornography . . .." *Id*. Rejecting the defendant's argument that the agents' search of the album violated his Fourth Amendment rights, the Sixth Circuit held that "based on [the] statements that the album contained child pornography, the agents were justified in opening the album to view the potentially incriminating evidence." *Id*. at 526. The court concluded that because neither private individual "was acting as a government agent when [he] first discovered the album, the album was in a common area of the house when the agents arrived, and there is no evidence that the agents exceeded the scope of the initial private search, . . . the district court properly denied Bowers's motion to suppress." *Id*. at 527.

In *Richards*, the court considered the government's search of a storage unit after two private individuals reported seeing suspected child pornography inside it. 301 F. App'x at 481-82. One of the private searchers had opened a suitcase in the unit that appeared to contain photographs of nude minors, and the other had inspected the storage unit and seen "various pornographic materials including photos of nude minors." *Id.* at 481. Five members of law enforcement conducted limited inspections confirming the presence of child pornography in the storage unit before obtaining a warrant; at least one of these involved entering the unit. *Id*. at 481-82. In holding that the government remained within the scope of the private search, the court stopped well short of requiring evidence that the private searchers had observed the same individual images later viewed by law enforcement. Instead, the court more generally determined that the "officers merely confirmed the prior knowledge that [the private searcher] learned earlier in the day – that unit 234 contained child pornography." *Id*. at 483. *See also Lichtenberger*, 786 F.3d at 486 (discussing *Richards*).

In this case, a reasonable officer in receipt of CyberTipline Report 5778397, which indicated that Google had identified two image files uploaded on its system as child pornography, described both of the images as falling into category "A1," which depicted a prepubescent child engaged in a sex act, and listed the file names as "young – tight fuck.jpg" and "!!!!!!Mom&son7.jpg," would have a "virtual certainty" that opening the images would only confirm that they contained child pornography, as reported by Google after its private search. *Cf. Lichtenberger*, 786 F.3d at 488. Just as in *Bowers*, where the agents were "justified in opening the album to view the potentially incriminating

evidence" based on the private searcher's "statements that the album contained child pornography," 494 F.3d at 526, Detective Schihl was justified in opening the two image files that had been identified by Google as constituting child pornography, and which were further described by classification and file name.

The Defendant's reliance on the Tenth Circuit's decision in *United States v. Ackerman*, 831 F.3d 1292, 1305, 1308-09 (10th Cir. 2016), *reh'g denied* (Oct. 4, 2016), is misplaced. In *Ackerman*, the court held that NCMEC is a governmental entity and, in the alternative, that it operated as the government's agent when reviewing materials submitted to the CyberTipline. It also concluded that NCMEC exceeded the scope of the private search conducted by AOL when NCMEC opened and viewed an email and four attached images that were included in AOL's CyberTipline Report, when AOL had only identified one of the four images as a hash value match for child pornography. *Ackerman*, 831 F.3d at 1308-09. The court in *Ackerman* explicitly recognized in dicta that its application of the private search doctrine might be different if NCMEC had limited its review to the single image identified by AOL as a hash value match to previously identified child pornography, or if AOL's private search had provided some information about the contents of the email and three additional attachments. 831 F.3d at 1306-07.

In this case, that Google's visual review of the two images occurred prior to its discovery of those images in the Defendant's account does not mean that Detective Schihl exceeded the scope of Google's private search when he visually reviewed the two images. As explained by Google, trained Google employees visually review suspected

images of child pornography to assess whether they meet the federal definition of child pornography prior to adding the hash value for that image to its repository of suspected child pornography images. *See* Exhibit 1 at ¶6. In addition, there is no real question that a hash value match between a file on Google's system and an image its repository – as occurred in this case – means that the matching file is the same image of child pornography as one previously added to Google's repository; when the hash values of two files match, there is over a 99.9% certainty that those files are identical down to the pixel level. *See, e.g., United States v. Cartier*, No. 2:06—cr—73, 2007 WL 319648 (D.N.D. Jan. 30, 2007), *affirmed*, 545 F.3d 442 (8th Cir. 2008). Instead, the Defendant argues that the fact that neither Google nor NCMEC visually reviewed the two flagged image files after they were found in his account using hash-value matching means that the CyberTipline report effectively contained no information about the content of those image files. [R. 27: Motion at 118.] The Defendant's argument misconstrues the private search doctrine and the facts of this case. While a hash value alone does not provide any information about the content of a file, or even the nature of a file (document, image, spreadsheet), Google only uses hash values of image files that it has opened, viewed, and determined to be child pornography. While the possibility still exists that Google erred in its original determination that the file constituted child pornography, that possibility is no greater than if a private person had viewed an image believed to be child pornography and then reported what was observed to law enforcement. And in both cases, the private search has frustrated any expectation of privacy in the image file by identifying its

contents (whether or not those contents meet the federal definition of child pornography).[4]

At the time that Detective Schihl received CyberTipline Report 5778397 and opened the two image files contained in that report, he could reasonably believe that opening those files would reveal only information with respect to which the expectation of privacy had "already been frustrated" by the private search. *Cf. Lichtenberger*, 786 F.3d at 485. Even if it were later determined that law enforcement somehow exceeded the scope of the private search – which it did not – the inquiry properly concerns whether a reasonable law enforcement officer would have believed that he was staying within the bounds of the private search. *Cf. Illinois v. Rodriguez*, 497 U.S. 177, 188-89 (1990) (in context of third-party consent doctrine, holding that agents can rely on a claim of authority from third party that later turns out to be false if based on "the facts available to the officer at the moment, . . . a man of reasonable caution . . . [would believe] that the consenting party had authority" to consent to a search of the premises). The application of Sixth Circuit authority regarding the private search doctrine to the facts of this case demonstrates that Detective Schihl stayed within the scope of Google's private search. Detective Schihl's review was limited to two specific images that Google had identified as likely child pornography and described as depicting prepubescent children engaged in

[4] In *United States v. Keith*, 980 F. Supp. 2d 33, 42-43 (D. Mass. 2013), the court held that NCMEC was a state actor and that its opening of single image file identified and submitted by AOL after hash value match was an expansion of AOL's private search. The government believes that the court in *Keith* erred in its application of the private search doctrine. In addition, the facts of this are distinguishable because Google provided additional information about the contents of the images, including a classification (that indicated that they depicted prepubescent children engaged in sex acts) and the sexually explicit file names.

sex acts, and which contained sexually explicit file names suggestive of child pornography; this provided a "near-certainty regarding what they would find and little chance to see much other than contraband." *Lichtenberger*, 786 F.3d at 486.

e. Even if Schihl exceeded the scope of Google's private search, the Defendant had no reasonable expectation of privacy in the images

If the Court finds that Detective Schihl's review of the two images that Google submitted to the CyberTipline exceeded the scope of Google's private search, it does not necessarily render Detective Schihl's review a "search" within the meaning of the Fourth Amendment. The Defendant still must meet his burden of showing that he had an actual, subjective expectation of privacy in the image files, and that his expectation is one that society is prepared to recognize as objectively reasonable. *See, e.g.*, *Rawlings*, 448 U.S. at 104-105; *United States v. Lanier*, 636 F.3d 228, 231 (6th Cir. 2011); *see also Jacobsen*, 466 U.S. at 122 (noting that additional invasions by the government that exceed the scope of the private search no longer fall within the private search exception to the warrant requirement and must be assessed for whether they constitute an "unlawful 'search' or 'seizure' within the meaning of the Fourth Amendment.").

The circumstances existing at the time of the allegedly warrantless review of the images by Detective Schihl undermine any claimed legitimate expectation of privacy by the Defendant. As an initial matter, the Defendant has not put forward anything to meet his burden of showing that he had an actual, subjective expectation of privacy in the two image files at issue. He has not suggested how he maintained a subjective expectation of privacy in images of child pornography uploaded to his Google account when Google's

terms of service explicitly stated that Google "prohibits [its] services from being used in violation of law" and "may review content to determine whether it is illegal …." *See* Exhibit 1 at ¶2. Equally important, the Defendant has failed to present any evidence or even suggest how he maintained an actual, subjective expectation of privacy these images after Google disabled his account, which occurred before Detective Schihl reviewed the two images submitted with Google's CyberTipline report about Miller.

Even if the Defendant could show that he had an actual, subjective expectation of privacy in the two images included in Google's CyberTipline report, he cannot demonstrate that any such expectation in these images is one that society is prepared to recognize as objectively reasonable, after Google exercised its right to monitor its system, identified the images as apparent child pornography, disabled his account, and submitted the images to the CyberTipline. Courts considering whether an expectation of privacy is objectively reasonable look to whether it arises from a source "outside the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." *Rakas v. Illinois*, 439 U.S. 128, 143–44 (1978). As in this case, a defendant may not be able to establish a legitimate expectation of privacy if his right to use or control a space in which people generally enjoy a reasonable expectation of privacy is dependent on rights provided by a third party, and the third party acts to terminate those rights.

More specifically, the Sixth Circuit has recognized that, while a hotel guest typically has a legitimate expectation of privacy in his hotel room and its contents, when the rental period expires or the hotel moves to evict the occupants because of non-

payment of rent, that expectation of privacy is no longer one that society is prepared to recognize as objectively reasonable. *See United States v. Lanier*, 636 F.3d 228, 232 (6th Cir. 2011); *United States v. Allen*, 106 F.3d 695, 699–700 (6th Cir. 1997). In *Allen*, the Sixth Circuit first found that the private search doctrine does not apply to the search of a hotel room (which is akin to a home), but then held that the actions taken by the hotel to evict the defendant from his room extinguished his privacy interests in the room's contents. 106 F.3d at 699-700. As the court in *Allen* explained:

> Upon learning that Allen was keeping contraband within the motel, the motel manager locked Allen out of his room. With this action, the motel manager divested Allen of his status as an occupant of the room, and concomitantly terminated his privacy interest in its contents. Once the manager, through private action took possession of the motel room, Allen could no longer assert a legitimate privacy interest in its contents.

Id.

Likewise, in *Lanier*, the Sixth Circuit found that law enforcement's entry into the defendant's hotel room after check-out time, and after the hotel reported seeing drugs in his room, did not intrude on any reasonable expectation of privacy held by the defendant. 636 F.3d at 232. In reaching this holding, the court noted that while "a hotel's practices and communications with the guest may modify the general rule" that the guest's privacy interests end at check-out time, no exceptions applied to the defendant where the search occurred after check-out time, he a defendant who did not ask or receive permission for a later check-out time and where the "hotel had no history of acquiescing in delayed departures by [the defendant]" did not retain a reasonable expectation of privacy in a his hotel room after check-out time. *Id*. at 232-33.

In these "hotel search" cases, the determinative question is whether the defendant had a reasonable expectation of privacy at the time that the room was searched by the government, rather than generally whether hotel guests have a reasonable expectation of privacy in their hotel rooms and the contents thereof. Against this backdrop, it is clear that the Defendant cannot establish that he had a legitimate expectation of privacy in the images contained in Google's CyberTipline report, at the time of Detective Schihl's allegedly unconstitutional warrantless review. The Defendant elected to use Google, a private internet service provider that expressly reserves the right to monitor content on its system for illegal materials, to upload images of child pornography. When Google determined that two images in the Defendant's account, on its system, constituted child pornography, it terminated the Defendant's account and submitted the images to the CyberTipline, both of which occurred the same day and prior to Schihl's review of the images.

The Defendant's claim to a legitimate expectation of privacy thus draws no support from concepts of "real or personal property law," and he cannot show lawful or even constructive possession of the two images at the time that they were reviewed by Detective Schihl. *Cf. Allen*, 106 F.3d at 699 (noting that, at the time of the government search, "Allen's tenancy properly ceased, both because he was not allowed to store illegal drugs on the premises and because his pre-paid rental period had elapsed."). When Google exercised its rights to monitor content on its system, terminated Miller's account, generated a report containing the two child pornography images detected, and turned it

over to NCMEC, the Defendant lost any claim that concepts of real or personal property law support his asserted privacy interests in the material that he seeks to suppress.

Neither has the Defendant shown that his claimed expectation of privacy draws legitimacy from "understandings that are recognized and permitted by society." In considering claims that an individual had a reasonable expectation of privacy in a hotel room and its contents, the Sixth Circuit has recognized that society generally would not recognize as reasonable any claimed expectation of privacy in a rented dwelling such as a hotel room when a third party has taken lawful steps to take control over that dwelling; an individual may lack a legitimate expectation of privacy in an otherwise protected place even where the private party has not yet exercised its right to exclude, as when the check-out time expires with no agreement or practice of extending the rental period. *Lanier*, 636 F.3d at 232-33. In this case, Google affirmatively exercised its rights to control the Defendant's account, by monitoring and then terminating his account, and submitting the two images to the CyberTipline. Detective Schihl's subsequent "intrusion," which was limited to the review of these two image files (each of which had a filename that was highly suggestive of child pornography) did not invade any expectation of privacy that society would be prepared to recognize as objectively reasonable. Under the facts of this case, Detective Schihl's review of the two images that the Defendant seeks to suppress did not constitute a search subject to Fourth Amendment scrutiny.

f. Law enforcement acted in good faith

Alternatively, even if Detective Schihl's review constituted a Fourth Amendment search, and even if that search was unreasonable, the good faith exception to the Fourth

Amendment's exclusionary rule applies here. This exception originated in *United States v. Leon*, 468 U.S. 897 (1984), in which the Supreme Court explained, "[i]f the purpose of the [Fourth Amendment's] exclusionary rule is to deter unlawful police conduct, then evidence obtained from a search should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment." 468 U.S. at 919 (*quoting United States v. Peltier*, 422 U.S. 531, 542 (1975)). The exclusionary rule serves to deter "deliberate, reckless, or grossly negligent conduct." *Herring v. United States*, 555 U.S. 135, 144 (2009). So, 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." *Id*.

There is no evidence of deliberate, reckless, or grossly negligent conduct by law enforcement in this case. When Detective Schihl reviewed the two images – which were included in the CyberTipline report – and subsequently acquired a search warrant for the contents of the Defendant's gmail account, he had no reason to believe that simply viewing the images constituted a violation of the Defendant's Fourth Amendment rights. There was no information readily apparent on the face on the CyberTipline report that indicated that the content of the images had not previously been reviewed; rather, as explained herein, the information provided suggested otherwise.

g. Not all the evidence is "fruit of the poisonous tree"

Finally, the Defendant seeks to suppress "any evidence obtained either directly or indirectly as a result of the illegal searches … and seizure of the contents of email

account miller694u@gmail.com and email attachments." [R. 27: Motion at 109.] As noted above, Detective Schihl obtained three different search warrants in this case: for the contents of the gmail account, the Defendant's residence, and the electronic media seized therefrom. To the extent that the Defendant claims that Detective Schihl's review of the images tainted the later searches of his home or the digital media, that claim likewise fails.

The Sixth Circuit and other circuits have adopted an interpretation of the "independent source" doctrine that incorporates consideration of the sufficiency of an affidavit to determine if probable cause exists without the tainted information. *See United States v. Jenkins*, 396 F.3d 751, 757-61 (6th Cir. 2005). Applying this approach to the present case, once the allegedly tainted information related to Schihl's review of the images is eliminated, the focus is on the written affidavits, which in this case provide sufficient probable cause for the warrants for the Defendant's home and the electronic media seized therefrom.

III. Conclusion

Based upon the foregoing, the Defendant's motion to suppress should be denied.

Respectfully Submitted,

CARLTON S. SHIER, IV
ACTING UNITED STATES ATTORNEY

By: /s/ Elaine K. Leonhard
Assistant United States Attorney
207 Grandview Drive
Ft. Mitchell, Kentucky 41017
Phone: (859) 652-7035
Fax: (859) 655-3211

CERTIFICATE OF SERVICE

On February 28, 2017, I electronically filed this document through the CM/ECF system, which will send the notice of electronic filing to all counsel of record.

/s/ Elaine K. Leonhard
Assistant United States Attorney