

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS**

UNITED STATES OF AMERICA,

Plaintiff,

vs.

Case No. 13-10176-01-EFM

WALTER ACKERMAN,

Defendant.

MEMORANDUM AND ORDER

This matter comes before the Court on Defendant Walter Ackerman's Motion to Suppress (Doc. 13). Defendant seeks the suppression of an email and its attachments arguing that they were obtained through an illegal search and seizure. Defendant also seeks the suppression of certain statements asserting that he should have been given a *Miranda* warning because his meeting with law enforcement was a custodial interrogation. The Court held a hearing on May 19 and 20, 2014. Because the Court finds that AOL and the National Center for Missing and Exploited Children ("NCMEC"), the parties who searched Defendant's emails, are not state actors, the Fourth Amendment is inapplicable to their conduct in this case. In the alternative, even if NCMEC's search could be considered a government search, NCMEC's search did not exceed the scope of AOL's search in such a way that would be constitutionally significant. Finally, with regard to Defendant's statements to law enforcement, the Court finds

that Defendant's meeting was not a custodial interrogation, and thus, the Court will not suppress Defendant's statements. Accordingly, the Court denies Defendant's motion.

I. Factual and Procedural Background¹

A. Background on AOL

AOL, formerly known as American Online and Quantum Computer Services, is an internet service provider. As part of AOL's services, it offers free and premium (paid) email service to its users. To use AOL's services, AOL requires its users to agree to its Terms of Service ("TOS"). As of April 19, 2013, these TOS state that a user must:

- a. Comply with applicable laws and regulations and not participate in, facilitate, or further illegal activities;
...
- d. Not post content that contains explicit or graphic descriptions or accounts of sexual acts or is threatening, abusive, harassing, defamatory, libelous, deceptive, fraudulent, invasive of another's privacy, or tortious;
- e. Not engage in an activity that is harmful to us or our customers, advertisers, affiliates, vendors, or anyone else
...

To prevent violations and enforce this TOS and remediate any violations, we can take any technical, legal, and other actions that we deem, in our sole discretion, necessary and appropriate without notice to you.

An AOL user is required to agree to these TOS if they have an account with AOL. If AOL makes changes to the TOS, AOL sends an email to the user's email address stating the date that the new TOS will become effective. A user's log-in after the effective date implies consent to accept the new TOS.

¹ The following facts are based on the parties' written briefs and from testimony given at the suppression hearing held on May 19 and 20, 2014. The Court allowed NCMEC to file an amicus brief in this case. Counsel representing NCMEC appeared at the suppression hearing and provided a brief summation of NCMEC's position at the close of the government's and Defendant's evidence.

AOL employs an Image Detection and Filtering Process (“IDFP”), an automated program that systematically scans emails sent, saved, or forwarded from an AOL account to scan for malware, viruses, and illegal images such as child pornography. As part of this IDFP, AOL developed and maintains a database of hash values associated with child pornography. A hash value is derived from a specific digital file and is an alphanumeric sequence that is unique to that digital file.

Greg Phillips, AOL’s Senior Technical Security Investigator, testified as to how AOL developed this database of hash values. Historically, people would report to AOL when they would receive a file containing child pornography. AOL’s graphic review team would then look at that file to determine if the image met the definition of child pornography. Once AOL made this determination, it would take a hash value of that file (child pornography image) and add it to its database. AOL uses a MD5 hash value. The MD5 hash value contains approximately thirty digits, and the hash value is derived from the image based on a computation from an algorithm. A hash value is sometimes referred to as a digital fingerprint because the hash value is unique to a specific digital file. Any alteration of the image or file would result in a different hash value.

AOL does not obtain hash values from any outside company and has only developed its database of hash values from the graphics review team at AOL. AOL’s database has grown from zero to approximately 100,000 hash values. AOL does not retain the images of child pornography.

When AOL, through its IDFP, detects a file that matches a hash value in its database, the email is captured, and AOL terminates the user’s account pursuant to its TOS. AOL then generates a report and creates a new email to send to NCMEC via NCMEC’s CyberTipline. AOL’s email and report includes the intercepted email and attached file(s); the user’s account

information; and the IP address of where the member was logged on. By statute, 18 U.S.C. § 2258A(a)(1), an internet service provider (such as AOL) is required to report to NCMEC's CyberTipline any child pornography it "obtains actual knowledge of . . . as soon as reasonably possible."

Mr. Phillips testified that AOL utilizes its IDFP to protect its business interests. He stated that AOL wants to protect its reputation and brand because it does not want to be associated with illegal activity. In addition, AOL wants its customers to stay with AOL and feel safe and secure.

B. Background on National Center for Missing and Exploited Children ("NCMEC")

NCMEC is a 501(c)(3) nonprofit organization established in 1984. Its headquarters are in Alexandria, Virginia. John Shehan, Executive Director of the Exploited Child Division at NCMEC, testified that NCMEC's mission is to help reunite families with missing children, reduce child sexual exploitation, and prevent child victimization. NCMEC receives its funding through federal grants, individual donations, and in-kind donations. Approximately seventy-five percent of its funding comes from federal grants, and twenty-five percent from private donations. The in-kind donations are calculated on top of that percentage.

NCMEC has five main divisions: missing children; child sexual exploitation; training; child safety and prevention; and child victim and family support. In the child sexual exploitation division, there are three main programs: the CyberTipline, the child victim identification program, and net smarts 411 (an internet safety help desk and hotline). NCMEC's CyberTipline is at issue in this case.

1. NCMEC's CyberTipline

NCMEC launched the CyberTipline in March 1998. It was created through a generous donation from a private company, and it was created to provide a central location to report information regarding child sexual exploitation. The CyberTipline provides online users, members of the general public, and internet service providers a way to report suspected child sexual exploitation either online or through its 24-hour toll free hotline. About one thousand of the approximate 5,000 internet service providers in the United States have a reporting relationship with the NCMEC. These internet service providers submit their CyberTipline reports online through the NCMEC's secure portal. By statute, 18 U.S.C. §2258A(c)(1), NCMEC must forward any report made through the CyberTipline (under 18 U.S.C. 2258A(a)1(a)) to an appropriate law enforcement agency.²

After a report is made to the CyberTipline, a NCMEC analyst will review the information that was provided. The analyst views the file to determine if it contains child pornography. If so, there is a section on the report stating "Child Pornography (Confirmed)." The analysis, however, does not include any information or description about the images. The NCMEC analyst also takes the IP address and the email address provided in the CyberTipline report and uses publicly available search engines and tools in an effort to identify the sender's geographic location. After the analyst finds the geographic location and completes the report, the report is made accessible to law enforcement. NCMEC sends a daily email that provides a brief summary of the reports just made available. Law enforcement then uses NCMEC's secure, virtual private

² When NCMEC launched its CyberTipline, there was not a reporting statute.

network to access and obtain the report. Access is limited through the virtual private network on a report by report and recipient by recipient basis.

C. Facts and Procedural History as to Defendant Walter Ackerman

Defendant Walter Ackerman was a user of AOL Mail and used the screen name “plains66952.” On April 22, 2013, AOL’s IDFP detected an email sent by “plains66952@aol.com” to “zoefeather@riseup.net,” which contained a hash value of previously identified child pornography. As a result of AOL’s discovery that Defendant violated AOL’s TOS, AOL immediately terminated Defendant’s account.

AOL submitted a report to NCMEC on April 23, 2013. This report included the email header information, including the involved usernames, the IP address of the sender, and the IDFP hash value. After receiving the report, NCMEC confirmed the presence of child pornography. After conducting its investigation and establishing that the likely geographic location of the sender was in Kansas, NCMEC forwarded the tip to the Kansas Internet Crimes Against Children (“ICAC”) Task Force in the Wichita/Sedgwick County Exploited and Missing Children’s Unit (“EMCU”). Detective Wright, who is assigned to ICAC in Wichita, Kansas, requested the assistance of Special Agent Rick Moore (“SA Moore”) of the Department of Homeland Security.

On May 17, 2013, SA Moore accessed and reviewed the CyberTipline report. SA Moore then began his investigation and started with confirmation of the ISP for the identified IP address. He issued a subpoena for that IP address as it was utilized on April 22, 2013. On May 21, 2013, SA Moore received the subscriber information from the ISP, which identified the IP address assigned to Michelle Ackerman in Lebanon, Kansas. The ISP also showed an additional authorized contact of Walter Ackerman.

On May 22, 2013, SA Moore served AOL with a preservation letter for email account plains66952@aol.com. On May 24, 2013, SA Moore applied for and obtained a search warrant for Defendant's residence in Lebanon, Kansas. On May 30, 2013, SA Moore executed the search warrant at Defendant's residence. Defendant's wife was at home, but Defendant was not. Defendant's wife stated that Defendant was at work in Beloit, Kansas. In executing the search warrant, agents found multiple digital items that revealed the presence of child pornography.

On that same day, SA Moore and SA Erin Russell went to Defendant's work. They were dressed in civilian clothes, and they covered their badges and guns. The agents contacted the manager and identified themselves by showing their credentials. They asked if they could speak to Defendant in a private area. The agents identified themselves to Defendant by showing him their credentials. SA Moore asked Defendant if he would speak to him in the private room that the manager had provided. Defendant said yes.

When walking into the private room, SA Moore activated a recorder. Defendant did not notice the recorder until approximately twenty-two minutes into the interview. The interview is approximately seventy-five minutes long, and all of it is recorded. During the interview, the agents informed Defendant that he was not under arrest. SA Moore then informed Defendant that they had conducted a search warrant at his house. Defendant indicated that he knew what the search warrant would be related to by stating "child pornography." SA Moore informed Defendant several times throughout the interview that Defendant was not under arrest. SA Moore also concluded the interview by stating that Defendant was not under arrest and that he would be providing the information to prosecutors for a later determination regarding charges.

On November 6, 2013, a grand jury indicted Defendant on one count of distribution of child pornography, a violation of 18 U.S.C. § 2252(a)(2), occurring on or about April 22, 2013,

and one count of possession of child pornography, a violation of 18 U.S.C. § 2252(a)(4)(B), occurring on or about May 30, 2013. Defendant has now filed a Motion to Suppress (Doc. 13). The Court held a hearing on May 19 and 20, 2014.

II. Analysis

Defendant seeks the suppression of the email and its attachments contending that it was obtained through an illegal search and seizure. Defendant also seeks suppression of his statements to police officers at a meeting at his work. The Court will address each issue in turn.

A. *Suppression of Defendant's Email and the Contents of any Attachments to that Email*

The government brings up approximately three broad issues encompassing six questions surrounding the alleged search and seizure of Defendant's email document. The Court will not address all of these issues. Instead, the Court will assume, without deciding, that Defendant has a reasonable expectation of privacy in his email. The Court will then address two issues surrounding AOL's and NCMEC's conduct in this case. The first issue is whether AOL or NCMEC should be considered a state actor such that Fourth Amendment principles are applicable. The second issue is even if NCMEC could be considered a state actor, whether NCMEC's search expanded AOL's search in a constitutionally significant way.

1. **AOL and NCMEC are not state actors such that Fourth Amendment principles are applicable.**

The Fourth Amendment is "wholly 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."³ "A search by a private

³ *United States v. Benoit*, 713 F.3d 1, 9 (10th Cir. 2013) (citing *United States v. Jacobsen*, 466 U.S. 109, 113-14 (1984)).

person becomes a government search if the government coerces, dominates, or directs the actions of a private person conducting the search.”⁴ To determine whether a search by a private person becomes a government search, there is a two-part inquiry: “1) whether the government knew of and acquiesced in the intrusive conduct, and 2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends.”⁵ With regard to the first prong, knowledge and acquiescence “encompass the requirement that the government agent must also affirmatively encourage, initiate, or instigate the private action.”⁶ As to the second part of the test, the Court does not simply inquire as to whether police benefitted from the private party’s conduct but instead must determine whether the private party had a “legitimate, independent motivation” in performing the search.⁷ Both parts of the test must be fulfilled before the private search will be considered a government search.⁸ “The totality of the circumstances guides the court’s determination as to whether the two-part inquiry has been met.”⁹

a. AOL is not a state actor and the Fourth Amendment is not applicable.

The first part of the test requires knowledge and acquiescence by a government official. Defendant argues that AOL’s search is a government search and attempts to rely upon Congressional testimony for this proposition. It appears that Defendant is suggesting that the government (through Congress) pressured internet service providers, like AOL, to implement

⁴ *United States v. Souza*, 223 F.3d 1197, 1201 (10th Cir. 2000) (quotation marks and citation omitted).

⁵ *Id.* (citing *Pleasant v. Lovell*, 876 F.2d 787, 796 (10th Cir. 1989)).

⁶ *United States v. Smythe*, 84 F.3d 1240, 1243 (10th Cir. 1996).

⁷ *United States v. Poe*, 556 F.3d 1113, 1124 (10th Cir. 2009) (citing *Smythe*, 84 F.3d at 1240). *See also Souza*, 223 F.3d at 1202.

⁸ *Souza*, 223 F.3d at 1201.

⁹ *Id.*

technology to gather information about child pornography to assist law enforcement. Thus, Defendant contends that a government official had knowledge of or acquiesced in AOL's conduct because the government encouraged the implementation of technology.

As an initial matter, the Court questions the appropriateness of Defendant's reliance on hearsay Congressional testimony for this proposition. More substantively, however, Congressional hearings regarding internet service provider's implementation of technology to detect child pornography does not demonstrate participation or knowledge of a government official in AOL's search in this case. It simply demonstrates that members of Congress, i.e., the government, may be generally aware of internet service providers' technology in searching for child pornography.

Although Congress enacted 18 U.S.C. § 2258A(a) to require internet service providers to report discovered child pornography, 18 U.S.C. § 2258A(f) specifically states that an internet service provider is *not required to monitor* its users or affirmatively seek child pornography transmitted by its users. Compliance with a reporting statute is quite different than a government agent directing one's actions. In addition, although the Tenth Circuit has not specifically addressed this question, several other circuit courts of appeal have determined that § 2258A(a)'s (or the predecessor statute to § 2258A) reporting requirement does not transform an internet service provider's private actions into government actions.¹⁰

¹⁰ See *United States v. Stevenson*, 727 F.3d 826, 829-30 (8th Cir. 2013) (determining that 18 U.S.C. 2258A's reporting requirements did "not transform an Internet 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, 637-38 (1st Cir. 2012) (addressing the predecessor statute, 42 U.S.C. § 13032(b)(1), and finding that although the statute required *Yahoo!* to report child pornography, there was no obligation to search for it and therefore the government did not exercise control over *Yahoo!*'s actions); *United States v. Richardson*, 607 F.3d 357, 364-67 (4th Cir. 2010) (addressing the predecessor statute, 42 U.S.C. § 13032(b)(1), and finding that "the statutory provision pursuant to which AOL reported [the defendant's] activities did not effectively convert AOL into an agent of the Government for Fourth Amendment purposes.").

Furthermore, there is no evidence to suggest that the government and law enforcement knew of or acquiesced in AOL's conduct with regard to the search of this Defendant's email in this case in any way. Here, AOL, through its IDFP, simply compared the hash value of a transmitted file to its database of hash values previously associated with child pornography with no government involvement. Thus, Defendant has no evidence with regard to the first prong of the Tenth Circuit's test that the government knew of or acquiesced in AOL's conduct.

As to the second prong—whether AOL intended to assist law enforcement or further its own ends—AOL's representative testified that AOL employs the IDFP to protect its own business interest and reputation.¹¹ Specifically, AOL does not want to be associated with illegal activity and wants to keep its customers safe and secure. Thus, with regard to the second prong, the evidence demonstrates that AOL was furthering its own ends when performing the search and had a legitimate, independent motivation in performing the search.¹² Accordingly, AOL is not a state actor, and Fourth Amendment principles are inapplicable to its conduct.

b. NCMEC is not a state actor and the Fourth Amendment is not applicable.

Defendant also contends that NCMEC's conduct constitutes a government search and relies heavily on an opinion from the District of Massachusetts, *United States v. Keith*,¹³ for this proposition. In the *Keith* decision, the court analyzed NCMEC's conduct under the First Circuit's three-factor test for determining whether a private party effectively acts as a

¹¹ Both prongs of the test must be met to establish a government search. *Souza*, 223 F.3d at 1201. Although the Court has found that Defendant cannot meet the first prong, the Court will still address the second prong.

¹² A recent case from the District of Massachusetts addressed AOL's role and also found that "AOL is motivated by its own wholly private interests in seeking to detect and deter the transmission of child pornography through its network facilities." *United States v. Keith*, 980 F. Supp. 2d 33, --, 2013 WL 5918524, at *5 (D. Mass. 2013).

¹³ *Id.*

government agent in conducting a search.¹⁴ The First Circuit’s three-part test requires a court to consider: “(1) the extent of the government’s role in instigating or participating in the search; (2) the government’s intent and the degree of control it exercises over the search and the private party; and (3) the extent to which the private party aims primarily to help the government or to serve its own interests.”¹⁵

As to the first factor, the District of Massachusetts found that because Congress authorizes and funds the CyberTipline that the government instigated the search.¹⁶ Regarding the second factor, the court determined that 18 U.S.C. § 2258A(c)(1)-(2) requires NCMEC to report discovered child pornography to law enforcement, and thus the government “controlled” NCMEC’s search.¹⁷ Finally, as to the third factor, the court found that NCMEC’s CyberTipline served no private purpose for NCMEC, separate from assisting law enforcement.¹⁸ Thus, the court concluded that “NCMEC’s examination of the contents of that emailed image file violated the Fourth Amendment because it was not authorized by a duly issued warrant (or by some constitutionally adequate substitute).”¹⁹

The Court finds the *Keith* court’s reasoning as to whether NCMEC’s conduct constitutes government action inapplicable here. Not only does the Court disagree with several of the *Keith* court’s factual conclusions, but the *Keith* decision employed a three-part test required by the

¹⁴ *Id.* at *5 (citing *United States v. Silva*, 554 F.3d 13, 18 (1st Cir. 2009)). The Tenth Circuit has a two-factor test, and the differences between the Tenth and First Circuit’s test will be discussed below.

¹⁵ *Id.* (citing *Silva*, 554 F.3d at 18).

¹⁶ *Id.* at *6.

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ *Id.* at *12.

First Circuit. This Court must employ the Tenth Circuit’s two-part test. Although the elements are similar, it appears that the Tenth Circuit requires more specific government involvement in the knowledge or the participation of the search.²⁰ For review, the two-part test in the Tenth Circuit is “1) whether the government knew of and acquiesced in the intrusive conduct, and 2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends.”²¹

As to the first element of the test, the majority of the cases previously considered by the Tenth Circuit involved a government agent present at the time the private party performed the search. With the exception of one case, the Tenth Circuit concluded that the private party’s search did not implicate Fourth Amendment principles because the government agent merely acted as a witness and did not encourage or instigate the search.²² Thus, generally, even though a government agent was present at the search, the private party’s search remained private and not one on behalf of the government.

²⁰ See, e.g., *Smythe*, 84 F.3d at 1243 (requiring under the first element of the test that the government affirmatively encourage or instigate the action). See also *United States v. Pervaz*, 118 F.3d 1, 6 (1st Cir. 1997) (noting the Tenth Circuit’s standard for determining government action and stating that “[w]e think that any specific ‘standard’ or ‘test’ is likely to be oversimplified or too general to be of help, and that all of the factors mentioned by the other circuits may be pertinent in different circumstances . . .”).

²¹ *Souza*, 223 F.3d at 1201.

²² See *Smythe*, 84 F.3d at 1243 (determining that a bus station’s employee’s search was a private one because although police were present they did not encourage, assist, or touch the package in any way and the employee had an independent basis for opening the package); *United States v. Leffall*, 82 F.3d 343, 349 (10th Cir. 1996) (finding that an airline employee’s opening of a package, while a police officer acted as a witness, did not amount to government action because the officer did not encourage the search and the airline employee acted in his employer’s interest in opening the package). See also *Benoit*, 713 F.3d at 9-10 (concluding that the first “search,” one without a police officer present, was a private one because there was no knowledge or acquiescence by the government and the second search, one with a police officer present, was not a government search because the officer did not assist, encourage, or direct the private party in showing the video).

In *United States v. Souza*, the Tenth Circuit determined that a search by a UPS employee was in reality a government search because the DEA agents present at the scene identified the item to be searched, encouraged the employee to open the item several times, and then helped the employee open the item by cutting open the box to look at its contents. *Souza*, 223 F.3d at 1201-02.

In *United States v. Poe*,²³ a government agent was not present when bounty hunters entered a residence and discovered illegal items.²⁴ The Tenth Circuit dismissed the defendant's argument that state involvement occurred because the state of Oklahoma was involved in the bail bonds industry and conferred the power of arrest to bounty hunters.²⁵ The court noted that "involvement in the bail bonds *industry* is insufficient to satisfy this inquiry; we require knowledge of or acquiescence in the challenged search."²⁶ Thus, the Tenth Circuit found that "after-the-fact involvement of the police does not implicate the Fourth Amendment."²⁷

In this case, there was no government agent present at the time NCMEC conducted its search. NCMEC does not have any law enforcement employees. Law enforcement was not involved in the processing of the CyberTipline report. Law enforcement did not, and cannot, become involved until the report is made available through NCMEC's virtual private network. And although NCMEC knows when the reports have been reviewed or downloaded by law enforcement agencies, NCMEC does not know anything more about when, or if, law enforcement agencies decide to investigate the report. There is accordingly no evidence that a government agent affirmatively encouraged, initiated, or instigated NCMEC's review of AOL's report.

Similar to the *Poe* case, a government agent did not know of or directly participate in NCMEC's review of AOL's report. It was only after NCMEC's review and upload of the

²³ 556 F.3d 1113.

²⁴ *Id.* at 1118-19.

²⁵ *Id.* at 1124.

²⁶ *Id.* (emphasis in original).

²⁷ *Id.*

emailed file that a government agent, SA Moore, became involved in the case. And although 18 U.S.C. § 2258A(c)(1) requires NCMEC to forward “each report made under subsection (a)(1) to any appropriate law enforcement agency designated by the Attorney General under subsection (d)(2),” the mere fact that a statute requires reporting of illegal conduct to law enforcement does not demonstrate government control.²⁸ As noted above, compliance with a reporting statute is an insufficient basis for finding knowledge of or acquiescence of the government in the challenged search.

With regard to the second part of the test,²⁹ the evidence demonstrates that NCMEC is a private, non-profit corporation with the mission of reuniting families with missing children, reducing child sexual exploitation, and preventing child victimization. NCMEC operates its CyberTipline to provide the public a way to report suspected child sexual exploitation. Although NCMEC’s CyberTipline also benefits law enforcement, the Court must determine whether the private party had a “legitimate, independent motivation” in performing the search.³⁰ And the Court answers this question in the affirmative. Mr. Shehan testified that the CyberTipline was created to provide a central location to report information regarding child sexual exploitation. And although CyberTipline’s reports are provided to law enforcement and ultimately helps law enforcement in combatting child pornography, Mr. Shehan stated that NCMEC operates the CyberTipline to provide a community service and to protect children.

²⁸ See, e.g., *Poe*, 556 F.3d at 1124 (noting that the state’s involvement in the bail bonds industry was insufficient to establish knowledge and acquiescence).

²⁹ Both prongs of the test must be met to establish a government search. *Souza*, 223 F.3d at 1201. Although the Court has found that Defendant cannot meet the first prong, the Court will also address the second prong.

³⁰ See *Poe*, 556 F.3d at 1124 (“We do not inquire if the police benefitted from the private conduct, but if the [private party] had a ‘legitimate, independent motivation’ to conduct the search.”) (citation omitted).

Indeed, NCMEC's stated mission is to help reunite families with missing children, reduce child sexual exploitation, and prevent child victimization. Mr. Shehan also stated that the information reported through the CyberTipline helps NCMEC's prevention and educational department. NCMEC, in analyzing the reports, can identify trends and thus tailor its child exploitation prevention messages to the general public. This testimony compels a finding that NCMEC has a legitimate, independent basis in operating the CyberTipline and is contrary to the *Keith* court's conclusion that the NCMEC's CyberTipline serves no private purpose separate from assisting law enforcement.³¹

In addition, it appears as though NCMEC would have conducted the search even if law enforcement did nothing with the information which further demonstrates a legitimate, independent motivation for NCMEC's search.³² Mr. Shehan testified that although NCMEC knows when the reports have been reviewed or downloaded by law enforcement agencies, NCMEC does not know whether law enforcement agencies decide to investigate the report. Thus, the second part of the test is not met. Under the totality of the circumstances, the Court concludes that NCMEC's search is not a government search and does not implicate Fourth Amendment principles.

2. Even if the Court did consider NCMEC to be a state actor, NCMEC's actions did not expand AOL's search in a constitutionally significant way.

Alternatively, even if the Court were to agree with Defendant that NCMEC should be considered a government actor, the Court would still have to consider whether NCMEC's conduct is subject to Fourth Amendment principles. Two United States Supreme Court cases are

³¹ *Keith*, 2013 WL 5918524, at *6.

³² *Poe*, 556 F.3d at 1124 (noting that the private party "would have conducted the search even if the police had not responded to their call.") (quotation marks and citation omitted).

relevant to the discussion. In *Walter v. United States*,³³ a package containing 8-millimeter film was mistakenly delivered to a private company.³⁴ The employees of the private company opened the package and found boxes of film which had labeling on its side, suggesting obscene material on the film.³⁵ The private party attempted to view the film by holding it to the light, but they were unsuccessful and then called the FBI.³⁶ After the FBI picked up the package, FBI agents viewed the films with a projector.³⁷ A plurality of the court determined that the private party's search only revealed boxes with labels suggesting that those boxes *may* contain obscene material, but the FBI's viewing of the film significantly expanded the search and must be characterized as a separate search.³⁸ Because the FBI significantly expanded the private party's search, the plurality concluded that the government's search violated the Fourth Amendment.³⁹

The other relevant case is *United States v. Jacobsen*.⁴⁰ In that case, a private party (FedEx) opened a box that had been damaged during transport and discovered what appeared to be illegal drugs.⁴¹ The private party then put the contents of the box back inside and contacted the DEA.⁴² The DEA then opened the box and removed the illegal drugs.⁴³ The United States

³³ 447 U.S. 649 (1980).

³⁴ *Id.* at 651.

³⁵ *Id.* at 651-52.

³⁶ *Id.* at 652.

³⁷ *Id.*

³⁸ *Id.* at 657.

³⁹ *Id.* at 657-58.

⁴⁰ 466 U.S. 109 (1984).

⁴¹ *Id.* at 111.

⁴² *Id.*

Supreme Court found that the government did not perform a search to which the Fourth Amendment was applicable because the private party had already performed the search and the government did not learn anything that had not been previously learned by the private party.⁴⁴ The court noted that to determine whether the Fourth Amendment is applicable to the government's search after a private party initially conducts the search, a court must consider the degree to which the government's conduct exceeded the private party's search.⁴⁵

The Court concludes that the facts in this case are more analogous to the facts in *Jacobsen* than the facts in *Walter*.⁴⁶ The key issue is determining the degree to which NCMEC's actions exceeded the scope of AOL's search. In this case, a hash value is significantly different than a label on a file. A label does not tell you anything about the file—except for what the file *may* contain. In contrast, a hash value is much more specific. As noted above, a hash value is derived from a specific digital file and is an alphanumeric sequence that is unique to that digital file. Any identical copy of that 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. AOL only retains a database of hash values already associated with child pornography. AOL's discovery of an email containing a hash value that matched its database of

⁴³ *Id.* at 111-12.

⁴⁴ *Id.* at 117 (“The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy had not already been frustrated.”).

⁴⁵ *Id.* at 115 (“The 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.”) (relying on *Walter*, 447 U.S. 649).

⁴⁶ The Court recognizes that, in *Keith*, the District of Massachusetts reached the opposite conclusion. *See Keith*, 2013 WL 5918524, at *8 (finding that *Jacobsen* was inapposite and *Walter* was the better analogy because NCMEC expanded the review because AOL's matching of hash values “does not itself convey any information about the contents of the file.”). For the reasons stated above, the Court disagrees with the *Keith* court's reasoning about AOL's hash values.

hash values, therefore, would convey that the file contains child pornography. NCMEC, in viewing the hashed file, did not learn anything additional that had not been previously learned by AOL. Thus, the opening of the file by NCMEC did not exceed the scope of AOL's search to the degree that it would be constitutionally significant. Accordingly, even if the Court considers NCMEC's search a government search, the Fourth Amendment would remain inapplicable to its conduct.

Finally, even if NCMEC's opening of the file could be considered an additional intrusion, the Court would still have to consider whether that intrusion/search violated Defendant's Fourth Amendment rights. In *Jacobsen*, the Supreme Court considered whether the "additional intrusion" of the FBI performing a field test on the white powder, which "exceeded the scope of the private search," was an unlawful search or seizure under the Fourth Amendment.⁴⁷ The court concluded that the chemical test that "merely disclose[d] whether or not a particular substance [was] cocaine d[id] not compromise any legitimate interest in privacy."⁴⁸ The court also stated that "government conduct that can reveal whether a substance is cocaine, and no other arguably 'private' fact, compromises no legitimate privacy interest."⁴⁹ Here, the "field test" had already been performed by AOL when its IDFP identified the hash value (child pornography) in Defendant's email. NCMEC's opening of the file would simply confirm that the file contains child pornography (which is illegal), and the opening of the file would not implicate any other legitimate privacy interest.

⁴⁷ *Jacobsen*, 466 U.S. at 122.

⁴⁸ *Id.* at 123. *See also United States v. Villa*, 348 F. App'x 376, 378 (10th Cir. 2009) (noting that "[t]here is no legitimate interest in possessing illegal substances; therefore, police conduct that only reveals the presence of illegal substances does not 'compromise any legitimate interest in privacy.'" (citing *Jacobsen*, 466 U.S. at 123).

⁴⁹ *Id.*

In sum, the Court concludes that AOL's search was not a government search. In addition, NCMEC's search was not a government search. And, alternatively, even if NCMEC's search could be considered a government search, NCMEC's search did not exceed the scope of AOL's search in such a way that would be constitutionally significant. Accordingly, the Court denies Defendant's motion to suppress Defendant's email and its attachments.

B. Suppression of Defendant's Statements

Defendant asserts that he should have been given a *Miranda* warning when he was questioned at work by government agents because the meeting was a custodial interrogation. "For *Miranda*'s protections to apply, custodial interrogation must be imminent or presently occurring."⁵⁰ "*Miranda* is therefore only applicable when (1) the suspect is in custody, and (2) any questioning meets the legal definition of interrogation."⁵¹ To determine whether an individual is in "custody," an individual "must be under formal arrest or have his freedom of action . . . curtailed to a degree associated with formal arrest."⁵² The "custody" determination is an objective one, and the inquiry is "whether a reasonable person in the suspect's position would have understood his situation . . . as the functional equivalent of formal arrest."⁵³ "To determine whether a law enforcement officer engaged in "interrogation," the court "must inquire whether law enforcement officials should have known that their words or actions—whether framed as a

⁵⁰ *United States v. Cash*, 733 F.3d 1264, 1276 (10th Cir. 2013) (citation omitted).

⁵¹ *Id.* at 1276-77 (quotation marks and citation omitted).

⁵² *Id.* at 1277 (quotation marks and citation omitted).

⁵³ *United States v. Hudson*, 210 F.3d 1184, 1190 (10th Cir. 2000) (quotation marks and citation omitted).

question or not—were reasonably likely to elicit an incriminating statement.”⁵⁴ This inquiry is also objective, and the focus is not on the subjective intent of the officer.⁵⁵

Initially, Defendant asserted in his brief that he was told that he would be arrested if he did not cooperate. At the hearing, the evidence demonstrated otherwise. Special Agent Moore recorded the meeting, and SA Moore told Defendant at the very beginning of the meeting: “You’re not under arrest. We’re not here to arrest you or anything. But I’d like to ask you why would you think we would be here talking to you.”⁵⁶ SA Moore then told Defendant that they had just conducted a search warrant at his house, Defendant then said that he had been “getting bored,”⁵⁷ and he had been trading pictures on the internet. He said that “he knew what it is, but he didn’t like to say it.”⁵⁸ After the female agent left the room, Defendant stated “child pornography” without any prompting. Defendant also explained what he believed child pornography was.

Throughout the approximate hour-long meeting, Defendant was told several times that he was not under arrest. Finally, SA Moore told Defendant at the end of the interview that he was not under arrest. The meeting was conversational, and it was not the functional equivalent of a formal arrest. Thus, the meeting was not a custodial interrogation, and the Court denies Defendant’s motion to suppress his statements to law enforcement officers.

⁵⁴ *Cash*, 733 F.3d at 1277.

⁵⁵ *Id.*

⁵⁶ Government’s Exhibit 4, Audio Interview.

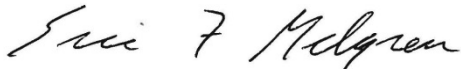
⁵⁷ *Id.*

⁵⁸ *Id.*

IT IS THEREFORE ORDERED that Defendant Walter Ackerman's Motion to Suppress (Doc. 13) is hereby **DENIED**.

IT IS SO ORDERED.

Dated this 1st day of July, 2014.


ERIC F. MELGREN
UNITED STATES DISTRICT JUDGE