IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

UNITED STATES OF AMERICA, *Plaintiff,* vs. WALTER ACKERMAN, *Defendant.*	Case No. 13-10176-01-EFM

MEMORANDUM AND ORDER

This matter is again before the Court on Defendant Walter Ackerman's Motion to Suppress (Doc. 19). Defendant seeks the suppression of an email and its attachments arguing that they were obtained through an illegal search and seizure. This Court originally denied Defendant's Motion to Suppress finding that AOL and the National Center for Missing and Exploited Children ("NCMEC"), the parties who searched Defendant's emails, were not state actors. Thus, the Fourth Amendment was inapplicable to their conduct in this case. In the alternative, this Court found that 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.

On appeal, the Tenth Circuit Court of Appeals reversed and found that NCMEC was a governmental entity. In the alternative, the circuit found that NCMEC acted as a government

agent. Finally, the Tenth Circuit found that NCMEC's search expanded AOL's private search. Thus, the Tenth Circuit remanded the case. In remanding the case, the Tenth Circuit noted that "hard questions remain to be resolved on remand."

The Court allowed additional briefing by both the government and Defendant. On September 19, 2017, the Court held a hearing. After considering the parties' arguments, the Court finds that Defendant did not have an objectively reasonable expectation of privacy in his email and the four attachments. Thus, NCMEC's search did not violate his Fourth Amendment rights. In the alternative, even if Defendant did have an expectation of privacy and his Fourth Amendment rights were violated, suppression is unwarranted due to the good faith exception. Thus, the Court denies Defendant's Motion to Suppress.

I. Factual and Procedural Background[1]

Defendant Walter Ackerman was a user of AOL Mail and used the screen name "plains66952." 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
> . . .

[1] A more detailed recitation of facts is set forth in this Court's previous Order. *See* Doc. 37. Only the facts pertinent to the issues in this Order will be set forth here. Some of these facts are taken from the evidence and testimony in the original hearing on Defendant's motion on May 19 and 20, 2014. Other facts are from this Court's and the Tenth Circuit Court of Appeal's previous opinions. During the hearing in September 2017, the Court did not allow any additional evidence but only heard arguments related to the evidence already before the Court.

> 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.

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. If an email user sends an email with images, either as an attachment to that email or embedded in the body of the email, AOL's IDFP compares those images with previously identified child pornography images. If a match occurs, AOL automatically terminates the user's account and the user can no longer access his email account.

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. AOL's detection system identified one of the four images attached to Defendant's email as child pornography.[2] As a result of AOL's discovery that Defendant violated AOL's TOS, AOL immediately terminated Defendant's account.

AOL then submitted a report to NCMEC through its CyberTipline on April 23, 2013. This report included Defendant's email along with the four attached images. A NCMEC analyst

[2] It was not until the case was before the Tenth Circuit that it became apparent that AOL only matched one of the four email images with a hash value.

viewed the email and the four attached images and confirmed that all four appeared to be child pornography.[3] NCMEC then alerted local law enforcement agents.

On November 6, 2013, a grand jury indicted Defendant on one count of distribution of child pornography and one count of possession of child pornography. Defendant filed a Motion to Suppress (Doc. 13). After conducting an evidentiary hearing, this Court denied Defendant's motion.

Defendant then entered into a conditional guilty plea, but he reserved his right to appeal the denial of his motion to suppress. On appeal, Defendant asserted that NCMEC's actions constituted an unreasonable search. The Tenth Circuit agreed and found that NCMEC was a governmental entity, or in the alternative, acted as a governmental agent. Next, it concluded that NCMEC's search exceeded the scope of AOL's private search.

The Tenth Circuit remanded the case and stated that "hard questions remain to be resolved on remand."[4] The Tenth Circuit stated that one of those hard questions was "whether the third-party doctrine might preclude [Defendant's] claim to the Fourth Amendment application."[5] It also appears that the Tenth Circuit left open the question of whether Defendant had a reasonable expectation of privacy given that it stated "the district court has yet to make any factual findings relevant to [Defendant's] subjective expectations of privacy or the objective reasonableness of those expectations in light of the parties' dealings (*e.g.*, the extent to which AOL regularly accessed emails and the extent to which users were aware of or acquiesced in

[3] The fact that NCMEC viewed all four of the images, rather than just the one that matched AOL's hash value, was an important factor in the Tenth Circuit's analysis.

[4] *United States v. Ackerman*, 831 F.3d 1292, 1308 (10th Cir. 2016).

[5] *Id.*

such access)."[6] The final issue to be resolved is whether one of the "hard questions" on remand encompasses the good faith doctrine and its applicability in this case.

II. Analysis

Defendant seeks the suppression of the email and its attachments contending that it was obtained through an illegal search and seizure. The Court will first consider whether Defendant had a reasonable expectation of privacy in his email and four attachments. Next, the Court will consider whether the government acted in good faith and whether the good faith doctrine is applicable in this case.

A. Reasonable Expectation of Privacy

When this Court previously considered whether Defendant had a reasonable expectation of privacy, the Court assumed without deciding that he did. On appeal to the Tenth Circuit, the circuit noted this fact.[7] The circuit also stated that this Court had not made any factual findings as to a reasonable expectation of privacy and that those facts may impact the legal analysis.[8] Thus, the Court will now consider Defendant's expectation of privacy in his email.

"A search only violates an individual's Fourth Amendment rights if he or she has a legitimate expectation of privacy in the area searched."[9] There is a two-part test in determining whether a reasonable expectation of privacy exists.[10] First, the defendant must demonstrate that

[6] *Id.* at 1305.

[7] *Id.* ("[T]hroughout its decision the court assumed that [Defendant] had a reasonable expectation of privacy in his email.").

[8] *Id.* (noting the lack of factual findings as to Defendant's subjective and objective expectations of privacy).

[9] *United States v. Ruiz*, 664 F.3d 833, 838 (10th Cir. 2012) (quotation marks and citation omitted).

[10] *See Smith v. Maryland*, 442 U.S. 735, 740 (1979).

he "manifested a subjective expectation of privacy in the area searched."[11] Next, there is the question of "whether society is prepared to recognize that expectation as objectively reasonable."[12]

The government asserts that a search did not occur because Defendant did not have a reasonable expectation of privacy in his email and the four attached images at the time NCMEC reviewed it. The government frames the issue narrowly. It does not rely on the third-party doctrine and agrees that Defendant had an expectation of privacy in his email account *before* AOL terminated his account. Instead, the government argues that Defendant fails to present any evidence that he had a subjective or objective expectation of privacy in the one email and four attachments to that email *after* AOL (the third-party email provider) terminated his account for violating its TOS.

Defendant testified that he believed his email was private. Thus, with regard to Defendant's subjective belief, he satisfies his burden. The relevant question in this case is whether Defendant's subjective expectation is objectively reasonable. Narrowed down even further, the question is whether Defendant had an objectively reasonable expectation of privacy in the one email and four attachments after AOL had terminated his account.

In this case, Defendant was a user of AOL and was subject to AOL's TOS. To have an account with AOL, a user must agree to the terms. If AOL updates its TOS, it sends an email to the AOL user that states that AOL is updating its TOS on a certain date and that the user's log-in after that date indicates that the user accepts the new TOS.

---

[11] *United States v. Johnson*, 584 F.3d 995, 999 (10th Cir. 2009) (citation omitted).

[12] *Id.* (citation omitted).

Here, Defendant agreed to AOL's TOS by using his email account. The TOS expressly alerted Defendant that he was not to participate or engage in illegal activity. In addition, the TOS provided that a user must not post explicit sexual acts. Furthermore, it informed Defendant that if he did not comply with the applicable TOS, it could take technical, legal or other actions (in its sole discretion) to enforce the TOS.

In at least two recent cases from different district courts, courts have determined that the existence of a TOS agreement diminishes a user's objectively reasonable expectation of privacy. In *United States v. Stratton*,[13] a case from the District of Kansas, the defendant had an account through electronic service provider Sony's PlayStation Network.[14] Users can communicate with other users online in a similar manner to email communication, and users must agree to Sony's TOS.[15] The defendant sent messages about child pornography and downloaded images that included child pornography.[16]

In *Stratton*, the court found the Tenth Circuit's reasoning regarding whether an employee had a legitimate expectation of privacy in images he downloaded on a work computer instructive.[17] The court noted that although the case before it did not involve an employee-employer relationship, the rationale that "the employer's regulations reduced the employee's expectation of privacy" applied equally to Sony and its users.[18] The court noted that users of

[13] 229 F. Supp. 3d 1230 (D. Kan. 2017).

[14] *Id.* at 1233.

[15] *Id.*

[16] *Id.* at 1235.

[17] *Id.* at 1241-42 (citing *United States v. Angevine*, 281 F.3d 1130 (10th Cir. 2002))

[18] *Id.* at 1242.

Sony's PlayStation had to agree to the TOS when signing up for an account.[19] The TOS included such terms that Sony reserved the right to monitor online activity and that users must not violate any laws.[20] Thus, the Court found that the TOS "explicitly nullified its users reasonable expectation of privacy."[21]

Similarly, in *United States v. Wilson*,[22] a case from the Southern District of California, the court determined that the defendant lacked a reasonable expectation of privacy in the child pornography files that he uploaded to his Google email account because he had agreed to Google's TOS when creating his Google account.[23] The court reasoned that the defendant was aware that Google may review and monitor his account for illegal activity.[24] Thus, the court found no reasonably objective expectation of privacy.[25]

In this case, AOL's TOS similarly limits Defendant's objectively reasonable expectation of privacy. As noted above, the TOS informed Defendant that he must comply with applicable laws and that he could not participate in illegal activities. AOL's TOS also informed Defendant that if he participated in illegal activities or did not comply with AOL's TOS, it could take technical, legal, or other actions without notice to him. Thus, the Court concludes that Defendant cannot establish a reasonably objective expectation of privacy in this particular email and its four

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] 2017 WL 2733879 (S.D. Cal. 2017).

[23] *Id.* at *7.

[24] *Id.*

[25] *Id.*

attachments (containing child pornography) after AOL terminated his account for violating its TOS.

In sum, even though the Tenth Circuit found that NCMEC is a governmental actor and/or entity and exceeded AOL's private search, this Court finds on remand that Defendant did not have a reasonable expectation of privacy in his email or the four attached images at the time of NCMEC's search. Because he did not have a reasonable expectation of privacy, NCMEC's conduct did not cause a violation of the Fourth Amendment and suppression is not warranted.

B. Good Faith Exception

Alternatively, even if Defendant could establish a reasonable expectation of privacy, suppression is unwarranted due to the good faith doctrine. As an initial matter, the parties disagree as to whether the government can assert the good faith doctrine on remand. When this case was initially before this Court, the government argued that even if a search occurred that violated the Fourth Amendment, the good faith exception would be applicable. This Court did not reach the issue and made no rulings in its previous order as to the applicability of the good faith doctrine.

Defendant appealed this Court's ruling to the Tenth Circuit but did not appeal any ruling on the good faith doctrine as there was no ruling from which to appeal. Instead, Defendant appealed the rulings that NCMEC was not acting as a governmental agent and even if it was, NCMEC's search did not surpass AOL's private search. The Tenth Circuit reversed on both issues. After making its findings, the Tenth Circuit noted that the government could have argued any number of reasons as to why NCMEC's search was still "reasonable."[26] The circuit noted

[26] *Ackerman*, 831 F.3d at 1308.

that the closest that the government came to briefing the question was whether NCMEC acted in good faith.[27] However, the circuit stated that the government had only incorporated by reference the good faith arguments it had presented to the district court and that this was insufficient to preserve a point for appellate review.[28]

"When a case is appealed and remanded, the decision of the appellate court establishes the law of the case and ordinarily will be followed by both the trial court on remand and the appellate court in any subsequent appeal."[29] "The law of the case doctrine precludes relitigation of a ruling of law in a case once it has been decided."[30] "Law of the case principles do not bar a district court from acting unless an appellate decision has issued on the merits of the claim sought to be precluded."[31]

Here, there has not been a ruling of law on the applicability of the good faith doctrine. On appeal, neither party could challenge this Court's legal decision on the good faith doctrine because this Court did not address the doctrine. Thus, the law of the case doctrine does not preclude consideration of this issue upon remand.

Substantively, the government argues that even if NCMEC's review of Defendant's email and the four attachments violated the Fourth Amendment, suppression is not warranted because

---

[27] *Id.*

[28] *Id.* There was no ruling, however, for the circuit to review because this Court made no findings regarding the good faith exception.

[29] *United States v. West*, 646 F.3d 745, 747-48 (10th Cir. 2011) (quotation marks and citation omitted).

[30] *Id.* at 748.

[31] *Wilmer v. Bd. of Cty. Comm'rs of Leavenworth Cty.*, 69 F.3d 406, 409 (10th Cir. 1995) (quotation marks and citation omitted); *see also Concrete Works of Colo., Inc. v. City & Cty. of Denver*, 321 F.3d 950, 992 (10th Cir. 2003) (citation omitted) (noting that the district court *had* decided an issue but when the party appealed the case, the party waived the issue by not briefing it to the appellate court and thus the law of the case precluded relitigation of that issue when the case was remanded to the district court).

NCMEC and law enforcement acted in good faith. Although evidence obtained in violation of the Fourth Amendment generally cannot be used, there are a few exceptions to the Fourth Amendment's exclusionary rule. One of those exceptions is when law enforcement acts in good faith, or in "objectively reasonable reliance," on a statutory scheme.[32]

For this proposition, the government primarily relies upon a United States Supreme Court case, *Illinois v. Krull*,[33] and *United States v. Keith*,[34] a case from the District of Massachusetts. In *Krull*, a police officer relied upon a state statutory scheme when he searched an automobile wrecking yard and ultimately found several stolen vehicles.[35] A day after the search, the statute was found unconstitutional for authorizing warrantless searches.[36] The Illinois courts suppressed the evidence finding that the statute was unconstitutional and that "good-faith reliance upon that statute could not be used to justify the admission of evidence under an exception to the exclusionary rule."[37] The United States Supreme Court reversed. Specifically, it found that the exclusionary rule was inapplicable to suppressing evidence obtained by a police officer who acted in objectively reasonable reliance on a statute that authorized a warrantless administrative search, even though the statute was later found unconstitutional.[38] Thus, the United States

[32] *See United States v. Vanness*, 342 F.3d 1093, 1097 (10th Cir. 2003) (citing *United States v. Leon*, 468 U.S. 897 (1984) and *Illinois v. Krull*, 480 U.S. 340 (1987)).

[33] 480 U.S. 340 (1987).

[34] 980 F. Supp. 2d 33 (D. Mass. 2013).

[35] *Krull*, 480 U.S. at 343.

[36] *Id.* at 344.

[37] *Id.* at 346.

[38] *Id.* at 357-58.

Supreme Court found that the officer's good faith reliance upon that statute did not warrant suppression of the evidence.

In *Keith*, the court considered similar facts to this case. There, AOL identified a matching hash value in an email and sent NCMEC a CyberTipline report with the suspect file.[39] The court first found that NCMEC acted as an agent of law enforcement when it examined the CyberTipline report and that Fourth Amendment principles were applicable to its conduct.[40] The court decided, however, that even though NCMEC's examination violated the Fourth Amendment, the exclusionary rule was inapplicable to its conduct.[41] Relying on the reasoning in *Krull*, the court concluded that Congress, by statute, had given NCMEC's CyberTipline a large role in the detection and prosecution of child pornography crimes.[42] The court stated "[t]here is nothing in the record in this case that would suggest either NCMEC or the police or the magistrate who issued the warrant knew or ought to have known that by relying on the CyberTipline report they were doing something that was unconstitutional under the Fourth Amendment.[43] Accordingly, the court declined to suppress the evidence.[44]

Defendant contends that the good faith exception is inapplicable here. He argues that the statutory scheme in *Krull* is different from the statutory scheme in this case because the statutory scheme in *Krull* expressly authorized warrantless searches. Specifically, the statute in *Krull*

---

[39] *Keith*, 980 F. Supp. 2d at 37.

[40] *Id*. at 41-43, 46.

[41] *Id.* at 46.

[42] *Id.*

[43] *Id.*

[44] *Id*. at 46-47.

allowed officials to "inspect" records "at any reasonable time during the night or day" and allowed "examination of the premises of . . . place of business."[45] In contrast, Defendant contends that the statute here does not authorize warrantless searches but instead simply allows NCMEC to possess contraband.

Defendant's argument draws too fine of a line. Under 18 U.S.C. § 2258A(a)(1), an electronic service provider is required to provide a report of any apparent child pornography to NCMEC's CyberTipline. This report may include information about the individual, historical reference, geographic location, and any images.[46] NCMEC is then required to forward this report and information to law enforcement.[47] In the Tenth Circuit's *Ackerman* opinion, it noted these statutes and stated that NCMEC is "statutorily authorized to receive contraband (child pornography) knowingly *and review* its contents intentionally."[48] It also stated that these statutes were effectively "a statutory grant of special law enforcement authority to a single entity and no other, authorizing and encouraging it to perform functions no other private person or entity may lawfully undertake."[49] The Tenth Circuit, in determining that NCMEC acted as a governmental agent recognized and acknowledged the breadth of the authority given to NCMEC by statute.[50] In addition, the Tenth Circuit noted that although the statutes do not require NCMEC to open and

[45] *Krull*, 480 U.S. at 343.

[46] 18 U.S.C. § 2258A(b)(1)-(4).

[47] *Id.* at § 2258A(c).

[48] *Ackerman*, 831 F.3d at 1297 (emphasis added) (citing 18 U.S.C. § 2258A(a), (b)(4)).

[49] *Id*. at 1303.

[50] *See id.* at 1301-02 ("Congress statutorily required AOL to forward [Defendant's] email to NCMEC; Congress statutorily required NCMEC to maintain the CyberTipline to receive emails like [Defendant's]; Congress statutorily permitted NCMEC to review [Defendant's] email and attachments; and Congress statutorily required NCMEC to pass along a report about [Defendant's] activities to law enforcement authorities.").

view the email attachments, "everyone accepts that Congress enabled NCMEC to review [Defendant's] email by excepting the Center from the myriad laws banning the knowing receipt, possession, and viewing of child pornography. Nothing about NCMEC's actions could possibly have come as a surprise."[51]

Based on the comprehensive statutory scheme governing NCMEC and its operation of the CyberTipline, NCMEC's conduct in reviewing the email and its four attachments was objectively reasonable and in good faith. NCMEC relied on a statutory scheme allowing it to perform a review. At the time of NCMEC's conduct, it would not have known that it was doing something unconstitutional. This conclusion is bolstered because at the time of the events in question (April 2013), no court had even considered NCMEC a governmental entity or agent of law enforcement.[52]

Furthermore, "exclusion has always been our last resort, not our first impulse."[53] Generally, exclusion is only applicable when it would result in "appreciable deterrence."[54] As noted by the court in the District of Massachusetts, "[n]o persuasive argument can be made that an organization like NCMEC needs to be deterred from acting in good faith in a way that is consistent with explicit congressional will."[55]

---

[51] *Id*. at 1302. At this time, these statutes have not been declared or considered unconstitutional.

[52] The decision in *Keith* in which the District of Massachusetts found that NCMEC acted as an agent of law enforcement did not occur until November 2013.

[53] *Herring v. United States*, 555 U.S. 135, 140 (2009) (citing *Hudson v. Michigan*, 547 U.S. 586, 591 (2006)).

[54] *Id.* at 141 (quotation marks and citations omitted).

[55] *Keith*, 980 F. Supp. 2d at 46.

Finally, "[t]he extent to which the exclusionary rule is justified by these deterrence principles varies with the culpability of the law enforcement conduct."[56] As noted above, until recently, NCMEC would not have even known that it was considered an agent of law enforcement and thus its culpability for its "law enforcement conduct" is minimal. In sum, even if NCMEC's search violated Fourth Amendment principles, NCMEC's conduct was objectively reasonable and excluding the evidence would not result in meaningful deterrence.

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

IT IS SO ORDERED.

Dated this 30th day of October, 2017.

ERIC F. MELGREN
UNITED STATES DISTRICT JUDGE

[56] *Herring*, 55 U.S. at 143.