**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF NEW MEXICO**

**UNITED STATES OF AMERICA,**

**Plaintiff,**

**vs.** **Cr. No. 14-3761 JCH**

**DONALD ALVIN TOLBERT,**

**Defendant.**

**MEMORANDUM OPINION AND ORDER**

This matter is before the Court on Defendant's *Motion to Suppress Evidence Obtained in Violation of the Fourth Amendment Under United States v. Ackerman* [Doc. 90] in which he asks the Court to suppress all evidence obtained either directly or indirectly as a result of the National Center for Missing and Exploited Children ("NCMEC") opening his emails and the attachments thereto. Defendant argues that under *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), NCMEC is a government entity or agency, and therefore its warrantless searches of his emails violated his rights under the Fourth Amendment, and all evidence obtained thereafter is "fruit of the poisonous tree." The Government filed a response [Doc. 93] and Defendant filed a reply [Doc. 114]. On April 24-25, 2018 and June 12, 2018, the Court held an evidentiary hearing on the motion to suppress, at which Defendant was present and the Government presented evidence in the form of witness testimony and exhibits. On July 3, 2018, both parties filed written closing arguments. Docs. 123 and 124. After considering the evidence, the briefs, and the arguments of counsel, the Court concludes that the motion to suppress should be denied.

## FINDINGS OF FACT

Defendant Donald Alvin Tolbert (hereafter, "Tolbert") has a 2006 state court conviction on two counts of criminal sexual contact of a child under age thirteen, among other charges. Tolbert served a term of years in prison until November of 2009, at which point he began serving concurrent terms of probation and parole. In 2010, the state arrested Tolbert for violating the terms of his probation and parole and reincarcerated him for 330 days. Then, the state released Tolbert a second time, subject to conditions of probation. As part of his release, Tolbert agreed to various standard conditions of probation, including allowing any probation or parole officer to visit him at his home or place of employment at any time, and permitting a warrantless search by the officer if he or she had reasonable cause to believe the search would produce evidence of a parole violation. Ex. A at 6-7. As a convicted sex offender, Tolbert also promised to provide all of his email addresses, usernames, and passwords to his probation officer. Ex. A at 3. Further, he agreed that any computer or electronic device to which Tolbert had access could "be examined for inappropriate content [which expressly included child pornography] at any time." Ex. A at 3.

On September 1, 2012, five emails with a total of fifteen attachments were sent through American Online ("AOL") by a user with the email address ddt123abc@aol.com —an email address allegedly belonging to Tolbert. *See* Exs. D1-D5 (NCMEC Cyber Tipline Report IDs 1576684, 1576685, 1576686, 1576688, and 1576689). Three of these emails were sent to a user with the email address donnieisagod@aol.com —also allegedly belonging to Tolbert. *See* Exs. D1, D2, and D3. The other two emails were sent to a third party email address, widd2703@web.de. Exs. D4 and D5. In accordance with its practice in 2012, AOL did not *initially* open or view the files attached to the

emails. Trans. 4/25/18 at 35; Trans. 6/12/18 at 129-30, 135.[1] However, by scanning the emails and attachments using software employing "hash value" matching[2], AOL detected the presence of suspected child pornography. As it is required to do by law, AOL electronically submitted the five emails and corresponding CyberTip reports concerning suspected child pornography to the National Center for Missing and Exploited Children ("NCMEC"). Exs. D1-D5; Trans. 4/24/18 at 18-20, 24; 18 U.S.C. § 2258A. These CyberTips provided by AOL to NCMEC included (1) the email addresses of both the senders and the recipients of the emails, (2) the subjects of the emails, along with all of their attachments; (3) identification of the specific attachments which had been hash value matched as child pornography; and (4) the IP address[3] corresponding to the email sender for all five emails. Exs. D1-D5. *See, e.g.*, Ex. D1 at 191.

AOL's software also automatically prevented the five emails and their attachments from reaching their intended recipients, then terminated and saved a snapshot of the user's account. Trans. 4/25/18 at 8, 15. The entire process was fully automated, meaning no AOL employee opened or read the emails or attachments before AOL sent the CyberTip to NCMEC. Trans. 4/25/18 at 14, 18, 64;

[1] The Court cites to the transcript, the date of the hearing, and the page number.

[2] A "hash value" is a unique 32-character string of alphanumeric characters that is the result of an algorithm that has been applied to a particular photograph or video. Trans. 4/25/18 at 8-9; Trans. 6/12/18 at 125-26; Ex. E at ¶ 5. No two photographs or videos will produce the exact same 32-character hash value unless the two are identical; any change to a photo or video, no matter how small, will result in a different hash value. Trans. 4/25/18 at 16; Ex. E at ¶ 7. AOL maintains a database of hash value strings generated from photographs and videos containing known or suspected child pornography. Trans. 4/25/18 at 9-10, 57-58; Trans. 6/12/18 at 124; Ex. E at ¶ 7. AOL maintains a system known as "image detection filtering process," or IDFP, that scans its users' emails for hash values that are identical to those in AOL's database. Trans. 4/25/18 at 7-9; Trans. 6/12/18 at 123-24, Ex. E at ¶ 7. AOL did not develop this system at the behest of law enforcement. Trans. 4/25/18 at 13; Ex. E at ¶¶ 8-9, 18.

[3] IP stands for internet protocol, and an IP address helps to locate where in the world a computer or other electronic device is being used. Trans. 4/24/18 at 63-64, 65-66.

Trans. 6/12/18 at 128-30. However, in 2012 an AOL employee did open and view the email and attachments the next business day after the CyberTip was sent to NCMEC in order to confirm that the hashed image did in fact belong in AOL's database of images of child pornography. Trans 4/25/18 at 14. 35, 64; Trans. 6/12/18 at 130.

On September 5, 2012, NCMEC[4] opened and then viewed the five emails and their attachments forwarded by AOL along with the CyberTips and determined that the attachments appeared to contain child pornography. Ex. D1 at 195. It did so without seeking or obtaining a search warrant. It then conducted various searches on various publicly available databases for the IP address associated with the five emails, for the two email addresses listed above, as well as for the names "Donnie T" and "Don Tolbert." *See* Ex. D1 at 195-217. The open source searches on the IP address were conducted in order to locate the sender in a particular geographic area—in this case, Albuquerque, New Mexico. Trans. 4/24/18 at 38-41 and 72-76; Ex. D1 at 197-203. NCMEC then performed public, online searches on some of the information sent by AOL in the CyberTip, including the two email addresses noted above that were associated with the five emails and other unique identifiers, such as "YUNGMUFFMAN" and then eventually to someone named "Donnie," then "Don Tolbert," then Margaret Tolbert and her Albuquerque address, and then eventually to a Donald Alvin Tolbert in Albuquerque, New Mexico with a specific address and date of birth. Trans. 4/24/18 at 77-87 ; Ex. D1 at 203-217.

NCMEC then forwarded the CyberTip reports containing those emails and attachments, as well as the results of its public record searches, to the New Mexico Attorney General's Office, Internet

[4] NCMEC was created in 1984. Trans. 4/24/18 at 15, 25. It is a nonprofit organization whose mission is to help reunited families with missing children, to reduce child sexual exploitation, and to prevent child victimization. *Id*. at 15. NCMEC also focuses on training; safety and prevention; and child victim and family services. *Id*. at 16-17. NCMEC serves as a clearinghouse for information about missing and exploited children. *Id*. at 21, 115.

Crimes Against Children ("ICAC") division. *See, e.g.*, Ex. D1 at 216. The ICAC is the clearinghouse for CyberTips with a connection to New Mexico. Trans. 4/24/18 at 164. An analyst with the Attorney General's Office reviewed the CyberTips, including the hash-matched images, and ran open source searches regarding the associated IP address to determine that the source of the emails is in New Mexico. *Id.* at 168-170. Then, the analyst refers the CyberTips to the Special Agent in Charge, who assigns them to law enforcement for further investigation. *Id*. at 171. Certain types of cases, including those involving registered sex offenders on probation, take high priority. *Id*. at 172-73, 194-96.

On September 7, 2012, Special Agent Owen Pena of the AG's office was assigned to conduct an investigation regarding the five CyberTips relating to "Donald Alvin Tolbert." Trans. 4/24/18 at 180, 183, 193. By using open source searches on the IP address associated with the email addresses donnieisagod@aol.com and ddt123abc@aol.com listed in the CyberTip reports, Pena verified the geographical connection between the IP address and Albuquerque, New Mexico. *Id*. at 182-83. Using that information, Pena obtained grand jury subpoenas duces tecum for information associated with the IP address from ISP CenturyLink as well as information from AOL regarding the two email addresses. *Id*. at 183; Ex. J. AOL's response to the subpoena resulted in information linking donnieisagod@aol.com with "Donald Tolbert" at an address in Albuquerque, New Mexico, 87105. *Id*. at 184-85. Century Link responded to the subpoena with information linking the IP address with "Margaret Tolbert" at an address on 57th Street in Albuquerque, New Mexico. *Id*. at 186. Pena further found that the IP address associated with the above was also associated with an account on a Russian file uploading website, IMGSRC, under the name YUNGMUFFMAN. *Id*. at 187. That public account contained pictures of young girls, some of them naked. *Id*. at 187-88; Ex. L. The "real name" listed for the owner of the account was "Donnie," with the email address ddt666abc@gmail.com. Ex. L. Under "user info," it states: "I love girls between 8-15. Someone told on me got my other 2 email

accounts cancelled. AOL has something that reads your emails." Ex. L. After determining that the emails in the CyberTips were associated with Donald Tolbert, Pena called Tolbert's probation officer and confirmed that he was a registered sex offender on probation in New Mexico. Trans. 4/24/18 at 189-90.

Pena contacted Christina Altamirano, an agent with Homeland Security Investigations specializing in internet crimes against children and sexual exploitation crimes. Trans. 5/25/18 at 67-69; Trans. 4/24/18 at 190. Altamirano met with Pena and reviewed the evidence that he had obtained regarding Tolbert. Trans. 5/25/18 at 69-70. This included subscriber information from AOL and Century Link, as well as five NCMEC reports and associated videos. Using that evidence, Altamirano prepared and obtained search warrants for AOL regarding the two email addresses mentioned in the CyberTip reports, ddt123abc@aol.com and donnieisagod@aol.com. *Id*. at 71. These warrants revealed subscriber information for the two email addresses, along with IP addresses, times, and dates the accounts were used. *Id*. at 71-72; Exs. M and N. Similarly, Pena obtained search warrants for Tolbert's residence, as well as that of Tolbert's mother. *Id*. at 74; Trans. 4/24/18 at 190-91; Exs. K1 and K2. At Tolbert's residence, officials seized cell phones, a notebook, photographs, books and videos. Trans. 5/25/18 at 74. At his mother's home, they found two computers, a digital camera, and a cell phone. *Id*. at 75. Police found photos and videos depicting child pornography on the two computers seized at Tolbert's mother's home. *Id*. at 75-76.

After the Tenth Circuit released the *Ackerman* decision, the Rio Rancho police department obtained a new search warrant for the two computers without the benefit of the contents of the emails and the attached videos and images. Trans. 5/25/18 at 105. The computers were reexamined, and child pornography images and videos were again found on those machines. *Id*. at 76-77. In an interview,

Margaret Tolbert told police that she and Defendant were the only ones with access to those computers. *Id*. at 79.

Altamirano testified in some detail, and with credibility, about the steps that she would have taken and the investigation she would have conducted if the CyberTips in this case had come to her without the opened emails and attachments (photos and videos) for her to examine. *See* Trans. 4/25/18 at 80-97. Altamirano explained that even without the emails and attachments, she still would have conducted an investigation that would have ended in obtaining the emails and attachments, as well as connecting them to Tolbert. *Id*. For example, Altamirano could have used the fact that AOL obtained a hash value match to obtain a search warrant for the emails and their attachments, as well as to obtained the name and address of the user associated with that account. *Id*. at 81-83. She also explained that once she had a name and address of the AOL account user, she could use law enforcement and open source databases to find out more information about that person. In this case, that information would have led Altamirano to Tolbert, and information about his prior criminal case. *Id*. at 83-86. Altamirano also admitted that she had never actually done this, as all of the NCMEC CyberTips she had worked with in the past contained opened emails and/or attachments. *Id*.at 99-100.

## DISCUSSION

Tolbert moves to suppress "all evidence obtained directly or indirectly as a result of NCMEC's warrantless search." Doc. 90 at 9. He reasons that under the Tenth Circuit's decision in *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), NCMEC is a government entity or agent and therefore was required to obtain a warrant prior to performing searches by opening his emails and their attachments. He contends that all evidence obtained as a result of the warrantless searches is "fruit of the poisonous tree" and must be suppressed.

In its opposition to the motion to suppress, the Government relies on numerous arguments in support of the conclusion that the exclusionary rule does not apply. First, the government contends that Tolbert had no legitimate expectation of privacy in his emails because of both the terms of his probation and the terms of the AOL user agreement. Second, it contends that despite the Tenth Circuit's ruling to the contrary in *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), NCMEC is not a governmental entity or agent and therefore cannot have violated Tolbert's Fourth Amendment rights. Third, it argues that the "special needs" exception to the warrant requirement applies here. Fourth, the government argues that under the "totality of the circumstances" exception to the warrant requirement, there was no constitutional violation. Fifth, the government contends that the "good faith" exception to the warrant requirement justified the search of Tolbert's emails. Sixth, the government argues that the email evidence should be not suppressed because it would have been inevitably discovered. Seventh, it contends that the evidence should not be suppressed due to the attenuation of the taint.

The Court concludes that despite the fact that NCMEC opened the emails and attachments without a warrant, the evidence should not be suppressed because both the good faith and the inevitable discovery exceptions to the warrant requirement apply here. Having reached that conclusion, the Court will not reach the other arguments raised by the parties.

## I. Legal Standard

The Fourth Amendment to our Constitution protects persons against unreasonable searches and seizures in their "persons, houses, papers, and effects." U.S. Const. amend. IV. "The basic purpose of this Amendment . . . is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Camara v. Mun. Court of City & Cnty. of S.F.*, 387 U.S. 523, 528 (1967). "The exclusionary rule has traditionally barred from trial

physical, tangible materials obtained either during or as a direct result of an unlawful" search or seizure. *Wong Sun v. United States*, 371 U.S. 471, 485 (1963).

## II. The *Ackerman* Decision

On August 5, 2016, the Tenth Circuit issued its opinion in *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016). Like the Defendant in this case, defendant Ackerman used AOL as an internet service provider (ISP) to send and receive email. By comparing the hash values generated from the images in Ackerman's email to AOL's library of known hash values for child pornography, the company's automated filter identified one of the images attached to Ackerman's email as child porn. AOL instantly stopped delivery of the message and closed Ackerman's account.

Once AOL identified a hash value match in Ackerman's email, the company forwarded a report to NCMEC's online CyberTipline. AOL's report included Ackerman's email along with all four attached images. A NCMEC analyst opened the email, viewed each of the attached images, and confirmed that all four (not just the one AOL's automated filter identified) appeared to be child pornography. After the analyst determined that Ackerman was the likely owner of the account, NCMEC alerted law enforcement agents in the area where he lived. A federal grand jury indicted Ackerman on charges of possession and distribution of child pornography.

There were two issues raised in the *Ackerman* case. First, Ackerman alleged that NCMEC's actions amounted to an unreasonable search of his email and its attachments because no one sought a warrant and no one invoked any recognized lawful basis for failing to seek one. Because the Fourth Amendment only protects against unreasonable searches undertaken by the government or its agents, Ackerman's motion to suppress raised the question of whether NCMEC qualifies as a governmental entity or agent. The second issue was whether NCMEC merely repeated or actually exceeded the

scope of AOL's investigation. This question arose because the Supreme Court's "private search" doctrine suggests the government does not conduct a Fourth Amendment "search" when it merely repeats an investigation already conducted by a private party like AOL.

As to the first issue, the Tenth Circuit held that the NCMEC is a governmental entity. The Court based this conclusion on five considerations. First, the court noted that NCMEC has law enforcement powers, and those powers extend well beyond those enjoyed by private citizens. NCMEC's two primary authorizing statutes—18 U.S.C. § 2258A and 42 U.S.C. § 5773(b)—mandate its collaboration with federal (as well as state and local) law enforcement in over a dozen different ways, many of which involve duties and powers conferred on and enjoyed by NCMEC but no other private person. For example, NCMEC is statutorily obliged to maintain an electronic tip line for ISPs to use to report possible Internet child sexual exploitation violations to the government. Under the statutory scheme, NCMEC must forward every single report it receives to federal law enforcement agencies and it may make its reports available to state and local law enforcement as well. *See id.* § 2258A(c). Second, ISPs are required to report any known child pornography violations to NCMEC—not to any other governmental agency, but rather to NCMEC alone. ISPs who fail to comply with this obligation face substantial (and apparently criminal) penalties payable to the federal government. *Id.* § 2258A(a)(1), (e). Third, when NCMEC confirms it has received a report, the ISP must treat that confirmation as a request to preserve evidence issued by the government itself. Failure to comply again opens an ISP to potential civil or criminal sanctions. Fourth, in aid of NCMEC's tip line functions, Congress has statutorily authorized it to receive contraband (child pornography) knowingly and to review its contents intentionally. *Id.* § 2258A(a), (b)(4). The court observed that these are actions that would normally subject private persons to criminal prosecution. *See* 18 U.S.C. § 2252A(a)(2) (knowing receipt or distribution); *id.* § 2252A(a)(5)(B) (knowing possession or access

with intent to view). Fifth, the Tenth Circuit compared NCMEC to Amtrak, and analogized cases wherein the Supreme Court held that Amtrak—a publicly owned corporation—is a governmental entity. Of primary consideration here were the level of governmental control over both NCMEC and Amtrak, the broad statutory mandates to which both entities are subject, their dependence on federal funding, the purpose behind each entity's creation, and the benefits they each conferred on the government. Based on all the foregoing factors, the Tenth Circuit concluded that NCMEC is a governmental entity. Alternatively, the Court found that NCMEC acted as an agent of the government, and was therefore subject to the Fourth Amendment under the *United States v. Souza*, 223 F.3d 1197 (10th Cir. 2000). Under *Souza*, to determine whether an entity is acting as a government agent, one must ask 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. The Tenth Circuit concluded that NCMEC satisfies both criteria.

The *Ackerman* court then turned to the second issue, which was whether the "private search doctrine" made the search permissible. The Supreme Court has concluded that even a "wrongful search ... conducted by a private party does not violate the Fourth Amendment." *Walter v. United States*, 447 U.S. 649, 656 (1980). And, "such private wrongdoing does not deprive the government of the right to use evidence that it has acquired lawfully." *Id*. In *United States v. Jacobsen*, 466 U.S. 109 (1984), FedEx employees opened a damaged package, found suspicious plastic bags of white powder inside, and passed the parcel to the government, along with a description of what they had found. *Id*. at 111. An agent from the Drug Enforcement Agency ("DEA") then repeated the same investigation, opening the package and examining its contents. *Id*. Finally, he subjected the white powder to a chemical drug test to confirm it was cocaine. *Id*. at 111-12. Considering all this, the Supreme Court held that no "search" implicating

the Fourth Amendment had taken place because there was a "virtual certainty" that the government could have discovered "nothing else of significance" in the package nor learned anything beyond what it had "already ... been told" by a private party. *Id*. at 119. "Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information." *Id*. at 117.

In *Ackerman*, the government attempted to analogize *Jacobsen* to the search NCMEC conducted on Ackerman's emails. The Tenth Circuit rejected this argument, stating:

> Yes, AOL ran a search that suggested a hash value match between one attachment to Mr. Ackerman's email and an image AOL employees had previously identified as child pornography. But AOL never opened the email itself. Only NCMEC did that, and in at least this way exceeded rather than repeated AOL's private search. Neither is there any doubt NCMEC's search of the email itself quite easily "could [have] disclose[d]" information previously unknown to the government besides whether the one attachment contained contraband. Indeed, when NCMEC opened Mr. Ackerman's email it could have learned any number of private and protected facts, for (again) no one before us disputes that an email is a virtual container, capable of storing all sorts of private and personal details, from correspondence to other private (and perfectly legal) images, video or audio files, and beyond. And we know, too, that this particular container did contain three additional attachments, the content of which AOL and NCMEC knew nothing about before NCMEC opened them too. As far as anyone knew at the time, they could have revealed virtually any kind of noncontraband information to the prying eye.

*Ackerman*, 831 F.3d at 1305-06 (citations omitted). Because NCMEC opened Ackerman's email first and did so in order to view not just the attachment that was the target of AOL's private search but three others as well, each of these steps—opening the email and viewing the three other attachments—was enough to risk exposing private, noncontraband information that AOL had not previously examined. Thus, the *Ackerman* court concluded that the search violated the Fourth Amendment.

However, the Tenth Circuit explicitly left open the questions of whether the third-party doctrine could preclude motions to suppress like Ackerman's, or that changes in how reports are

submitted or reviewed might allow NCMEC to access attachments with matching hash values directly, without reviewing email correspondence or other attachments with possibly private, noncontraband content—and in this way perhaps bring the government closer to a successful invocation of the private search doctrine. The court also left open the possibility that the government could cite exigent circumstances, the attenuation doctrine, the special needs doctrine, or the good faith exception to excuse warrantless searches or avoid suppression in at least some cases.

## III. The Good Faith Exception

The government argues even if NCMEC's search of Tolbert's emails violated the Fourth Amendment, suppression is unwarranted because NCMEC and law enforcement officers acted in good faith. The Court agrees.

As the Supreme Court has explained, the purpose of the exclusionary rule is not to remedy a private wrong, but rather as a practical means of deterring future unlawful behavior by law enforcement. *United States v. Calandra*, 414 U.S. 338, 347 (1974). Thus, "[t]he deterrent purpose of the exclusionary rule necessarily assumes that the police have engaged in willful, or at the very least negligent, conduct" to deprive a defendant of a guaranteed right. *United States v. Peltier*, 422 U.S. 531, 539 (1975) (internal quotation marks omitted). As a result, the Court has held that the deterrent effect of exclusion of evidence is minimal where an officer has acted on an objectively reasonable belief that his actions did not violate the Fourth Amendment. *United States v. Leon*, 468 U.S. 897, 922 (1984). In *Leon*, the Court concluded that the exclusionary rule should not be applied to prevent the use in a criminal prosecution of evidence obtained by officers whose reliance on a warrant issued by a magistrate was objectively reasonable, even though it was later determined that probable cause for the

issuance of the warrant was lacking. "Penalizing the officer for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations." *Id*. at 921. 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." *Herring v. United States*, 555 U.S. 135, 144 (2009).

In *Leon*, the Court applied the good faith exception because the officers acted in objectively reasonable reliance on a warrant issued by a magistrate. However, the good faith exception is not restricted to situations in which police officers rely upon a warrant later found to be invalid. For example, the Supreme Court has also held that the exclusionary rule should not be applied to suppress evidence obtained by officers who acted in objectively reasonable reliance on a statutory scheme that authorized warrantless administrative searches, even though the statute was later found to violate the Fourth Amendment. *Illinois v. Krull*, 480 U.S. 340 (1987). In *Krull*, the Court explained that in light of the deterrent purpose of the exclusionary rule, "evidence 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." *Krull*, 480 U.S. at 348-49 (internal quotation marks and citation omitted).

This case is similar to *Krull* in that there was a statutory scheme in place which expressly authorized NCMEC to open emails and attachments forwarded to it by ISPs and then forward the information obtained to members of law enforcement; nowhere in the statute does Congress require NCMEC to obtain a warrant. As the Tenth Court set forth in great detail in *Ackerman*, Congress created a detailed statutory scheme endowing NCMEC, an incorporated entity, *Ackerman*, 831 F.3d at 1295, with the right to take the actions it did in this case: "Congress's statutes don't require NCMEC to open and view email and attachments like Mr. Ackerman's. But everyone accepts that Congress has

authorized and funded NCMEC to do just that. And everyone accepts that Congress enabled NCMEC to review Mr. Ackerman's email by excepting [NCMEC] 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." *Ackerman*, 831 F.3d at 1302.

What was a surprise to NCMEC, however, was the fact that it would be considered a government entity or government agent that was required to obtain a warrant prior to viewing emails and attachments contained in CyberTips. To the Court's knowledge, the First Circuit was the first federal court to suggest that NCMEC was a government agent; that ruling, in *United States v. Cameron*, 699 F.3d 621, 645 (1st Cir. 2012), was issued on November of 2012, a couple of months after the events in this case. *Cameron* was later followed by the Tenth Circuit's *Ackerman* opinion in 2016, approximately four years after NCMEC reviewed Tolbert's emails in 2012. In September of 2012, when NCMEC opened Tolbert's emails, no court had held that NCMEC was a government entity and therefore was required to obtain a warrant prior to doing what it was statutorily authorized to do: opening emails and attachments that had been forwarded to it.[5]

Nor can this Court assert that NCMEC and law enforcement could not have reasonably relied either on the statutory scheme authorizing NCMEC to view the attachments to Tolbert's emails without a warrant, or on their apparent belief that NCMEC was a private entity. Although Tolbert argues that it should have been immediately obvious to the employees of NCMEC and to law enforcement agencies that NCMEC is a government agent, that argument is undermined by the fact that even the district court in *United States v. Ackerman*, 2014 WL 2968164, No. 13-10176-01-EFM, at *7-8 (D. Kan. July 1, 2014) (unpublished), concluded that NCMEC was not a state actor. Of course,

[5] In contrast, at least one federal court had found prior to that time that NCMEC is a private entity that is not subject to the Freedom of Information Act's disclosure requirements. *See Lazaridis v. U.S. Dep't of Justice*, 713 F. Supp. 2d 64, 67-69 (D.D.C. 2010).

the Tenth Circuit ultimately reached the opposite conclusion and reversed the district court on this issue. However, the question is not whether law enforcement reached the wrong conclusion, but rather whether their belief in the legality of their actions was objectively reasonable at the time. This court concludes that it was. Law enforcement in this case naturally assumed that the statutory authority granted to NCMEC was enough to justify opening the emails. Thus, a reasonable law enforcement officer could conclude that by opening an email or attachment that NCMEC had already opened, he was merely repeating a search previously performed by a private party as permitted by the private search doctrine. The Court finds no evidence of deliberate, reckless, or grossly negligent conduct by either NCMEC or the police who reasonably assumed that these were the statutorily authorized actions of a private party.

When Altamirano and Pena acquired the search warrants for AOL's records, Tolbert's home, and Margaret Tolbert's home, they had no reason to believe that AOL had provided NCMEC with information procured in violation of Tolbert's Fourth Amendment rights. There was no evidence NCMEC had exceeded the scope of its authority when it relied on the information AOL provided and opened the hash matched images. And, when the officers executed the search warrant on Tolbert's and his mother's respective homes, they had no reason to believe the warrants were obtained in violation of Tolbert's Fourth Amendment rights. When an officer relies on a warrant, a presumption exists that the officer acts in good faith. *United States v. Cardall*, 773 F.2d 1128, 1133 (10th Cir. 1985*); see also Leon*, 468 U.S. at 922 ("[A] warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search." (internal quotation marks and citations omitted)). Thus, it would serve no deterrent purpose to exclude the evidence obtained as a result of those warrants.

Other federal district courts have reached the same conclusion in similar cases. For example, in *United States v. Stratton*, 229 F. Supp. 3d 1230, 1233 (D. Kan. 2017), the defendant used his Sony PlayStation3 to send child pornography over the PlayStation Network. *Id*. On more than one occasion[6], *id*. at 1233, 1235, other PlayStation3 users reported that defendant had engaged in improper use of the network. As a result of these reports from its customers, Sony reviewed the offending messages and images. Concluding that it was required to report to NCMEC under 18 U.S.C. § 2258A, Sony forwarded the messages and images to NCMEC, along with defendant's email address, home address, IP address, and the date that he opened the account. *Id*. at 1234. NCMEC determined that the files contained child pornography and made the files available to law enforcement, who then served a subpoena on Google and CenturyLink. *Id*. at 1235. Through information obtained from those subpoenas, law enforcement was able to obtain the defendant's IP history, his IP address, and finally his physical address. *Id*. An agent from the Kansas Bureau of Investigation reviewed the information that Sony had provided to NCMEC, the subpoenas issued to Google and CenturyLink, their responses, and other publically available information. Based on this information, the agent obtained a warrant to search defendant's residence. *Id.* The *Stratton* court held that the Fourth Amendment did not apply to the search of defendant's messages because (1) Sony, the party that conducted the initial searches, was a private party; (2) NCMEC did not exceed the scope of Sony's private search; and (3) the defendant lacked a reasonable expectation of privacy in the information Sony sent to NCMEC due to Sony's Terms of Service Agreement. *Id*. at 1236-1242. However, as an alternative basis for its ruling, the *Stratton* court concluded that even if there were a Fourth Amendment violation, the good faith exception should preclude exclusion of the evidence. *Id* at 1243-

[6] Sony received reports about the defendant in June and December of 2012, as well as in July of 2013. *Id* at 1234-35.

44. The court stated, "There was no evidence NCMEC had exceeded the scope of its authority when it relied on the information Sony provided. And, when the officers executed the search warrant on defendant's home, they had no reason to believe the warrant was obtained in violation of defendant's Fourth Amendment rights." *Id*. at 1243.

In *United States v. Keith*, 980 F. Supp. 2d 33 (D. Mass. 2013)—a decision that was not issued until after the 2012 searches in this case—AOL used hash value matching to identify a suspect file in an email sent on November 26, 2009. *Id*. at 37. The following day, AOL sent a CyberTipline report to NCMEC. *Id*. In accordance with its practice at the time, no AOL employee opened or viewed the file before sending it to NCMEC. *Id*. An analyst at NCMEC "opened and examined the image file, determined that it met the criteria for classification as child pornography, investigated the IP address from which the offending email originated, and determined that the IP address was located within Massachusetts." *Id*. NCMEC then sent the information to law enforcement personnel in Massachusetts, along with information about the email sender's IP address and internet service provider. *Id*. at 37-38. By subpoenaing records from the internet service provider, law enforcement linked the IP address with a computer at the defendant's home. *Id*. at 38. The *Keith* court held that while NCMEC was a government entity, the evidence should not be suppressed because the good faith exception applied. The court stated:

> Congress has by statute given NCMEC's CyberTipline a significant role in the investigation and subsequent prosecution of child pornography crimes, and has directed that it be supported by government grants. While I have concluded that NCMEC conducts its CyberTipline program as an agent of law enforcement so that its inspections of the content of emails are subject to the Fourth Amendment, it still must be acknowledged that those who heretofore regarded NCMEC's role only as that of a private party, so that the Fourth Amendment was inapplicable, were not acting in willful or negligent disregard of constitutional principles, but rather pursuant to a view of NCMEC's statutorily sanctioned role and activity that was, under all the circumstances, objectively reasonable, just as the officers' view of the statutory

> scheme was found to be in *Krull*. In that case the Court explained that "evidence 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." *Krull*, 480 U.S. at 348-49, 107 S.Ct. 1160 (internal quotation marks and citation omitted).
>
> There 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. No 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.

*Id*. at 46. As required by *Leon*, 468 U.S. at 907, and *Herring v. United States*, 555 U.S. 135, 141-42, (2009), the *Keith* court weighed any possible deterrent value from applying the exclusionary rule against the "substantial social costs" of suppressing the evidence. 980 F. Supp. 2d at 46. The court concluded that because the deterrent value was "minimal" under the circumstances, the social costs of suppression tipped against the defendant's motion to suppress. *Id*.

In this case, suppression would have very little deterrent effect because the law enforcement officers involved had no knowledge, nor could they properly be charged with knowledge, that NCMEC was required to get a warrant before opening Tolbert's emails and attachments. At the same time, there is a significant social cost if the evidence were to be suppressed. Thus, the Court concludes that the good faith exception applies and the motion to suppress should be denied. *See also United States v. Reddick*, 2017 WL 1353803, Cr. No. 2:16-CR-928 (S.D. Tex. 2017) (unpublished) (denying motion to suppress on the grounds that police officer acted in good faith in obtaining search warrant based in part on NCMEC search).

For the first time in his written closing argument [Doc. 123], Tolbert relies on the Supreme Court's very recent decision in *Carpenter v. United States*, No. 16-402, — U.S. —, 138 S. Ct. 2206 (2018) (Roberts, J.) to argue that none of the exceptions to the warrant requirement

can apply here. Specifically, Tolbert contends that it was improper for law enforcement to use grand jury subpoenas directed toward AOL and CenturyLink in order to find out identifying information relating to his IP address and his email accounts. According to Tolbert, under *Carpenter* this action constituted a "search" that required a warrant, not a mere subpoena. However, Tolbert attempts to stretch *Carpenter* too far.

In *Carpenter*, after the FBI identified the cell phone numbers of several robbery suspects, prosecutors were granted court orders to obtain the suspects' cell phone records under the Stored Communications Act. Among this information was cell-site location information (CSLI). Each time a phone connects to a radio antenna or "cell site," it generates a time-stamped record, or CSLI, which wireless carriers collect and store for their own business purposes. In *Carpenter*, wireless carriers produced CSLI for the defendant's phone, and the Government was able to obtain 12,898 location points cataloging Carpenter's movements over 127 days—an average of 101 data points per day. Carpenter moved to suppress the data, arguing that the Government's seizure of the records without obtaining a warrant supported by probable cause violated the Fourth Amendment. The Supreme Court agreed. It noted that individuals have a reasonable expectation of privacy in the whole of their physical movements, and that allowing government access to these types of comprehensive cell-site records without a warrant contravenes that expectation. The Court then noted that in *United States v. Jones*, 565 U.S. 400 (2012), it had recognized the privacy concerns raised by GPS monitoring, and stated that the privacy interests in CSLI data was even greater because it gives the Government the ability to retrace a person's past whereabouts with near-perfect accuracy, subject only to the five-year retention policies of most wireless carriers. The Supreme Court contrasted this high expectation of privacy in the exhaustive and revealing chronicle of CSLI location information with the much lower

expectation of privacy in some types of information voluntarily turned over to third parties, such as bank records and run-of-the-mill phone records. *Id*. at 2216 (citing *United States v. Miller*, 425 U.S. 435 (1976) (no expectation of privacy in financial records held by a bank), and *Smith v. Maryland*, 442 U.S. 735 (1979) (no expectation of privacy in records of dialed telephone numbers conveyed to telephone company)). In *Miller*, while investigating the defendant for tax evasion the Government subpoenaed his banks, seeking several months of canceled checks, deposit slips, and monthly statements. The Court concluded not only was defendant unable to assert possession or ownership of the records because they belonged to the banks, 442 U.S. at 440, but also that there was a limited expectation of privacy in the records because the checks were "not confidential communications but negotiable instruments to be used in commercial transactions," and the bank statements contained information "exposed to [bank] employees in the ordinary course of business." *Id*. at 442. The Supreme Court then concluded that Miller had "take[n] the risk, in revealing his affairs to another, that the information [would] be conveyed by that person to the Government." *Id*. at 443.

The information subpoenaed by law enforcement in this case is much more like the bank and telephone records in *Miller* and *Smith* than the comprehensive, detailed, and long-term location information in *Carpenter*. The grand jury subpoenas in this case (Ex. J) requested identifying information, such as the name and address of the person who opened the account, the date the account was opened, the detailed method of payment, telephone numbers used to access the internet, email address, connection address, IP address, and any identifying information. The privacy interest in this type of identifying data, which presumably any AOL or CenturyLink employee could access during the regular course of business, simply does not rise to the level of

the evidence in *Carpenter* such that it would require law enforcement to obtain a search warrant. The grand jury subpoenas were valid.

Thus, the good faith exception applies, and the motion to suppress will be denied.

**IV. Inevitable Discovery**

Subject to a few exceptions, evidence obtained in violation of the Fourth Amendment will be suppressed under the exclusionary rule; the inevitable discovery doctrine is one such exception. *United States v. Cunningham*, 413 F.3d 1199, 1203 (10th Cir. 2005). Under it, illegally obtained evidence may be admitted if it "ultimately or inevitably would have been discovered by lawful means." *Nix v. Williams*, 467 U.S. 431, 444 (1984). The "inevitable discovery exception applies whenever an independent investigation inevitably would have led to discovery of the evidence, whether or not the investigation was ongoing at the time of the illegal police conduct." *United States v. Larsen*, 127 F.3d 984, 986 (10th Cir. 1997). The government bears the burden of proving by a preponderance of the evidence that the evidence would have been discovered without the Fourth Amendment violation. *Cunningham*, 413 F.3d at 1203.

In both *Cunningham* and *United States v. Souza*, 223 F.3d 1197 (10th Cir. 2000), the Tenth Circuit applied inevitable discovery to situations like the one here, where there was one line of investigation that would have led inevitably to the obtaining of a search warrant by independent lawful means. In *Cunningham*, police searched the defendant's home after getting his consent. 14 F.3d at 1202. The defendant later contested the search, claiming his consent was coerced. *Id*. The court held that even if the search was illegal, the evidence was admissible because the officers "would have obtained a search warrant" if the search had not occurred. *Id*. at 1205. Similarly, in *Souza* police illegally opened a UPS package that contained drugs. 223 F.3d at 1200, 1202. The Tenth Circuit held the evidence admissible under inevitable discovery

because the officers "would have obtained a warrant" had the illegal search not occurred. *Id*. at 1206. Thus, evidence should not be excluded when the investigation would inevitably have discovered the contested evidence by lawful means.

In this case, the Government has met its burden to show that the evidence provided to NCMEC in the various CyberTips would have inevitably led law enforcement to obtaining a warrant and searching Tolbert's home even if NCMEC, Pena, and Altamirano had not opened the attachment to Tolbert's email before doing so. In its various CyberTips to NCMEC, which contained only information collected by a private entity, AOL transmitted a significant amount of information regarding the email accounts of the senders, including the originating email addresses, the email addresses of the intended recipient(s), the names of the files that were hash-matched using AOL's IDFP, the hash values for those files, the IP addresses from which the emails originated, and the subjects of the emails. In this case, that included the email addresses ddt123abc@aol.com and donnieisagod@aol.com, as well as the IP address 67.0.46.137. Then, a NCMEC analyst ran "open source" queries—that is, he or she used information available to members of the public online—with regard to the information described above. The open source query of the IP address showed that the sender's location was in Albuquerque, New Mexico and the internet service provider was Century Link. Searching the email address ddt123abc@aol.com showed a profile on IMGSRC for a user calling himself "YUNGMUFFMAN[7]," whose profile said that his real name was "Donnie" and that his email address was ddt666abc@gmail.com. That profile also gave a date of birth and the following statement under "User info": "I love girls between 8-15. someone [sic] told on me got my other 2 email accounts cancelled. AOL has

[7] The Government presented evidence at the hearing that this username conveys that the owner is a man who likes the genitalia of young women. Trans. 4/25/2018 at 93-94, 97-98.

something that reads your emails." Then, the NCMEC performed a search on open sources for the email address donnieisagod@aol.com and found a blank profile for "Don Tolbert." At this point, the email and IP addresses found in the header information sent by AOL to NCMEC pointed to a Don or Donnie Tolbert in Albuquerque, New Mexico with a stated sexual interest in young girls who had sent an email with an attachment with the same hash value as a known file containing child pornography. From there, the NCMEC analyst searched the National Sex Offender Public Website for the name "Don Tolbert." That search, in turn, led to a hit on "Donald Alvin Tolbert," a sex offender in Albuquerque who not only was convicted of criminal sexual contact of a minor under age thirteen, but who also had the same date of birth as "YUNGMUFFMAN," the person with the IMGSRC profile with a professed sexual interest in young girls. The NCMEC then transmitted this information—all of which either had been obtained from a private party or generated from publicly available sources—to the New Mexico Attorney General's Office.

At this point, without looking at the attachment in question or opening the emails themselves, the NMAGO would have had ample evidence to support probable cause for a search warrant to open the emails and their attachments, and for NMAGO to continue its own investigation. *See* Trans. 4/24/2018 at 202-204. In fact, this is what Pena did by conducting his own open source investigation (which also led him to Donald Tolbert, registered sex offender) and by securing grand jury subpoenas for the email addresses identified by AOL in the CyberTips. At that point, the evidence that AOL provided in response to the subpoena would have led law enforcement to Tolbert's residence, as well as to his mother's home—all without opening the emails or their attachments.

There are two additional sources of information that would have led to inevitable discovery of the evidence without opening the five emails or their attachments. They are the two additional CyberTips from AOL to NCMEC that are not the subject of the motion to suppress. *See* Exs. B (CyberTip #1522765) and C (CybertTip #1544073). Those two CyberTips—dated July 18, 2012 and August 8, 2012, respectively— also both referred to emails containing images that AOL hash-matched with known child pornography. *Id.* The first report concerns an email sent from username "Donnie T" at dat666@aol.com. Ex. B. Using open source searches, the NCMEC analyst was able not only to trace the sender's IP address to Albuquerque, New Mexico, but also to link that email address to someone using the name "Donnie Tolbert." *Id*. The NCMEC analyst then forwarded this information to the New Mexico Attorney General's Office, ICAC Task Force. *Id*.; *see also* Trans. 4/24/2018 at 96-97. With regard to the second CyberTip dated August 8, 2012, *see* Ex. C, it referred to an email sent from abc123ddt@aol.com and which contained the same file attachment referred to in Government's Exhibit B. *See* Exs. B and C; Trans. 4/24/2018 at 99-100. Again, the IP address led the analyst to Albuquerque, New Mexico. Based on this information, the NCMEC analyst also forwarded this report to the New Mexico Attorney General's Office. Both Pena and Altamirano testified credibly that in the absence of the other five CyberTips, and in the absence of anyone from law enforcement actually viewing the images contained in the attachments, they would have continued to investigate these two additional reports. Trans. 4/25/2018 at 87-97, 202-06. The information available from public sources—just like it did with the five other CyberTips previously discussed—would inevitably have led to the same open source searches that revealed the identity of Donald Albert Tolbert as the alleged sender of the emails, and then eventually to the search warrants for his and his mother's homes.

Thus, the same evidence that Tolbert seeks to suppress would have been inevitably discovered through independent means. Accordingly, the motion to suppress will be denied

**IT IS THEREFORE ORDERED**.that Defendant's *Motion to Suppress Evidence Obtained in Violation of the Fourth Amendment Under United States v. Ackerman* [Doc. 90] is **DENIED.**

**UNITED STATES DISTRICT JUDGE**