**NO. 18-5578**

---

**UNITED STATES COURT OF APPEALS**
**FOR THE SIXTH CIRCUIT**

---

**UNITED STATES OF AMERICA**

**Plaintiff-Appellee,**

**v.**

**William J. Miller,**

**Defendant-Appellant.**

---

**On Appeal From The Judgment**
**Of The United States District Court**
**For the Eastern District of Kentucky at Covington**
**Honorable David L. Bunning**

---

**District Court No. 2:16-cr-00047-1**

---

# BRIEF OF APPELLANT WILLIAM J. MILLER

---

ERIC G. ECKES
(CJA Appointed)
Pinales Stachler Young Burrell & Crouse Co., L.P.A.
455 Delta Ave., Suite 105
Cincinnati, Ohio 45226
Telephone: (513) 252-2723
Fax: (513) 252-2751

**ORAL ARGUMENT REQUESTED**

**CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT**

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, Defendant-Appellant makes the following disclosure of corporate affiliations:

1. Is said party a subsidiary or affiliate of any parent corporation not named in this appeal? **No**

2. Is there a publicly owned corporation, not a party to the appeal, that owns greater than ten percent (10%) of the party's stock? **No**

/s/ Eric G. Eckes
Eric G. Eckes
Counsel for Defendant-Appellant William J. Miller

# TABLE OF CONTENTS

# TABLE OF AUTHORITIES

## Federal Cases

**Federal Statutes**



**Rules**

## STATEMENT REGARDING ORAL ARGUMENT

Defendant-Appellant, William J. Miller, respectfully requests an opportunity to present oral argument. Oral argument would be useful for the Court in understanding the issues in this case, particularly the complicated suppression issue involving modern technology. Likewise, there is minimal case law involving the denial of Miller's suppression motion, and oral argument would assist this Court in properly addressing the issue.

## STATEMENT IN SUPPORT OF JURISDICTION

This is an appeal from the judgment order entered by the district court on May 29, 2018. (Judgment, R. 88, Page ID # 444). Miller filed timely notice of appeal on May 31, 2018. (Notice of Appeal, R. 90, Page ID # 452). This Court has jurisdiction over this appeal pursuant to 28 U.S.C. § 1291.

## ISSUES PRESENTED FOR REVIEW

1. Whether the District Court Erred When Denying Miller's Motion to Suppress?

2. Whether Miller's Due Process Rights and his Right to Confrontation, Pursuant to the Fifth and Sixth Amendments of the United States Constitution, were Violated when the District Court Overruled his Objection to the Admission of the Cybertipline Report?

3. Whether the District Court Erred when Denying Miller's Rule 29 Motion?

## STATEMENT OF THE CASE

William Miller was initially indicted on November 17, 2015 for transportation

of child pornography and possession of child pornography, in violation of 18 U.S.C. § 2252(a)(1) and 18 U.S.C. § 2252(a)(4)(B) respectively. (Indict., R. 1, Page ID # 1). The United States filed two superseding indictments on January 12, 2017 and November 9, 2017. (Indict., R. 20, Page ID # 88) (Indict., R. 62, Page ID # 327). The second superseding indictment charged Miller with one count of receipt of child pornography, six counts of distribution of child pornography, and one count of possession of child pornography, in violation of 18 U.S.C. § 2252(a)(2) and 18 U.S.C. § 2252(a)(4)(B) respectively. (Indict., R. 62, Page ID # 327).

On January 31, 2017, Miller filed a Motion to Suppress in which he attacked the validity of two separate searches and the seizure of the contents of email account miller694u@gmail.com and email attachments. (Motion to Suppress, R. 27, Page ID # 109). Oral argument was heard on the Motion to Suppress on April 12, 2017 and April 19, 2017. (Tr. of Motion Hrg. Vol. 1, R. 99, Page ID # 964) (Tr. of Motion Hrg. Vol. 2, R. 100, Page ID # 990). The district court issued a Memorandum Order denying Miller's Motion to Suppress on June 23, 2017. (Order, R. 48, Page ID # 259).

On January 16, 2018, a jury trial commenced. (Minute Entry, R. 69). During the trial, the district court admitted a National Center for Missing and Exploited Children's ("NCMEC") CyberTipline Report over Miller's objection. (Jury Trial Day 1 Tr., R. 95, Page ID # 536). After the United States' case-in-chief, Miller orally

motioned for a judgment of acquittal. (Jury Trial Day 2 Tr., R. 96, Page ID # 805). The district court denied the motion. (Jury Trial Day 2 Tr., R. 96, Page ID # 809). Miller renewed the motion for judgment of acquittal after the jury returned its verdict of guilty. (Jury Trial Day 3 Tr., R. 97, Page ID # 907). The district court denied the renewed motion. (Jury Trial Day 3 Tr., R. 97, Page ID # 907-08). On May 29, 2018, the district court sentenced Miller to 150 months imprisonment. (Judgement, R. 88, Page ID # 445).

## STATEMENT OF THE FACTS

On July 9, 2015, Google became aware that two flagged images of apparent child pornography were being uploaded to an email in the account miller694u@gmail.com. (R and R, R. 41, Page ID # 217). Google learned of the potential uploading by utilizing a modern proprietary "hashing" technology. (*Id.*) In effect, Google's technology searches every file loaded onto its network to compare the file's hash value against a list of hash values of potentially illegal files. This search process is automated, and the attachments were seized and forwarded to NCMEC without any manual review of the attachments by Google. (*Id.* at Page ID # 219). Google also provided the IP addresses that were used to create the Google account ("Creation IP") and to upload the two files in question ("July Email IP"). (*Id.*)

Upon receipt of the attachments from Google, NCMEC conducted an

investigation, which was formalized as a Cybertipline Report. (Cybertipline Report, R. 33-2, Page ID # 167). As part of the NCMEC investigation, an analyst "add[ed] additional value" to the information provided by Google in the following ways: 1.) the analyst "geolocated" the IP addresses provided by Google to a specific alleged longitude and latitude, and 2.) the analyst conducted "online open source searching" which resulted in the analyst finding and attaching to the Cybertipline Report a Tumblr page allegedly associated with the suspect. (Jury Trial Day 1 Tr., R. 95, Page ID # 529, 541-42, 544) (Cybertipline Report, R. 33-2, Page ID # 167-177).

On August 13, 2015, Detective Aaron Schihl received the Cypbertipline Report from NCMEC, which included the attachments from the email. (R and R, R. 41, Page ID # 220). At this point, no person had opened or reviewed the email attachments. Detective Schihl opened the attachments and reviewed them without a warrant. (*Id*.). Detective Schihl subsequently obtained a warrant to search Mr. Miller's home. (*Id*.) The probable cause listed in the warrant application was based on Detective Schihl's observations after searching the attachments. (*Id*.) (Jury Trial Day 1 Tr., R. 95, Page ID # 572).

The search of the home revealed child pornography images on an external hard drive and other electronic evidence connecting the hard drive to a computer owned by Miller. (Jury Trial Day 2 Tr., R. 96, Page ID # 759, 771, 773, 778). No evidence of child pornography was found on Miller's computer, or any of the other

numerous electronic devices seized in the search. (*Id.* at Page ID # 750-51).

A warrant was then utilized to obtain all data from the email account miller694u@gmail.com. (Jury Trial Day 1 Tr., R. 95, Page ID # 583). The account contained around 4000 emails, which consisted almost entirely of ads from adult dating websites, and gchats (Google's messaging application within gmail) between the user of the email address and women in Africa. (*Id.* at Page ID # 588-89).

The email address also contained emails between the user and a person named "Larry Ward" where child pornography was sent and received. (*Id.* at Page ID # 605-13) (Jury Trial Day 2 Tr., R. 96, Page ID # 630-34). In addition, there was an email that coincided with the July 9th, 2015 email from which Google became aware of the potential uploading of child pornography. (Jury Trial Day 2 Tr., R. 96, Page ID # 639-40). The July 9th email and the Larry Ward exchanges in May were the basis for all the distribution and receipt counts. The possession count involved the images and videos found on the external hard drive.

The Google warrant materials also provided the Creation IP and the July Email IP. The IP addresses did not match. Notably, Mr. Miller's home public IP address from July of 2014 through July of 2015 was 74.132.31.22. (Jury Trial Day 2 Tr., R. 96, Page ID # 673), which matches the July Email IP. The Creation IP from January of 2015 (and for many other future log-ins to that account) was 74.139.62.188. (*Id.* at Page ID # 672).

In addition, the miller694u@gmail.com emails included multiple automated alerts stating that the email address had been logged into from a new location and/or from a new internet service provider (*i.e.* Chrome vs. Firefox). (*Id.* at Page ID # 609, 669-70). The location of some of the log-ins suggested that the log-ins occurred in Louisville, Kentucky, nowhere near Miller's home. (*Id.* at Page ID # 668). Critically, one of the Louisville, KY new login-in alerts was generated on May 15, 2015, a date where child pornography was distributed and received by the user of miller694u@gmail.com. (*Id.* at Page ID # 669-71).

Most importantly to Miller's defense, several emails were addressed to "Fred" ("the Dear Fred emails"). (*Id.* at Page ID #674-79). These emails involved the purchasing of an LG phone and tablet from Sprint. (*Id.*). The emails contained attachments that showed an LG phone and tablet were purchased and paid for with a credit card in the name of Fred Miller. (*Id.* at Page ID # 678-79). Essentially, the "Dear Fred" emails, the new login alerts, and the child pornography receipt/distribution emails were the only emails in the entire 4000 that were unrelated to gchats and dating website ads/requests.

Miller argued that there was a reasonable alternate explanation to the allegation that he was the user of miller694u@gmail.com. The alternate explanation was that his brother, Fred Miller, used the email address, saved the child pornography to the external hard drive, and created a fake internet "persona" as his

younger brother Bill for the chats (Skype and gchat) and dating websites, including the Tumblr page. Witnesses testified that Fred Miller often used the computers in Miller's home (thereby using the public IP address of the home router) and had access to the external hard drive. (*Id.* at Page ID # 813, 820, 825).

## SUMMARY OF ARGUMENT

First, the district court should have granted Miller's suppression motion. The government conducted a search of the email attachments when a detective opened those attachments without a warrant. The warrantless search was a trespass on constitutionally protected space, thereby triggering Fourth Amendment protection notwithstanding any limitations of the *Katz* test. Alternatively, when applying the *Katz* test, Miller had a reasonable expectation of privacy in email attachments, which was violated when the detective exceeded the scope of the prior search by Google. In effect, the attachments were a sealed private container that was not previously opened by any private searcher, rendering the private search doctrine inapplicable. Moreover, the initial hash value search conducted by Google was a violation of Miller's Fourth Amendment rights as Google was a state actor when conducting its search. Second, the district court further erred when admitting NCMEC's Cybertipline Report over Miller's objection because the admission violated *Crawford*, and greatly prejudiced Miller. Third, there was insufficient evidence to

convict Miller on all counts because there was significant evidence of additional, open access to both the email account in question and the external hard drive.

## ARGUMENT

### I. The District Court Erred when Denying Miller's Motion to Suppress.

In reviewing the district court's denial of a motion to suppress, the appellate court uses two complementary standards of review in which factual findings are reviewed for clear error and questions of law are reviewed *de novo*. *United States v. Blair*, 524 F.3d 740, 747 (6th Cir. 2008). Whether a search was reasonable under the Fourth Amendment is a question of law. *Id.*

The Fourth Amendment protects an individual against unreasonable searches and seizures. "It is fundamental that all searches without a warrant are unreasonable unless it can be shown that they come within one of the exceptions to the rule that a search must be made pursuant to a valid warrant." *Coolidge v. New Hampshire*, 403 U.S. 443, 454-455 (1971) (". . . the most basic constitutional rule in this area is that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment-subject only to a few specifically established and well delineated exceptions . . . [,which] . . . are 'jealously and carefully drawn.").

#### a. The warrantless opening of Miller's emails constituted a "search" under the Fourth Amendment.

A "search" occurs either when the government violates a person's "reasonable

expectation of privacy" or when the government "obtains information by physically intruding on a constitutionally protected area." *United States v. Jones*, 565 U.S. 400, 406, n.3 (2012).

**i. Reasonable Expectation of Privacy**

A person has a "reasonable expectation of privacy in the contents of his emails 'that are stored with, or sent or received through, a commercial ISP.'" *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). In most situations, a subscriber agreement will not be "sweeping enough to defeat a reasonable expectation of privacy in the contents of an email account." *Id*. at 286.

Here, Miller had a reasonable expectation of privacy in his emails and their attachments. The unfavorable nature of the emails, which suggest sexual promiscuity outside of marriage, indicates that the user had not intended for the emails to be viewed. These negative aspects illustrate a subjective expectation of privacy. *See Id.* at 284. In addition, the expectation of privacy was objectively reasonable. Although an internet service provider was used—Google—the email contents were not being exposed to a third party in a manner that forfeited Miller's reasonable expectation of privacy. *See Id.* (analogizing an internet service provider to a transporter of mail); *see also Carpenter v. United States*, 138 S. Ct. 2206, 2269 (2018) (Gorsuch, N., dissenting) ("[F]ew doubt that e-mail should be treated much like the traditional mail it has largely supplanted—as a bailment in which the owner retains a vital and

protected legal interest."). Rather, Miller gave Google limited access rights. Such limited access is not, however, a key to analyze and disseminate Miller's personal information without restraint. *Warshak,* 631 F.3d at 284; *see also Carpenter*, 138 S. Ct. at 2263 (Gorsuch, N., dissenting) ("Consenting to give a third-party access to private papers that remain my property is not the same thing as consenting to a *search of those papers by the government*.") (emphasis in original). Therefore, Miller maintained an objectively reasonable expectation of privacy in the contents of his emails. Accordingly, the warrantless opening of Miller's emails constituted a search under the Fourth Amendment.

**ii. Physical Trespass**

The warrantless opening of Miller's private email correspondence also qualified as a "[physical intrusion] on a constitutionally protected area." *Jones*, 565 U.S. at 406, n.3. The Fourth Amendment provides the same protection against governmental invasions that the common law did at the time of the founding. *Id.* at 950, 953. "At common law, a suit for trespass to chattels could be maintained if there was a violation of 'the dignitary interest in the inviolability of chattels.'" *Id.* at 957, n.2 (Alito, J., concurring).

In *United States v. Ackerman*, 831 F.3d 1292, 1308 (10th Cir. 2016), the Tenth Circuit found that opening email attachments constituted a search whether viewed through the lens of *Jacobsen/Walter/Katz*, or through the traditional trespass test

suggested by *United States v. Jones*, 132 S.Ct. 945 (2012). According to the Tenth Circuit, the "warrantless opening of (presumptively) private correspondence . . . seems pretty clearly to qualify as exactly the type of trespass to chattels that the framers sought to prevent when adopting the Fourth Amendment." *Id*. at 1307.

In this case, Detective Schihl's actions constituted a search because his opening of the email attachments involved a "physical intrusion (a trespass) on a constitutionally protected space or thing ('persons, houses, papers, and effect') for the purpose of obtaining information." *Ackerman,* 831 F.3d at 1307. Miller had substantial legal interests in his private email correspondence, and thus, had a Fourth Amendment interest in its protection. *See generally* 18 U.S.C.S. § 2701 (creating a set of privacy protections for electronic communications held by providers of "electronic communication services"); *see also United States v. Kernell*, 2010 U.S. Dist. LEXIS 36477, *13-15 (E.D. Tenn. Mar. 17, 2010) (finding that an individual has a property right to the exclusive use of the information and pictures contained in their email account). Further, the government's contact with Miller's emails was intentional and violative of his rights in those emails. Accordingly, law enforcement cannot open the email attachments free from the Fourth Amendment's warrant requirement.

Whether analyzed under the *Katz* test or the traditional trespass test, it is clear that a search took place. Notably, however, the *Katz* test requires further analysis

regarding the private search doctrine. Importantly, the private search doctrine is a limitation on *Katz*, not the traditional trespass inquiry. Just because a private party may use a modern technology to frustrate a person's reasonable expectation of privacy in their email attachments, "Fourth Amendment protections for your papers and effects do not automatically disappear." *Carpenter*, 138 S. Ct. at 2268 (Gorsuch, N., dissenting) (emphasis in original) (explaining how the third-party doctrine is a limitation on *Katz* and does not apply to the tradition trespass analysis). Indeed, "True to [the words of the Fourth Amendment] and their original understanding, the traditional approach asked if a house, paper, or effect was *yours* under law. No more was needed to trigger the Fourth Amendment." *Carpenter*, 138 S. Ct. at 2267-68 (Gorsuch, N., dissenting) (emphasis in original). Thus, regardless of how this Court views the *infra* argument regarding the private search doctrine, Miller's motion to suppress should have been granted.

**b. The government exceeded the initial search by Google, thereby conducting an unreasonable warrantless search.**

The Supreme Court addressed the scope of the private search doctrine in both *Walter v. United States*, 447 U.S. 649 (1980), and *United States v. Jacobson*, 466 U.S. 109 (1984). The facts in this case more closely align with *Walter*. *See United States v. Keith*, 980 F. Supp. 2d 33 (D. Mass. 2013) (finding *Jacobsen* inappropriate where NCMEC, a state actor, opened and viewed the contents of a file obtained from AOL's private search).

In *Walter*, law enforcement was provided illegal movies with labels on them. *Walter*, 447 U.S. at 652. The labels on the movies were quite descriptive. *Id*. at 654. Indeed, the labels described "the nature of the contents of these films." *Id*. at 654. While the films initially were found in a mailed box, which had been opened by a private searcher, the films themselves were separate unopened containers. In effect, the labels on the films clearly indicated the illegal nature of what was inside the containers. When law enforcement searched the films, a distinct and separate warrantless search took place. *Id*. Emphasizing that the law had been clear "ever since 1878" when it was "established that sealed packages in the mail cannot be opened without a warrant," the Supreme Court suppressed the contents of the films. *Id*. (citing *Ex Parte Jackson*, 96 U.S. 727 (1877)). This suppression occurred "notwithstanding that the nature or the contents of these films was indicated by the descriptive material on their individual containers." *Id*.

The comparison between *Walter* and the facts of this case is evident. The private searcher—Google—conducted one type of new and modern search of the entire email address contents. The private searcher then seized and provided two individual containers to law enforcement (via NCMEC) with descriptive labels on the containers (hash values). Detective Schihl then conducted a separate and distinct warrantless search on the containers (the email attachments). The *Keith* Court described the logical comparison of *Walter* to this factual scenario as follows:

"Although the media in which the criminally obscene material was stored are different in *Walter* and this case, the pattern is the same. A label (here, hash value) that is examined without opening the film or file suggested the nature of the contents." *Keith*, 980 F. Supp. 2d at 42. When opining on the specific scenario presented in Miller's case, the *Keith* Court said, "[I]t cannot seriously be contended that the law enforcement agency could open and inspect the contents of the file without regard to the Fourth Amendment's warrant requirement."[1] *Id.* at 41-42.

The suppression litigation in the district court involved arguments of whether hash values could be distinguished from the labels in *Walter*. For instance, the Magistrate Judge's R and R distinguished hash values and labels by recognizing that hash values are much better than an average label at identifying and revealing the contents of a container. (R and R, R. 41, Page ID# 238). However, the illegality of the search in *Walter* did not hinge on how precise the labels were. *Walter* holds that when law enforcement receives a sealed container, a warrant is required even if the *nature of the contents of the container* are indicated (or revealed) by descriptive material on the outside of the container. *Walter*, 447 U.S. at 654.

[1] In *Keith*, the email attachments were seized by AOL and provided to NCMEC. NCMEC then opened the attachments before providing them to the police, and thus, the *Keith* Court had to decide whether NCMEC was a state actor. In that context, the *Keith* Court opined that if the police were the first to open the attachments (like in Miller's case), then "it could not seriously be contended" that a warrant was not required. *Id*. at 41-42.

Although not binding precedent, the Tenth Circuit addressed a similar situation in *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016). In *Ackerman,* AOL's automated filter system—using hash values—stopped an email being sent by the defendant. The filter noted that one of the four attachments contained child pornography. *Id.* at 1294. AOL then sent a report to NCMEC through the Cybertipline. The report contained the defendant's email and the attachments. Similar to Detective Schihl, a NCMEC analyst opened and reviewed the attachments and confirmed they contained child pornography. The analyst then reported the information to law enforcement agents.

The Tenth Circuit found that NCMEC, as a state actor, had exceeded the original search by AOL. The *Ackerman* court analyzed the issue citing to *United States v. Jacobsen,* 466 U.S. 109, 118 (1984). In *Jacobsen*, the Supreme Court wrote "[t]he Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated. In such a case the authorities have not relied on what is in effect a private search, and therefore presumptively violate the Fourth Amendment if they act without a warrant." *Id*. at 118. In other words, assuming *arguendo* that this Court finds Google to be private actor, the question becomes whether the government could have learned more information than what the Google search revealed. *See Ackerman,* 831 F.3d at 1306. The court in *Ackerman* answered this question in the affirmative finding that

the NCMEC analyst had opened the attachments and looked at the contents of the email. Therefore, the Court held that NCMEC exceeded the original search.

"Under the private search doctrine, the critical measures of whether a governmental search exceeds the scope of the private search that preceded it are how much information the government stands to gain when it *re-examines* the evidence and, relatedly, how certain it is regarding what it will find." (R and R, R. 41, Page ID# 231) (quoting *Lichtenberger*, 786 F.3d at 485-86) (emphasis added). Simply put, Detective Schihl's search was not a *re-examination*. The Google search was different not only in scope, but in type from the search of Detective Schihl. The attachments were uncompromised when sent to Detective Schihl; he broke the seal. In the words of the Supreme Court in *Walter*, "the [hash values] are not sufficient to support a conviction . . . Further investigation -- that is to say, a search of the contents of the [email attachments] -- was necessary in order to obtain the evidence which was to be used at trial." *Walter*, 447 U.S. at 654.

The law—as set forth in *Walter*—directs law enforcement to get a warrant when they receive a sealed container even when a label (or hash value) describes the illegal nature of the contents. Therefore, the district court's denial of Miller's motion to suppress is at direct odds with a significant holding of *Walter*, while simultaneously expanding the private search doctrine. With such an expansion, law enforcement would now seem to be expected to ascertain whether a private party

had used a modern technology to learn information about the potential contents of a citizen's unopened container. If the modern technology utilized by the private party has the capability to frustrate a citizen's reasonable expectation of privacy in the contents of a citizen's sealed container, law enforcement would be excused from the Fourth Amendment's warrant requirement.

In short, Miller requests this Court reaffirm the law of *Walter*, and not expand the private search doctrine. Such an expansion would create significant and detrimental means for avoidance of the Fourth Amendment's warrant requirement. The government would be permitted to search through all sorts of private and sensitive information intended to be hidden from the public inside a sealed container. Searching a citizen's sealed container would be free of the warrant requirement whenever a private party uses modern technology to provide law enforcement a reliable indication of the contents of the container.

**c. Google was a state actor when it searched miller694@gmail and seized specific email attachments.**

In *Lugar v. Edmondson,* the Supreme Court held that an entity is a state actor if the constitutional deprivation is "fairly attributable to the State." 457 U.S. 922, 937 (1982). The Sixth Circuit looks at three tests to determine if an action is under color of law by a state actor and thus fairly attributable to the state. *Lansing v. City of Memphis,* 202 F.3d 821, 828 (6th Cir. 2000). The tests include public function, state compulsion, and the nexus test. *Id*. at 829. Google was a state actor in this case

because of its nexus relationship with NCMEC, an entity that qualifies as a state actor under the public function test.

The public function test requires that the private entity or individual utilize a power that has been traditionally exclusive to the state. *Carl v. Muskegon Cty.,* 763 F.3d 592, 596 (6th Cir. 2014); *Romanski v. Detroit Entm't, L.L.C.,* 428 F.3d 629, 637 (6th Cir. 2005). Given the nature of its purpose and duties, NCMEC exercises law enforcement powers traditionally exclusive to the state and its law enforcement officers. In *Romanski*, the Sixth Circuit delineated when an entity is a state actor that offers traditionally exclusive law enforcement power. 428 F.3d at 637 (entity is a state actor when given "broad delegation of power" traditionally exclusive to police).

In effect, NCMEC is a state actor because it enjoys a "broad delegation of power" that provides it with more law enforcement powers than private individuals could invoke. *See* 18 U.S.C.A. § 2258(A) (West); 42 U.S.C.A. § 5773(B) (West). For example, NCMEC has statutorily delegated powers which *mandate* that it is the *sole* collaborator—with regards to its duties—with state and federal law enforcement. *U.S. v. Ackerman,* 831 F.3d 1292, 1296 (10th Cir. 2016). Of particular interest to this case is the Cypertipline. NCMEC, to the exclusion of all others, maintains the tipline. *Id*. In addition, Internet Service Providers must report any exploitation to NCMEC, not law enforcement agencies. *Id*. Then, NCMEC must forward a report to law enforcement. *Id*. In addition, unlike a private entity, NCMEC

can receive and forward the child pornography without prosecution. *Id*. at 1297.

Although the Sixth Circuit has not addressed whether NCMEC qualifies as a state actor, the Tenth Circuit, in a detailed and thorough opinion, in *Ackerman* held that NCMEC qualifies as a state actor because it performs the police function as described above. *Id*. Furthermore, the statutory construction of NCMEC qualifies it as a governmental entity in and of itself. *Id*.[2] With NCMEC as a state actor, the next question becomes whether Google has a nexus relationship with NCMEC.

In the Sixth Circuit, a private entity's action is a state action "when there is a sufficiently close nexus between the state and the challenged action of the regulated entity so that the action of the latter may be fairly treated as that of the state itself." *Lansing v. City of Memphis,* 202 F.3d 821, 830 (6th Cir. 2000). Additionally, a private entity may be a state actor if it is a willful participant in joint activity with the State or its agent." *Wilkerson v. Warner*, 545 F. App'x 413, 420 (6th Cir. 2013); *See also Marie v. Am. Red Cross*, 771 F.3d 344, 363 (6th Cir. 2014) (applying the entwinement test for determining if a state action exists).

The determination of whether a private entity is a state actor must take into

[2] The Tenth Circuit analogized NCMEC to Amtrak and the Supreme Court ruling in *Case Lebron v. National R.R. Passenger Corp.* 513 U.S. 374 (1995). The Tenth Circuit found similarities between Amtrak and NCMEC: both have a special statute for governmental goals which are heavily regulated with specific procedures, and the statute provides obligations and powers to the entities. Further, both have funding connected to the federal government.

consideration all circumstances and facts and no one fact is dispositive. *Brentwood Acad. v. Tennessee Secondary Sch. Athletic Ass'n,* 531 U.S. 288, 295-96 (2001). Further, "only by sifting facts and weighing circumstances can the nonobvious involvement of the State in private conduct be attributed its true significance." *Burton v. Wilmington Parking Auth.,* 365 U.S. 715, 722 (1961).

In short, NCMEC is law enforcement and Google has become NCMEC's agent through its close relationship and collaborative crime fighting efforts. Google is not only tied to NCMEC through the mandatory reporting requirements and penalties for a failure to report, but also through its requirement to preserve evidence. 18 U.S.C. 2258A(a), (e), (f). To be sure, Google and NCMEC have developed a close and collaborative relationship where NCMEC has intimate knowledge of Google's searching activities and encourages them. For example, as encouragement, NCMEC gives awards to Google for its efforts.[3]

In regard to collaboration, NCMEC provides hash values to Google to use in its searches, exhibiting NCMEC's knowledge of such searches. (Declaration of Cathy McGoff, R. 33-1, Page ID# 161). In return, Google provides hash values to NCMEC. (*Id*.). As further collaboration, Google redesigned the Cybertipline form

[3] https://www.washingtonpost.com/news/the-switch/wp/2015/05/06/how-google-and-other-tech-firms-fight-child-exploitation/?utm_term=.2367697e46fb

for NCMEC—the exact Cybertipline at issue in this case.[4] Google also proudly makes statements to the public that it has joined forces with NCMEC, that the organizations are collaborative partners, and the organizations should engage in "borderless communication."[5]

The above collaboration establishes a nexus, a nexus where NCMEC has full knowledge of Google's searches and assists them by providing additional hash values. Further, Google's intent in searching its users' email accounts (and forwarding the fruits of the searches immediately and automatically to NCMEC) cannot be said to be "entirely independent" of NCMEC's intent to collect evidence for prosecution. (R and R, R. 41, Page ID# 224). Google is directly and indispensably assisting NCMEC with collecting evidence, and therefore, Google's intent is clearly intertwined with NCMEC's law enforcement purpose.

## II. Miller's Due Process Rights and his Right to Confrontation, Pursuant to the Fifth and Sixth Amendments of the United States Constitution, Were Violated when the District Court Overruled his Objection to the Admission of the Cybertipline Report.

[4] http://www.prnewswire.com/news-releases/google-technology-makes-reporting-child-sexual-exploitation-easier-136318218.html

[5] https://googleblog.blogspot.com/2006/08/coalition-against-child-pornography.html; https://www.google.com/landing/protectchildren/;https://googleblog.blogspot.com/2013/06/our-continued-commitment-to-combating.html; http://www.prnewswire.com/news-releases/google-technology-makes-reporting-child-sexual-exploitation-easier-136318218.html; http://www.missingkids.com/partners/Google

The Sixth Amendment provides that, "[i]n all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him." The admissibility of out-of-court statements under the Confrontation Clause turns upon whether the statement is "testimonial." *Davis v. Washington*, 547 U.S. 813, 823 (2006). "Where testimonial statements are at issue, the only indicium of reliability sufficient to satisfy constitutional demands is the one the Constitution actually prescribes: confrontation." *Crawford v. Washington*, 541 U.S. 36, 68-69 (2004). Testimonial statements are thus inadmissible "unless the witness appears at trial or, if the witness is unavailable, the defendant had a prior opportunity for cross-examination." *Id.* at 54. Appellate review of objections like the one presented here are reviewed *de novo*. *United States v. Robinson,* 389 F.3d 582, 592 (6th Cir. 2004).

In *Melendez-Diaz v. Massachusetts*, 557 U.S. 305 (2009), the Supreme Court indicated that business records are not immune from scrutiny under the Confrontation Clause. Rather, all statements, whether contained in business records or not, are considered "testimonial" if they "were made under circumstances which would lead an objective witness reasonably to believe that the statement would be available for use at a later trial." *Id.* at 310 (quoting *Crawford*, 541 U.S. at 52). For instance, the Court in *Melendez-Diaz* concluded that "certificates of analysis" were testimonial because they were "functionally identical to live, in-court testimony" by the laboratory analysts stating the substance seized by the police was cocaine. *Id.* at

310-11. Therefore, whether or not the certificates qualified as business records, the analysts were subject to confrontation under the Sixth Amendment. *Id.* at 324.

Although the Sixth Circuit has yet to address the exact issue of Cybertipline Reports, the First Circuit has held that CyberTipline Reports are testimonial in nature. *See United States v. Cameron*, 699 F.3d 621 (1st Cir. 2012). In *Cameron*, Yahoo! received an anonymous report that child pornography images were contained in the defendant's Yahoo! account. *Id.* at 628. Yahoo! then sent a CP Report to NCMEC, who in turn sent a CyberTipline Report to the Maine State Police ICAC unit. *Id.* at 629. The First Circuit initially addressed whether the CyberTipline Report was a "statement" for purposes of the Sixth Amendment's Confrontation Clause. Holding that the CyberTipline Report was a statement, the court emphasized that the report went beyond simply furnishing pre-existing records. *Id.* at 651. Rather, the NCMEC employee who created the report "analyzed the information [from Yahoo!], picked the IP address from which the most recent image was uploaded, and included this information, along with the date and time of that upload, in the CyberTipline Report." *Id.* at 651. Thus, the CyberTipline Report conveyed an analysis that had not existed previously, making it a "separate, independent" statement. *Id.*

The First Circuit then concluded that NCMEC's CyberTipline Report was testimonial because the primary purpose of the report was to "establish or prove past

events potentially relevant to later criminal prosecution." *Id.* Indeed, the court found that the report specifically served as a conduit for passing information to law enforcement; the records did not exist before criminal activity was discovered, and the record was created for the express purpose of reporting criminal activity and identifying the perpetrator of that activity. *Id.* As such, the First Circuit held that the CyberTipline Report could not be admitted without giving the defendant the opportunity to cross-examine its author—i.e., the NCMEC employee who analyzed the information contained in the CP Report sent by Yahoo!. *Id.* at 651-52. *See also United States v. Morrissey*, 895 F.3d 541 (8th Cir. 2018) (assuming, without deciding, that the NCMEC confirmations were testimonial).

Here, the trial court admitted NCMEC's CyberTipline Report against Miller, despite the fact that he had no opportunity to cross-examine its author. As found in *Cameron*, the CyberTipline Report was a testimonial statement for purposes of the Sixth Amendment's Confrontation Clause. At trial, the executive director of NCMEC's Exploited Children Division testified to both the nature and the contents of the report. The executive director defined the CyberTipline as a "centralized reporting tool for child exploitation." (Jury Trial Day 1 Tr., R. 95, Page ID # 525). She continued, stating that the CyberTipline program receives information regarding child sexual exploitation and the analysts subsequently review that information and try to provide a location. (*Id.* at Page ID#529). She further made clear that the

analysts will often "add additional value" to the information provided by Google (i.e. conduct an investigation) before forwarding it to law enforcement. (*Id.*).

When the analyst is finished, they make the report available to the appropriate law enforcement agency. (*Id.*). Notably, "[t]he reports are only made available to law enforcement." (*Id.*). In fact, the reports may be accessed only through a virtual private network, where the report is password-protected. (*Id.* at Page ID#546). The unique username and password for these reports are made available specifically to the law enforcement agency to which NCMEC referred the report. (*Id.*). Once the report is made available to law enforcement, NMEC's involvement ends; NCMEC ceases its investigation. (*Id.* at Page ID # 547). Based on the foregoing, the CyberTipline Report was "made under circumstances which would lead an objective witness reasonably to believe that the statement would be available for use at a later trial." Thus, the trial court erred in admitting the CyberTipline Report against Miller when he had no opportunity to cross-examine the analyst that created the report.

The admission of NCMEC's report significantly prejudiced Miller. Miller maintained the same defense throughout trial: Somebody else, presumably Fred Miller, was using the email address where the child pornography was distributed and received. To that end, Miller argued that it was critical to recognize that the Creation IP in January of 2015 was not Miller's known public IP address. (Jury Trial Day 3 Tr., R. 95, Page ID # 877). Miller had the same IP address from July of 2014 until

July of 2015. A different public IP address created the Google account in question. (*Id*.) This fact was one of the main reasonable doubts presented in Miller's closing.

In rebuttal, the United States argued directly from the Cybertipline Report in the following inaccurate and misleading manner: the NCMEC analyst "geo-resolved both of the IP addresses that were given to it [the Creation IP and the July Email IP]," and those IP addresses "both resolve back to . . . the exact same latitude and longitude. The defendant's house." (*Id.* at Page ID # 891). This statement by the United States was both 1.) incorrect (the defense objected to facts not in evidence, which was overruled), and 2.) only able to be asserted because the defendant could not cross-examine the analyst.

First, the incorrect part. The Cybertipline report lists the following geolocated coordinates for both the Creation IP and the July Email IP: 39.023998, -84.562401. (Cybertipline Report, R. 33-2, Page ID # 172). As quoted above, the United States argued that these coordinates were "the defendant's house." This is simply not true, and unbelievably prejudicial. Miller requests this Court take judicial notice of Exhibit A, which is a map of the analyst's geolocated longitude and latitude and the defendant's residential address (the address is part of the record). (Fed. R. Evid. 201, Advisory Comm. Notes (f) provides "judicial notice may be taken at any stage of the proceedings, whether in the trial court or on appeal.").

Second, the misleading part. Miller had no recourse when the United States made its argument in rebuttal, particularly because he had no opportunity to confront the NCMEC analyst during trial. The process of geolocating an IP address is not difficult. There are many publicly available tools for doing so on the internet. Once the IP address is placed in the geolocating tool, it responds with multiple options for the longitude and latitude of the IP address. The analyst then chooses which longitude and latitude to put in the Cybertipline Report. In this case, the analyst presumably (counsel must presume because no cross was available) chose a certain latitude and longitude for both the Creation IP and the July Email IP. While there were likely many options, the analyst chose the two that matched.

Miller was never able to cross the analyst on the fact that he or she could have picked a different latitude and longitude from the separate lists, making it look like the IP addresses came from two different locations (which would fit the defense's theory). The analyst's choice aligned with the prosecution's theory (confirmation bias at its best) and Miller did not have the opportunity to cross the biased choice. In fact, counsel proffered during the trial that he had geolocated the Creation IP and it came back with a list of potential longitudes and latitudes. Counsel was able to find one near the nursing home where Fred Miller lived. (Jury Trial Day 3, R. 97, Page ID #901-02). This would have been fodder for cross-examination of the analyst.

In total, Miller's right to confrontation was violated when the Cybertipline Report was admitted over his multiple objections. Due to the prejudice suffered from the report's admission, Miller's convictions should be reversed, and his case remanded for a new trial.

## III. The District Court Erred when Denying Miller's Rule 29 Motion as there was Insufficient Evidence for All Counts.

The appellate court reviews *de novo* the district court's judgment denying a motion for acquittal, viewing "the evidence in the light most favorable to the prosecution" and affirming only if "any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *United States v. Lowe*, 795 F.3d 519, 522 (6th Cir. 2015) (quoting *United States v. Washington*, 715 F.3d 975, 979 (6th Cir. 2013)).

In general, evidence is insufficient to support a finding beyond a reasonable doubt when the State fails to establish that the defendant had exclusive possession of the device receiving child pornography. *See Lowe*, 795 F.3d at 523. In *Lowe*, a user downloaded child pornography to a computer found in a common area of the home that the defendant shared with his wife and a minor relative. *Id.* at 520. The proof at trial showed that the computer was not password protected and automatically connected to the internet. *Id.* at 521. The peer-to-peer file sharing system used to download child pornography to the computer was also not password protected, and it started running whenever the computer was turned on. *Id.* The Sixth

Circuit determined that the limited evidence of defendant's ownership and use of the laptop was insufficient to find the defendant guilty beyond a reasonable doubt when two other people had open access to both the laptop and the file-sharing program. *Id.* at 523. Accordingly, the Sixth Circuit held that no reasonably juror could infer that defendant downloaded, possessed, and distributed the child pornography found on the computer "without improperly stacking inferences." *Id.*

Although not binding on this Court, the Sixth Circuit relied on *United States v. Moreland*, 665 F.3d 137 (5th Cir. 2011), in deciding *Lowe*. In *Moreland*, the defendant, his wife, and his father all had access to a computer found to contain child pornography. *Id.* at 143. The evidence presented at trial showed that the father frequently used the computers late at night and had an interest in pornography. *Id.* at 147. Based on this evidence, the Fifth Circuit held that the government had not introduced sufficient evidence to prove that the defendant, rather than the father, had downloaded and viewed the child pornography. *Id.* at 150-52.

Much like the shared computers in *Lowe* and *Moreland*, the evidence presented in this case establishes that someone other than Miller, namely Fred Miller, had shared access to the miller694u@gmail.com email account and the external hard drive in question. For instance, the miller694u@gmail.com email inbox contained multiple automated Google alerts stating there were new sign-ins from various possible locations (*i.e.* Lousiville, KY) and internet service providers.

(Jury Trial Day 2 Tr., R. 96, Page ID # 609, 668). In total, four new sign-in alerts occurred on different dates, including on a date of distribution/receipt. (Id. at Page ID # 669-70).

Furthermore, there were several emails sent to and from miller694u@gmail.com regarding the purchase of an LG cell phone and tablet. (*Id.* at Page ID #674-79). The incoming emails were addressed to "Fred". (*Id.*). The receipts attached to the "Dear Fred" emails were billed to Fred Miller and the remaining balance for the phone and tablet was paid with a credit card *in the name of Fred Miller*. (*Id.* at Page ID # 678-79). Neither an LG cell phone nor an LG tablet were found during the search of Miller's house. (*Id.* at Page ID # 698, 716).

Further, several witnesses testified that Fred Miller frequently visited Miller's house. (*Id.* at Page ID # 813, 820, 825). These same witnesses testified that Fred had access to and used the various computers and electronic equipment at Miller's house. (*Id.*). Finally, the hard drive containing child pornography was found in a common area of Miller's home, specifically the living room. (*Id.* at Page ID # 696).

Based on the foregoing, the State failed to prove that Miller had exclusive possession of the miller694u@gmail.com email account or the external hard drive. Accordingly, the evidence presented at trial was insufficient to support a finding beyond a reasonable doubt that Miller, rather than Fred, received, distributed, and possessed child pornography.

## CONCLUSION

For the reasons stated above, Miller requests this Court reverse his conviction for all counts.

Respectfully submitted,

/s/ Eric G. Eckes
ERIC G. ECKES (Ky. Bar No. 93604)
(CJA Appointed)
Pinales, Stachler, Young, Burrell & Crouse Co., LPA
455 Delta Ave., Suite 105
Cincinnati, Ohio 45226
(513) 252-2723
(513) 252-2751
eeckes@pinalesstachler.com

**CERTIFICATE OF SERVICE**

I hereby certify that a copy of the foregoing has been served via this Court's ECF system to:

Charles P. Wisdom Jr.
U.S. Attorney's Office
260 W. Vine Street
Suite 300
Lexington, KY 40507

on this 10th day of October, 2018.

/s/ Eric G. Eckes
ERIC G. ECKES (Ky. Bar No. 93604)
Counsel for Defendant-Appellant

## DESIGNATION OF RELEVANT DISTRICT COURT DOCUMENTS

| Docket Number | Document Description | Page ID # |
|---|---|---|
| 1 | Indictment | 1-3 |
| 20 | Superseding Indictment | 88-91 |
| 27 | Motion to Suppress | 109-120 |
| 33 | United States' Response to Motion to Suppress with Exhibits | 138-197 |
| 41 | Report and Recommendation | 217-243 |
| 48 | Memorandum Order Re: Motion to Suppress | 259-277 |
| 62 | Second Superseding Indictment | 327-331 |
| 69 | Minute Entry | 357-358 |
| 88 | Judgment | 444-450 |
| 90 | Notice of Appeal | 452-453 |
| 95 | Trial Transcript Day 1 of Trial | 495-623 |
| 96 | Trial Transcript Day 2 of Trial | 624-843 |
| 97 | Trial Transcript Day 3 of Trial | 844-909 |
| 99 | Transcript Volume 1 of Motion Hearing | 964-989 |
| 100 | Transcript Volume 2 of Motion Hearing | 990-1039 |

## CERTIFICATE OF COMPLIANCE

This brief has been prepared using 14-point proportionally spaced font.

Exclusive of the corporate disclosure statement, table of contents, table of authorities, statement with respect to oral argument, the certificate of service, designation of relevant documents, and certificate of compliance, the brief contains 7,276 words.

I understand that material representations can result in the Court's striking of the brief and imposing sanctions. If the Court so directs, I will provide an electronic version of the brief and/or copy of the word or line printout.

/s/ Eric G. Eckes