CASE NO. 18-5578

UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

UNITED STATES OF AMERICA — PLAINTIFF-APPELLEE

V.

WILLIAM J. MILLER — DEFENDANT-APPELLANT

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF KENTUCKY

BRIEF OF THE PLAINTIFF-APPELLEE UNITED STATES OF AMERICA

ROBERT M. DUNCAN, JR.
UNITED STATES ATTORNEY

CHARLES P. WISDOM JR.
CHIEF, APPELLATE DIVISION

BY: ELAINE K. LEONHARD
ASSISTANT UNITED STATES ATTORNEY
207 GRANDVIEW DR., SUITE 400
FT. MITCHELL, KENTUCKY 41017
(859) 652-7035
Elaine.K.Leonhard@usdoj.gov

COUNSEL FOR PLAINTIFF-APPELLEE

TABLE OF CONTENTS

TABLE OF AUTHORITIES

I. Cases

II. Statutes & Rules

STATEMENT REGARDING ORAL ARGUMENT

The United States does not request oral argument.

STATEMENT OF THE ISSUES

I. Did the district court err in denying Miller's motion to suppress?

II. Did the district court err in admitting the NCMEC CyberTipline report?

III. Was the evidence sufficient to support Miller's convictions?

STATEMENT OF THE CASE

On July 9, 2015, an individual using Google email (gmail) account miller694u@gmail.com uploaded two images of child pornography to an email. [R. 33: Response at 169-70.] Google became aware of the images because "since 2008, Google has been using its own proprietary hashing technology to tag confirmed child sexual abuse images." [*Id*. at 161 (¶ 4).] Google's scanning process is described as follows:

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

[*Id*.]

When the software identified the two images of child pornography, it triggered both an "Automatic Report" to the National Center for Missing and Exploited Children (NCMEC) CyberTipline, which is required by law, as well as an automatic disabling of the gmail account. [*Id*. at 161-62 (¶¶ 7-8, 10), 169.] The Automatic Report sent by Google to NCMEC contained the following information: (1) the incident type (child pornography) and time; (2) the email address used; (3) the IP address for the computer used; and (4) the number of files uploaded, the file names, and a categorization that indicated that the images depicted a prepubescent minor engaging in a "sex act" or sexually explicit conduct. [*Id*. at 169-72.] Google did not review the contents of the email to which the images were attached, and advised NCMEC that "[t]he reported user uploaded the attached media to an email in Gmail, which may or may not have been sent." [*Id*. at 170; *see also id*. at 162 (¶ 10).]

The classification of the report as "Automatic" meant that the images were scanned by Google's proprietary hashing technology (rather than reviewed by a Google employee concurrently with submitting the report) and found to contain hash values that matched files that had previously been identified by a Google employee as depicting child pornography. [*Id*. at 161-62.] Google utilizes this technology because it "has a strong business interest in . . . ensuring [its] products

are free of illegal content, and in particular, child sexual abuse material." [*Id*. at 161 (¶ 3).] In a similar vein, Google "rel[ies] on users who flag suspicious content they encounter so [Google] can review it and help expand [its] database of illegal images." [*Id*. (¶ 5).] Importantly, "[n]o hash is added to [Google's] repository without the corresponding image first having been visually confirmed by a Google employee to be apparent child pornography." [*Id*.]

Once NCMEC received the report by Google, it undertook a series of steps, some of which were automated and others that were done by an analyst. [R. 105: Lindsey Olson, TR (Trial Day 1) at 1091-92.] For example, NCMEC's systems automatically geographically resolved the IP addresses provided by Google via a publicly-available online search. [*Id*. at 1092-93; R. 33: Response at 196 (¶ 16).] That search revealed that the IP addresses were associated with a Time Warner Cable account with a potential geographic location of Ft. Mitchell, Kentucky. [R. 105: Lindsey Olson, TR (Trial Day 1) at 1093; R. 33: Response at 196 (¶ 16).] A NCMEC analyst then searched the email address that was used to upload the images using Google, Facebook, MeetMe, and other publicly-available websites. [R. 105: Lindsey Olson, TR (Trial Day 1) at 1095-97; R. 33: Response at 196 (¶ 15).] Importantly, NMCEC did not review the two images provided by Google; in fact, the CyberTipline report expressly stated, "[p]lease be advised that NCMEC

has not opened or viewed any uploaded files submitted with this report and has no information concerning the content of the uploaded files other than information provided in the report by the ESP." [R. 105: Lindsey Olson, TR (Trial Day 1) at 1095; R. 33: Response at 174, 196 (¶ 15).] Rather, NCMEC simply forwarded the images—as part of the CyberTipline report—to the Kentucky Internet Crimes Against Children (ICAC) task force, which is headed by the Kentucky State Police (KSP). [R. 105: Lindsey Olson, TR (Trial Day 1) at 1097.] The CyberTipline report was made available to KSP via a virtual private network (VPN). [*Id*.] KSP then sent the report to the Kenton County Police Department, where it was ultimately reviewed by Detective Aaron Schihl. [R. 105: Aaron Schihl, TR (Trial Day 1) at 1107-08.]

On August 13, 2015, Detective Schihl reviewed the CyberTipline report, including the images that Google provided to NCMEC. [*Id*. at 1107.] Schihl then obtained—via subpoena—subscriber information from Time Warner Cable for the subject account. [*Id*. at 1114.] That information identified William Miller's wife, Tania, as the subscriber, along with an address on Mercury Street in Ft. Mitchell, Kentucky. [*Id*. at 1114-16.]

On October 22, 2015, Schihl obtained a search warrant for the contents of miller694u@gmail.com account; the affidavit in support included the information

contained in the CyberTipline report, the information provided by Time Warner Cable, and a description of what the images depicted, which Schihl indicated was based upon his review of the images themselves. [*Id*. at 1117; R. 33: Response at 178-80.] The results produced by Google included subscriber information identifying William Miller as the account holder, and thousands of emails, including evidence of receipt and distribution of child pornography. [R. 105: Aaron Schihl, TR (Trial Day 1) at 1117-23.]

Detective Schihl then obtained a search warrant for Miller's home, which was searched on October 29, 2015. [*Id*. at 1123; R. 33: Response at 181-86.] Officers located several items of digital evidence, including an Acer laptop and a Toshiba external hard drive. [R. 105: Aaron Schihl, TR (Trial Day 1) at 1127.] When he was interviewed, Miller admitted that he primarily used the laptop and child pornography had "popped up" on it, along with what appeared to be a demand for ransom from the FBI. [*Id*. at 1128-33.] Miller also admitted that he purchased the hard drive one year prior at a yard sale and that it contained child pornography, though he claimed it was already on the hard drive when he purchased it. [*Id*. at 1133-34, R. 106: Aaron Schihl, TR (Trial Day 2) at 1197-99.] These items were forensically examined and found to contain child pornography, as well as evidence linking Miller to the items and the items to crimes. [R. 105:

Aaron Schihl, TR (Trial Day 1) at 1128; R. 106: Michael Johnson, TR (Trial Day 2) at 1300-29.]

William Miller was charged with distribution, receipt, and possession of child pornography. [R. 1: Indictment at 1; R. 20: Superseding Indictment at 88; R. 62: Second Superseding Indictment at 327.] He moved to suppress the evidence that Google sent to NCMEC and that Detective Schihl reviewed, as well as the evidence that was found on the devices seized from his residence. [R. 27: Motion at 109.] According to Miller, Google was a "government actor" that conducted a warrantless search of his email; alternatively, he argued that even if Google conducted a private search, Schihl "exceeded the initial search by Google, and therefore violated [his] Fourth Amendment rights." [*Id*.at 111-18.] Finally, Miller contended that the traditional trespass theory of searches applied. [*Id*.]

The district court denied Miller's motion. [R. 48: Opinion and Order at 259.] The court rejected Miller's claim that Google is a government actor and further concluded that Schihl's actions did not exceed the scope of Google's private search. [*Id*. at 263-75.] Finally, the court found that no "physical trespass" occurred. [*Id*. at 276.]

Miller proceeded to trial. [R. 69: Minute Entry at 357; R. 70: Minute Entry at 359; R. 72: Minute Entry at 396.] The government's first witness was Lindsey

Olson, NCMEC's Executive Director of the Exploited Children Division. [R. 105: Lindsey Olson, TR (Trial Day 1) at 1075.] After explaining the origins of NCMEC's founding, its mission, and its various programs, the government sought to admit the CyberTipline report that NCMEC generated in this case. Olson authenticated the report and explained that CyberTipline reports are made and kept in the ordinary course of NCMEC's business by someone who had knowledge of the events described therein. [*Id*. at 1080-81.] Miller objected on the ground that the report was hearsay: "this report to be is akin to a police report, and police reports are not admissible in their entirety to a jury." [R. 105: Eric G. Eckes, TR (Trial Day 1) at 1082.] The district court disagreed. [R. 105: Court, TR (Trial Day 1) at 1082.] Counsel persisted:

> That's the first objection is that it's akin to a police report. The second would be that within this is hearsay. So let's say it's a business record. Any business record that comes in still is subject to objections of hearsay within hearsay. If this witness has no personal knowledge of an investigation that got conducted that said, you know, we got on the—I mean, here's what it is, Judge. We got on the internet, we searched for all this stuff, we found all this stuff. We found the profile, we screen-shotted the profile, we then put that into our report. That's similar to like a police officer getting up there and not having to testify to what prior officers did.

[*Id*. at 1083.] The district court overruled the objection and the report was admitted. [R. 105: Court, TR (Trial Day 1) at 1085.]

Following Ms. Olson's testimony, counsel continued, "the crux of my objection, Judge, is NCMEC is a *de facto* or has found to be an investigative agency." [R. 105: Eric G. Eckes, TR (Trial Day 1) at 1100.] The court took a brief recess and when it resumed, counsel continued:

> Just on the prior objection, I just want to raise the case law of *Crawford* in addition to it, because it's—I've articulated this, but I didn't use the word *Crawford*, that you have an analyst reporting to the executive director, who then testified, and I was not able to cross-examine the analyst.

[*Id*. at 1101.] The district court maintained its prior ruling.

The balance of the government's proof established that a subscriber named "William Miller" set up a gmail account (miller694u@gmail.com) on January 29, 2015. [R. 105: Aaron Schihl, TR (Trial Day 1) at 1119-21.] The emails, themselves, revealed that Miller was in, fact, the user. [*Id*. at 1138-41; R. 106: Aaron Schihl, TR (Trial Day 2) at 1193-95.] Miller used his real name and even sent photographs of himself when communicating with others. [R. 105: Aaron Schihl, TR (Trial Day 1) at 1138-41; R. 106: Aaron Schihl, TR (Trial Day 2) at 1193-95; R. 106: Michael Johnson, TR (Trial Day 2) at 1302.] He also told a common story to the people he was communicating with; a story that had elements of truth to it. [R. 105: Aaron Schihl, TR (Trial Day 1) at 1140-41; R. 106: Aaron Schihl, TR (Trial Day 2) at 1194-95.] For example, Miller told people

that his wife's name was Tania, he had four adult children, and he owned a trucking company. [R. 105: Aaron Schihl, TR (Trial Day 1) at 1140-41; R. 106: Aaron Schihl, TR (Trial Day 2) at 1194-95.] Child pornography was transmitted—sent and received—via the gmail account. [R. 105: Aaron Schihl, TR (Trial Day 1) at 1139-65; R. 106: Aaron Schihl, TR (Trial Day 2) at 1181-91.]

Forensic examination of Miller's laptop revealed a user account named "Bill," evidence of the IP address that was used to send the July 9, 2015 email, link files that indicated that the Toshiba hard drive had been connected to the laptop, and Skype messages from a user with the display name "Bill Miller." [R. 106: Michael Johnson, TR (Trial Day 2) at 1301-10.] Forensic examination of Miller's hard drive also revealed Skype messages requesting, among other things, "naked pics" of girls or young boys and offering to pay for sex online, and 571 files depicting child pornography. [*Id*. at 1310-12, 1326-28.] The videos and images of child pornography were found in user-created folders labeled "Ass," "Dick," "Fingers," "Gay," "Young gay," "Incest," "Piss," "Pre-teens," "Boys," "Sucking," "Teens," and "Preteens." All but one of the files—and the folders they were found in—were created on the same date, July 2, 2015, and just days before the CyberTipline report was generated. [*Id*. at 1316-17.] The same images that were transmitted via the miller694u@gmail.com account were found on the hard drive,

as was a folder labeled "Me" that contained photographs of Miller. [*Id*. at 1326.] Miller attempted to point the finger at his brother, Fred, but the jury was not persuaded. [R. 105: Eric Eckes, TR (Trial Day 1) at 1072-74; R. 97: Eric Eckes, TR (Trial Day 3) at 872.]

During the government's closing argument, it reminded the jury of all the above. [R. 97: Elaine K. Leonhard, TR (Trial Day 3) at 854-71.] On the issue of the IP addresses that Google provided to NCMEC, the government argued:

> The IP address of the initial login, the created date of the Gmail account, and the IP address that was captured in the email on July 9th of 2015 that contained those two images of the—disabled his account, they both resolved back to Time Warner Cable at the exact same latitude and longitude. The defendant's house.

[*Id*. at 891.] Miller objected, citing facts not in evidence, but was overruled. [R. 97: Colloquy, TR (Trial Day 3) at 891.] After the case was submitted to the jury, defense counsel supplemented his objection, which he conceded was really an attempt to "complete the record on [the] prior objection to this [CyberTipline] report coming in and to the analyst that theoretically created this latitude and longitude . . . ." [R. 97: Eric G. Eckes, TR (Trial Day 3) at 899.] When pressed, counsel acknowledged that he did not cross-examine Ms. Olson about the process of geographically resolving an IP address generally or the reliability or precision of that process in this case specifically. [R. 97: Colloquy, TR (Trial Day 3) at 901-

02.] The jury convicted Miller on all counts. [R. 75: Verdict at 401-02.] He was sentenced to 150 months in prison and fifteen years of supervised release. [R. 88: Judgment at 445-46.] This appeal followed. [R. 90: Notice of Appeal at 452.]

SUMMARY OF THE ARGUMENT

I. The district court properly denied Miller's motion to suppress. Miller's reasonable expectation of privacy in the files attached to the July 9, 2015, email was frustrated by Google's proprietary software by the time Detective Schihl viewed them. Detective Schihl stayed within the scope of that private search and did not physically intrude on any protected space of Miller's, therefore, no Fourth Amendment violation occurred.

Google uses proprietary software to review content on its platform for its own business interests. Google did so in this case without any participation by—or intent to assist—the government. Google did not forfeit its private status by reporting illegal content to NCMEC.

II. The district court did not err in admitting the NCMEC CyberTipline report. The report qualifies as a "business record" that was properly authenticated and does not constitute testimonial hearsay. In fact, the portion of the report that Miller takes issue with is not hearsay at all; rather, it contains automated results

produced by NCMEC's systems. Miller's right of confrontation, therefore, was not violated by its admission.

Miller's complaint that he was denied the opportunity to cross-examine the analyst who prepared the report rings hollow because the analyst did not geographically resolve the IP address as Miller alleges. Rather, that portion of the report was generated automatically by NCMEC's systems. More importantly, Miller could have cross-examined the NCMEC witness about that process and the reliability and precision the results, but deliberately chose not to.

Even if the district court erred in admitting the CyberTipline report, it was harmless. All of the emails from the miller694u@gmail.com account—including the email that generated the tip from Google to NCMEC and the attachments, which depicted child pornography—were admitted without objection. So, too, were all of the IP addresses logged by Google. Finally, Miller was convicted of four other counts of distribution of child pornography and the admission of the CyberTipline report was not relevant to any of those counts.

III. The evidence was sufficient to sustain Miller's convictions. The proof established that a gmail account set up by "William Miller" was used to send and receive child pornography. The content of the emails revealed that Miller was,

in fact, the user. Miller used his name, told the same story, and sent photographs of himself when he communicated with others using the email address.

Additionally, the same images of child pornography that were sent from, and received by, the gmail account were found on an external hard drive that was seized from Miller's residence. Miller admitted that he purchased the hard drive, that it belonged to him, and that he knew it contained child pornography. Finally, the child pornography was located in user-created folders and organized by content. The files and the folders were created on the same date, July 2, 2015, which directly refuted Miller's story that the child pornography was on the hard drive when he bought it at a yard sale one year prior. Finally, the hard drive contained a folder labeled "Me" that contained photographs of Miller.

ARGUMENT

I. The district court did not err in denying Miller's motion to suppress.

One of the fundamental principles of the Fourth Amendment is that it protects "an expectation of privacy that society is prepared to consider reasonable." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). "When a government agent infringes on this reasonable expectation, a 'search' occurs for the purposes of the Fourth Amendment, and the government must obtain a warrant or demonstrate that an exception to the warrant requirement applies." *United States v. Lichtenberger*,

786 F.3d 478, 482 (6th Cir. 2015). But the Fourth Amendment only protects against "governmental action; it is wholly inapplicable 'to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.'" *Jacobsen*, 466 U.S. at 113-14. This Circuit uses a "two-factor analysis" in determining "whether a private party is acting as an agent of the government" such that the Fourth Amendment applies: "(1) the government's knowledge or acquiescence" to the search, and "(2) the intent of the party performing the search." *United States v. Hardin*, 539 F.3d 404, 418 (6th Cir. 2008). If "the intent of the private party conducting the search is entirely independent of the government's intent to collect evidence for use in a criminal prosecution," then "the private party is not an agent of the government." *Id*.

When a private party conducts a search that frustrates an individual's reasonable expectation of privacy and delivers information to the government, the Fourth Amendment is "implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated." *Jacobsen*, 466 U.S. at 117. To determine whether "additional invasions" of privacy by a government actor are subject to Fourth Amendment scrutiny, they must be "tested by the degree to which they exceeded the scope of the private

search." *Id*. at 115 (citing *Walter v. United States*, 447 U.S. 649 (1980)). As this Court has explained, a government search will be deemed to stay within the scope of the private search when "the officers in question had near-certainty regarding what they would find and little chance to see much other than contraband." *Lichtenberger*, 786 F.3d at 486.

In this case, Google reviewed content that was transmitted via its platform and did so as a private entity. Miller's argument to the contrary, *see* Miller's Brief at 17-21, has been repeatedly rejected. *See United States v. Stevenson*, 727 F.3d 826, 831 (8th Cir. 2013) (noting that "AOL's decision on its own initiative to ferret out child pornography does not convert the company into an agent or instrument of the government for Fourth Amendment purposes . . . . AOL's voluntary efforts to achieve a goal that it shares with law enforcement do not, by themselves, transform the company into a government agent."); *United States v. Cameron*, 699 F.3d 621, 637-38 (1st Cir. 2012) (holding Yahoo!, Inc., did not act as agent in searching e-mails and sending reports to NCMEC); *United States v. Richardson*, 607 F.3d 357, 366 (4th Cir. 2010) (holding that AOL's scanning of email communications for child pornography did not trigger Fourth Amendment's warrant requirement because no law enforcement officer or agency asked provider to search or scan defendant's emails); *United States v. Stratton*, No. 15-40084-010-DDC, 2017 WL

169041, at *4-6 (D. Kan. Jan. 17, 2017) (holding that Sony was not government agent when it searched images stored on defendant's PS3); *United States v. DiTomasso*, 81 F. Supp. 3d 304, 309-11 (S.D.N.Y. 2015) (chat service provider Omegle held not to be Government agent and its search of defendant's chat messages held to be pure private search beyond the reach of the Fourth Amendment); *United States v. Miller*, No. 8:15CR172, 2015 WL 5824024, at *4 (D. Neb. Oct. 6, 2015) (holding that Google is "private, for profit entity" that "complied with its statutory duty to report violations of child pornography laws" and did not become a state actor by doing so); *United States v. Ackerman*, No. 13-10176-01-EFM, 2014 WL 2968164, at *5-6 (D. Kan. July 1, 2014) (holding that AOL is not state actor), *rev'd on other grounds*, 831 F.3d 1292 (10th Cir. 2016); *United States v. Drivdahl*, No. CR-13-18-H-DLC, 2014 WL 896734, at *3-4 (D. Mont. Mar. 6, 2014) (holding that Google is not government agent); *United States v. Keith*, 980 F. Supp. 2d 33, 40-42 (D. Mass. 2013) (holding that AOL is not government agent). More importantly, though, Miller has made no showing that Google's conduct was anything other than independent (of law enforcement), voluntary, and motivated by its own business interests.

The district court joined the chorus noted above in rejecting Miller's argument that Google is a government actor. [R. 48: Opinion and Order at 263-

67.] The court found that Google has a strong and legitimate business interest in monitoring and safeguarding its platform; an interest that exists independently of any legal obligation to report child pornography and is devoid of any intent to assist law enforcement. [*Id*.] The district court also concluded that Detective Schihl did not exceed the scope of Google's private search. According to the court, "the digital fingerprints produced by hashing provide 'virtual certainty'" that the images viewed by Schihl would be the same as those seen and determined to be child pornography by Google. The court found it equally important that the CyberTip "did not include any email body text or header information associated with the reported content" or any images that Google had not previously viewed and, therefore, Detective Schihl had "little chance to see much other than contraband." [*Id*. at 274.] Finding that the "private search doctrine" controlled, the district court declined to find that a trespass occurred. [*Id*. at 276.]

When reviewing a district court's denial of a motion to suppress evidence, this Court reviews the factual findings for clear error and the legal conclusions as to the existence of probable cause *de novo*. *United States v. Hill*, 195 F.3d 258, 264 (6th Cir. 1999). "It is well settled that in seeking suppression of evidence the burden of proof is upon the defendant to display a violation of some constitutional or statutory right justifying suppression." *United States v. Feldman*, 606 F.2d 673,

679 n.11 (6th Cir. 1979). "When reviewing the denial of a motion to suppress evidence, [this Court] must consider the evidence in the light most favorable to the government." *United States v. Garza*, 10 F.3d 1241, 1245 (6th Cir. 1993).

The district court properly concluded that Detective Schihl's search was insulated by the private search doctrine. Since then, the Fifth Circuit reached the same conclusion, for precisely the same reason, in *United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018). In that case, the defendant uploaded digital image files to Microsoft SkyDrive, a cloud-hosting service that uses PhotoDNA to automatically scan the hash values of user-uploaded files and compare them against the hash values of known images of child pornography. *Id*. at 637-38. "When PhotoDNA detects a match between the hash value of a user-uploaded file and a known child pornography hash value, it creates a 'CyberTip' and sends the file—along with the uploader's IP address information—to . . . NCMEC." *Id*. at 638.

In early 2015, Microsoft sent CyberTips to NCMEC based on the hash values of files that the defendant had uploaded to SkyDrive; NCMEC then forwarded the CyberTips to the Corpus Christi Police Department. *Id.* Upon receiving the CyberTips, a detective opened each of the suspect files and confirmed that each contained child pornography. *Id*. The detective then obtained

a search warrant for the defendant's home. *Id*. The search uncovered additional evidence of child pornography. *Id.*

The defendant was indicted for possession of child pornography in violation of 18 U.S.C. § 2252(a)(2) and (b)(1). *Id*. He filed a motion to suppress arguing, in part, that the detective's warrantless opening of the files associated with the CyberTips was an unlawful search. *Id*. The district court disagreed; so did the Fifth Circuit:

> [t]he private search doctrine decides this case. A private company determined that the hash values of files uploaded by [the defendant] corresponded to the hash values of known child pornography images. The company then passed this information on to law enforcement. This qualifies as a "private search" for Fourth Amendment purposes. And the government's subsequent law enforcement actions in reviewing the images did not effect an intrusion on [the defendant's] privacy that he did not already experience as a result of the private search. Accordingly, we affirm the judgment of the district court.

Id. at 637.

Much like the district court, the court in *Reddick* relied primarily on the Supreme Court's decision in on *United States v. Jacobsen*, 466 U.S. 109 (1984). In that case, employees of Federal Express observed a package that had been damaged in transit, opened it, and discovered a white powder. *Id.* at 111. The employees contacted the Drug Enforcement Administration, whose agents conducted chemical field tests on the white powder and determined that the

powder was cocaine. *Id.* The Court concluded that any expectation of privacy the recipients might have had in the package's contents was abrogated when the Federal Express employees opened and searched the package and discovered the white powder. *Id*. at 118-21. The government's subsequent use of that information—its test to discern the powder's chemical composition—infringed no expectation of privacy that had not already been infringed. *Id*. at 121-26.

The court in *Reddick* analogized: when the defendant's '"package' (that is, his set of computer files) was inspected and deemed suspicious by a private actor," "whatever expectation of privacy [the defendant] might have had in the hash values of his files was frustrated . . . ." *Reddick*, 900 F.3d at 639. And when the detective opened the files, there was no "significant expansion of the search that had been conducted previously by a private party sufficient to constitute a separate search." *Id.* (citing *Walter*, 447 U.S. at 657). The court concluded by noting an important distinction, "[s]ignificantly, there is no allegation that [the detective] conducted a search of any of [the defendant's] files other than those flagged as child pornography." *Id.*; *compare with Ackerman*, 831 F.3d at 1294, 1306 (reversing denial of motion to suppress where NCMEC opened the email and not just the attachment that was hash match for known child pornography, but three others as well).

That same distinction exists in this case. Google's proprietary software scanned and identified two files attached to an email sent from an account subscribed to by "William Miller" as child pornography. Prior to that, a Google employee visually reviewed the files and determined that they were child pornography, and the hash values were added to Google's library. Google's automated scanning process then triggered an automatic report to NCMEC, which did not review the attachments or the contents of the email. Detective Schihl then opened the attachments, reviewed the images, and confirmed what Google had already concluded—that the images depicted child pornography. Schihl's "search" did not expand what Google had already done; and, because of what Google had already done, Schihl was near-certain of what he would find: child pornography.

Contrary to Miller's argument, there was no "warrantless opening of Miller's private email correspondence," *see* Miller's Brief at 10. Rather, Schihl's review was limited to two files that had the same hash values as files that had been viewed by a Google employee and determined to depict child pornography—files that were sent by Google, to NCMEC, and then to him. As a result, Miller's attempt to characterize Schihl's conduct as a "physical intrusion," *see* Miller's Brief at 10-12, fails.

Unlike in *Jones*, the government never physically occupied private property for the purpose of obtaining information. *United States v. Jones*, 565 U.S. 400, 404-05 (2012). Schihl, himself, did not enter into any space; rather he was simply the recipient of information, which then visually observed. *Id*. at 412 (noting that the Court "has to date not deviated from the understanding that mere visual observation does not constitute a search."). And if the files themselves are considered "space," it was already charted by the time Schihl entered. Under these circumstances, Miller's Fourth Amendment rights, therefore, were not violated.

II. The district court did not err in admitting the NCMEC Cyber Tipline report.

Miller claims his convictions must be reversed because the district court erred by admitting the CyberTipline report (Government Exhibit 7) into evidence in violation of his rights under the Confrontation Clause. *See* Miller's Brief at 21-28. But the Confrontation Clause is only implicated when evidence constitutes testimonial hearsay. The CyberTipline report, itself, is a non-testimonial business record and the portion of the report that Miller objects to is not hearsay. Thus, the Confrontation Clause was not violated.

A document may be admitted as a "business record" under Rule 803(6) if it satisfies four requirements: 1) it was "created in the course of a regularly

conducted business activity," 2) it was "kept in the regular course of that business," 3) it resulted from a "regular practice of the business" to create such documents, and 4) it was "created by a person with knowledge of the transaction or from information transmitted by a person with knowledge." *United States v. Collins*, 799 F.3d 554, 582-83 (6th Cir. 2015) (citing *Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC*, 774 F.3d 1065, 1071-72 (6th Cir. 2014); Fed. R. Evid. 803(6)). Until 2004, "business records" were routinely admitted over Confrontation Clause challenges because Rule 803(6) was deemed a "firmly-rooted" hearsay exception that sufficiently ensured the exhibit's reliability. *See generally Ohio v. Roberts*, 448 U.S. 56, 66 (1980) (holding that a hearsay statement of an unavailable witness is admissible under the Confrontation Clause if it "bears adequate indicia of reliability," and that the requisite reliability "can be inferred without more in a case where the evidence falls within a firmly rooted hearsay exception."). In *Crawford v. Washington*, 541 U.S. 36, 68 (2004), however, the Supreme Court overruled the "reliability standard" and instead held that the admissibility of an out-of-court statement under the Confrontation Clause turns upon whether the statement is "testimonial." The Court emphasized that "[w]here testimonial statements are at issue, the only indicium of reliability sufficient to satisfy constitutional demands is the one the Constitution actually

prescribes: confrontation." *Id*. at 68-69. Although the Court declined to "spell out a comprehensive definition of 'testimonial,'" the Court noted as an aside that business records "by their nature" ordinarily would not be so characterized. *Id*. at 56, 68.

In subsequent decisions, the contours—imprecise as they are—of what constitutes "testimonial hearsay" have taken shape. In *Melendez-Diaz*, for example, the Court held that the admission of affidavits from forensic analysts who had performed drug analysis on evidence seized from a suspect but did not themselves testify violated the Confrontation Clause. *Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 329 (2009). The Court explained:

> Business and public records are generally admissible absent confrontation not because they qualify under an exception to the hearsay rules, but because—having been created for the administration of an entity's affairs and not for the purpose of establishing or proving some fact at trial—they are not testimonial. Whether or not they qualify as business or official records, the analysts' statements here—prepared specifically for use at petitioner's trial—were testimony against petitioner, and the analysts were subject to confrontation under the Sixth Amendment.

Id. at 324. Similarly, in *Bullcoming v. New Mexico*, 564 U.S. 647, 651, 657 (2011), the Supreme Court held that blood-alcohol analysis was testimonial and, therefore, triggered the right of confrontation, which was violated when an analyst who did not perform the test testified. Finally, in *United States v. Maga*, 475 F.

App'x 538 (6th Cir. 2012), this Court considered whether forms prepared by an IRS employee and showing that the defendant had not filed federal income tax returns were "testimonial" statements that triggered the right to confrontation. *Id*. at 541. The Court concluded they were, relying in large part on the fact that the forms were generated "under circumstances where one could reasonably believe that the government would use them at trial," and were not "exact copies of the data the IRS ordinarily maintains in its master files." *Id*. at 542. Additionally, the Court relied on the Supreme Court's recognition that evidence becomes testimonial in nature when it goes beyond a mere restatement of "raw, machine-produced data" and includes "representations not revealed in the raw data." *Id*. (citing *Bullcoming*, 564 U.S. at 660).

Miller objected to the admission of the NCMEC report below on several grounds, but did not raise a Confrontation Clause challenge until after the evidence was admitted and the witness was excused. This Court generally reviews the district court's evidentiary rulings for abuse of discretion. *United States v. Warman*, 578 F.3d 320, 345 (6th Cir. 2009). But in this case, Miller failed to raise the specific issue he raises now until after the evidence was admitted. Thus, it is arguable that this Court's review is limited to plain error. *See Collins*, 799 F.3d at 584-85 (holding that plain error review applied where the defendants raised

a "lengthy" objection at trial but did not raise any concerns regarding the violation of their constitutional right to confront the witnesses against them). "Plain error review applies even if the forfeited assignment of error is a constitutional error." *United States v. Cromer*, 389 F.3d 662, 672 (6th Cir. 2004); *see also United States v. Hadley*, 431 F.3d 484, 498 (6th Cir. 2005) (reviewing a Confrontation Clause claim for plain error because "Defendant raised only a hearsay objection to [the contested] statements at trial, and did not challenge their admissibility on constitutional grounds"). Regardless of which standard of review applies, the result is the same: no error occurred and, even if it did, it was harmless in light of the other evidence that was admitted.

The NCMEC CyberTipline report qualifies as a "business record" under Federal Rule of Evidence 803(6). The report is not testimonial because it was "created for the administration of [NCMEC's] affairs and not for the purpose of establishing or proving some fact at trial." *Melendez-Diaz*, 557 U.S. at 323-24. And it was properly authenticated by Ms. Olson. *Compare with United States v. Baker*, 538 F.3d 324, 331 (5th Cir. 2008) (noting that the government failed to admit the NCMEC report via witness who had personal knowledge of how report was prepared or NCMEC's practice of preparing such a report).

More importantly, the specific part of the report that Miller challenges (the geolocation of the IP addresses)—does not constitute hearsay. The hearsay rule applies only to out-of-court statements, and it defines a statement as "a person's oral assertion, written assertion, or nonverbal conduct." Fed. R. Evid. 801(a), (c). Here, the challenged assertion was not made by a person—it was made by NCMEC's computer systems.

As explained by Ms. Olson at trial, Sections A and B of the CyberTipline report are automated. The contents of Section A were entered by the internet service provider (in this case, Google); as explained by Google, that process in this case was completely automated. Likewise, the contents of Section B are automatically generated by NCMEC's systems. That includes the geolocation results of the relevant IP addresses. There was simply no human analysis of the information memorialized in either Section A or B of the CyberTipline report in this case. Thus, those portions of the report do not qualify as "statements" of the analyst who assisted in preparing it. *See generally United States v. Lizarraga-Tirado*, 789 F.3d 1107, 1109-10 (9th Cir. 2015) (joining other circuits that "have held that machine statements aren't hearsay" in holding that "[a] tack placed by the Google Earth program and automatically labeled with GPS coordinates isn't hearsay."); *see United States v. Lamons*, 532 F.3d 1251, 1263-65 (11th Cir. 2008)

(noting that Confrontation Clause is concerned with statements of human witnesses); *United States v. Moon*, 512 F.3d 359, 362 (7th Cir. 2008) (noting that Confrontation Clause does not forbid use of raw data produced by instruments); *United States v. Washington*, 498 F.3d 225, 230 (4th Cir. 2007) (holding no violation of Confrontation Clause when statements came from raw data produced by machine); *United States v. Hamilton*, 413 F.3d 1138, 1142 (10th Cir. 2005) (determining header information produced by machine was not hearsay); *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir. 2003) (same).

That fact, alone, distinguishes this case from *United States v. Cameron*, 699 F.3d 621 (1st Cir. 2012), which held that admission of the NCMEC CyberTipline report without giving the defendant the opportunity to cross-examine the analyst who prepared it violated the defendant's rights under the Confrontation Clause. The government argued that the report was not testimonial hearsay. The *Cameron* court rejected that argument, reasoning:

> As mentioned earlier, the only reasonable explanation we can surmise is that the NCMEC employee who created these reports analyzed the information contained in the Image Upload Data sent by 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. We note that the Yahoo! CP Reports did not specify whether the "Suspect IP Address" was the IP Address from which the most recent image of child pornography had been uploaded, a representation which was in fact made in the CyberTipline Reports. Therefore, in order to make this

> representation, the NCMEC employee who prepared the CyberTipline Reports had to have analyzed the Image Upload Data sent by Yahoo!.
>
> In doing so, the NCMEC employee undertook a similar exercise to the one performed by the Yahoo! employee who created the CP Reports; they both analyzed the underlying information in the Image Upload Data and then used that information to create a separate, independent statement. The new statement made by NCMEC can be characterized along these lines: "based on the Yahoo! data, we have determined that the IP Address used by the suspect to upload the most recent image of child pornography is X, and the date and time of this upload is Y and Z."

Id. at 651.

Contrary to Miller's contention, no such analysis took place in this case. The fields in Section B of the NCMEC CyberTipline report, including the geolocation of the relevant IP addresses, were automatically generated by NCMEC's computers. In the end, though, like in *Cameron*, even if the district court erred in admitting the CyberTipline report, it was harmless because the email and attachments that were the impetus for the NCMEC CyberTipline report were admitted without objection by Miller. So, too, were the IP addresses that were provided by Google pursuant to a search warrant. Finally, Miller was convicted of four other counts of distribution of child pornography and the admission of the CyberTipline report was not relevant to any of those counts.

Miller's complaint about the government's closing argument has some merit. The assertion that the IP addresses resolved to a specific address—Miller's

residence—was, indeed, a misstatement. Although improper, the statement was isolated and, as set forth below, the evidence of Miller's guilt was overwhelming. Miller's argument that the misstatement exacerbated the alleged Confrontation Clause violation is disingenuous where counsel acknowledged that he had geographically resolved the IP addresses and could have cross-examined Ms. Olson about that process and/or the reliability and the precision of the results, but elected not to.

III. The evidence was sufficient to sustain Miller's convictions.

Miller was convicted of distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. § 2252(a)(2), (4). Section 2252(a) provides that "[a]ny person who . . . (2) knowingly receives, or distributes" or "knowingly possesses" child pornography "shall be punished as provided in subsection (b) . . . ." 18 U.S.C. § 2252(a). Miller persists in the same argument he made at trial: that he is not the person who committed the crimes. According to Miller, "[i]n general, evidence is insufficient to support a finding beyond a reasonable doubt when the State [sic] fails to establish that the defendant had exclusive possession of the device receiving child pornography." Miller's Brief at 28. His continued reliance on *United States v. Lowe*, 795 F.3d 519 (6th Cir. 2015), is misplaced.

Miller first cited to *Lowe* in moving—pursuant Federal Rule of Criminal Procedure 29—for judgment of acquittal at the conclusion of the government's case-in-chief. [R. 106: Eric G. Eckes, TR (Trial Day 2) at 1356.] Miller argued that "[t]here has been testimony that other people lived in the home . . . ," but acknowledged that there was no testimony that anyone else used the devices (the Acer laptop and Toshiba external hard drive) that had been admitted into evidence. [*Id*. at 1356-57.] The district court concluded that *Lowe* was easily distinguishable in denying Miller's motion for judgment of acquittal:

> Here we have the fact that the images were sent and received through the email assigned to this Mr. Miller—or assigned to miller694u@gmail.com. We've got photos of Mr. Miller sent from that email or chat, Google chat, if you will. I think the facts of this case are far different than those in *Lowe*, and there's certainly sufficient evidence from which a jury could conclude that the United States has sustained its burden on all seven accounts.

[R. 106: Court, TR (Trial Day 2) at 1360.] Miller renewed his motion following testimony by his wife, mother-in-law, and daughter, noting "[t]here's more evidence now about access to the computer," yet acknowledging "there's been nothing new about access to the emails." [R. 106: Eric G. Eckes, TR (Trial Day 2) at 1381-82.] The court remained unpersuaded and maintained its prior ruling that "[t]here's certainly sufficient evidence from which a reasonable jury could conclude that all the elements of the offense[s] have been satisfied based upon the

testimony of the prior government witnesses and the images that were found." [R. 106: Court, TR (Trial Day 2) at 1382.]

This Court reviews *de novo* a challenge to the sufficiency of the evidence in a criminal case. *United States v. Howard*, 621 F.3d 433, 459 (6th Cir. 2010). The Court must, however, view the evidence below in light most favorable to the prosecution and ask whether any rational trier of fact could have found the contested elements of a crime beyond a reasonable doubt. *United States v. Garcia*, 758 F.3d 714, 718 (6th Cir. 2014); *Jackson v. Virginia*, 443 U.S. 307, 319 (1979). "[A]n appellate court's reversal for insufficiency of the evidence is in effect a determination that the government's case against the defendant was so lacking that the trial court should have entered a judgment of acquittal, rather than submitting the case to the jury." *United States v. Wettstain*, 618 F.3d 577, 583 (6th Cir. 2010). A defendant bears a "very heavy burden" when he challenges the sufficiency of the evidence, as this court will not independently weigh the evidence nor make credibility determinations of the witnesses who testified before the jury at trial. *Garcia*, 758 F.3d at 718. Miller cannot overcome that burden.

In *Lowe*, this Court determined that it was unreasonable to infer that the defendant downloaded child pornography even though he owned and occasionally used the laptop on which the images were found. *Lowe*, 795 F.3d at 523. Because

two other people had access to the laptop, the Court determined that the evidence was insufficient to show that the defendant was the one who downloaded the child pornography. *Id*. at 523-24. According to the Court, "the evidence presented . . . fell well short of what we have found sufficient . . . in other cases involving multiple possible users of a single device:"

> In *United States v. Oufnac*, 449 F. App'x 472 (6th Cir. 2011), for instance, "ample other evidence" linked the defendant to images found on a shared device. *Id*. at 476. Although the computer in question had three user accounts, pornographic images appeared only in Oufnac's personal "My Documents" folder within his password-protected account. *Id*. at 473, 476-77. Oufnac's former girlfriend testified about finding child pornography on his computer on several previous occasions. When she confronted him, he said the images were "none of her business" but admitted that they aroused him, and, on one occasion, he agreed to destroy a compact disc on which she found "files and files and files and files" of child pornography. *Id*. at 473, 476. Oufnac also admitted to law enforcement that he recently viewed child pornography, although he later claimed that the images were "fake." *Id*. at 474, 476.
>
> Similarly, in *United States v. Mellies*, 329 F. App'x 592 (6th Cir. 2009), we sustained a defendant's conviction for possessing child pornography found on a laptop and compact discs in his home office, notwithstanding evidence that his wife and stepson occasionally used the laptop. *Id*. at 595, 607-08. The images were primarily stored in password-protected files and folders. *Id*. at 607. Mellies was "associated with" all but two of the hundreds of documents and thousands of emails stored on the laptop, and he was the only member of the household whose fingerprints appeared on compact discs containing child pornography. *Id*. at 595. Further, a detective testified that Mellies told arresting officers: "I'm not a part of some sort of a ring" and "[T]his is something that doesn't have anything to do with anybody else at all." *Id*. at 594.

Lowe, 795 F.3d at 524.

This case is distinguishable from *Lowe* in every meaningful way. First, the child pornography was transmitted via an email account that was subscribed to by "William Miller." In addition, the emails themselves told the story of who was using the account: William Miller. He used his own name, told the substantially the same story (which had elements of truth to it) to the people he was communicating with, and even transmitted photographs of himself when communicating via email. Miller's attempt at trial to label someone else the antagonist failed.

Moreover, the same images that Miller sent and received via the gmail account were found on an external hard that was seized from his residence. And when he was interviewed, he admitted that he purchased the hard drive and that he knew it contained child pornography, though he claimed the contraband pre-existed his possession. The forensic evidence revealed otherwise. Child pornography was found in user-created folders—that were created just a few months before Miller's home was searched and the hard drive was seized—and was organized by content. In short, Miller's "fingerprints"—digital and otherwise—were on all the evidence where the child pornography was found or through which it was shared.

CONCLUSION

This Court should affirm Miller's conviction and sentence.

Respectfully submitted,

ROBERT M. DUNCAN, JR.
UNITED STATES ATTORNEY

CHARLES P. WISDOM JR.
CHIEF, APPELLATE DIVISION

By: s/ Elaine K. Leonhard
Assistant United States Attorney
207 Grandview Drive, Suite 400
Ft. Mitchell, Kentucky 41017
(859) 652-7035
Elaine.K.Leonhard@usdoj.gov

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a)(7)(B). According to a computer count, the principal brief contains 8,092 words.

s/ Elaine K. Leonhard
Assistant United States Attorney

CERTIFICATE OF SERVICE

On December 19, 2018, I electronically filed this brief through the ECF system, which will send the notice of docket activity to:

Eric G. Eckes
Attorney for William J. Miller

s/ Elaine K. Leonhard
Assistant United States Attorney

APPELLEE'S DESIGNATION OF DISTRICT COURT DOCUMENTS

Record Entry	Description of Document	Page ID#
1	Indictment	1-3
20	Superseding Indictment	88-91
27	Motion	109-20
33	Response	138-97
48	Opinion and Order	259-77
62	Second Superseding Indictment	327-31
69	Minute Entry	357-58
70	Minute Entry	359-60
72	Minute Entry	396-97
75	Verdict	401-02
88	Judgment	444-50
90	Notice of Appeal	452-53
97	Trial Day 3 Transcript	844-909
105	Trial Day 1 Transcript	1046-174
106	Trial Day 2 Transcript	1175-394