**APPENDIX A**

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

---

| | |
|---|---|
| UNITED STATES OF AMERICA,<br>*Plaintiff-Appellee,*<br><br>v.<br><br>WILLIAM J. MILLER,<br>*Defendant-Appellant.* | No. 18-5578 |

Appeal from the United States District Court
for the Eastern District of Kentucky at Covington.
No. 2:16-cv-00047-1—David L. Bunning,
District Judge.

Argued: December 11, 2018

Decided and Filed: December 3, 2020

Before: McKEAGUE, KETHLEDGE, and MURPHY,
Circuit Judges.

---

**COUNSEL**

**ARGUED:** Eric G. Eckes, PINALES, STACHLER, YOUNG, BURRELL & CROUSE CO., L.P.A., Cincinnati, Ohio, for Appellant. Elaine K. Leonhard, UNITED STATES ATTORNEY'S OFFICE, Ft. Mitchell, Kentucky, for Appellee. **ON BRIEF:** Eric G. Eckes, PINALES, STACHLER, YOUNG, BURRELL

& CROUSE CO., L.P.A., Cincinnati, Ohio, for Appellant. Elaine K. Leonhard, UNITED STATES ATTORNEY'S OFFICE, Ft. Mitchell, Kentucky, Charles P. Wisdom, Jr., UNITED STATES ATTORNEY'S OFFICE, Lexington, Kentucky, for Appellee. Alan Butler, ELECTRONIC PRIVACY INFORMATION CENTER, Washington, D.C., Ryan T. Mrazik, PERKINS COIE LLP, Seattle, Washington, for Amici Curiae.

---

**OPINION**

---

MURPHY, Circuit Judge. Courts often must apply the legal rules arising from fixed constitutional rights to new technologies in an evolving world. The First Amendment's rules for speech apply to debate on the internet. *Packingham v. North Carolina*, 137 S. Ct. 1730, 1735–36 (2017). The Second Amendment's rules for firearms apply to weapons that did not exist "at the time of the founding." *District of Columbia v. Heller*, 554 U.S. 570, 582 (2008). The Supreme Court has made the same point for the rights at issue in this criminal case: The Fourth Amendment right against "unreasonable searches" and the Sixth Amendment right to confront "witnesses." *See Kyllo v. United States*, 533 U.S. 27, 34–36 (2001); *Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 315–17 (2009). We must consider how the established rules for these traditional rights should apply to a novel method for combatting child pornography: hash-value matching.

A hash value has been described as "a sort of digital fingerprint." *United States v. Ackerman*, 831 F.3d 1292, 1294 (10th Cir. 2016). When a Google employee views a digital file and confirms that it is child pornography, Google assigns the file a hash value. It then

scans Gmail for files with the same value. A "match" signals that a scanned file is a copy of the illegal file. Here, using this technology, Google learned that a Gmail account had uploaded two files with hash values matching child pornography. Google sent a report with the files and the IP address that uploaded them to the National Center for Missing and Exploited Children (NCMEC). NCMEC's systems traced the IP address to Kentucky, and a detective with a local police department connected William Miller to the Gmail account. Miller raises various constitutional challenges to his resulting child-pornography convictions.

He starts with the Fourth Amendment, arguing that Google conducted an "unreasonable search" by scanning his Gmail files for hash-value matches. But the Fourth Amendment restricts government, not private, action. And while Google's hash-value matching may be new, private searches are not. A private party who searches a physical space and hands over paper files to the government has not violated the Fourth Amendment. *Burdeau v. McDowell*, 256 U.S. 465, 475 (1921). That rule covers Google's scan of virtual spaces and disclosure of digital files.

Miller next argues that the police detective conducted an "unreasonable search" when he later opened and viewed the files sent by Google. This claim implicates another settled rule: Under the private-search doctrine, the government does not conduct a Fourth Amendment search when there is a "virtual certainty" that its search will disclose *nothing more* than what a private party's earlier search has revealed. *United States v. Jacobsen*, 466 U.S. 109, 119 (1984). So we must ask whether the detective's manual search would disclose anything more than what Google's hash-value search showed. Critically, Miller

does not dispute the district court's finding about a hash-value match's near-perfect accuracy: It created a "virtual certainty" that the files in the Gmail account were the known child-pornography files that a Google employee had viewed. Given this (unchallenged) reliability, *Jacobsen*'s required level of certainty is met.

Miller thus asks us to depart from *Jacobsen*'s idiosyncratic definition of a Fourth Amendment "search," noting that the Supreme Court recently clarified that such a "search" also occurs when the government trespasses onto property to obtain information. *United States v. Jones*, 565 U.S. 400, 404–08 (2012). At the least, Miller says, the detective's opening of the files qualifies as a search in this "trespass-to-chattels" sense. He raises a legitimate (if debatable) point. The Supreme Court has long required the government to obtain a warrant to open sealed letters, the equivalent of modern emails. *Ex parte Jackson*, 96 U.S. 727, 732–33 (1877). Yet, well before *Jacobsen*, the Court also allowed the government to rely on letters illegally taken and opened by private parties. *Burdeau*, 256 U.S. at 474–75. And Google arguably "opened" the files and committed the "trespass" here. In the end, though, we need not resolve this debate. We find ourselves bound by *Jacobsen* no matter how this emerging line of authority would resolve things.

Miller lastly argues that the admission of NCMEC's report at trial violated his Sixth Amendment right to confront "witnesses." This right's basic rule (that a defendant must have the opportunity to cross-examine those who make testimonial statements) certainly applies to new types of witnesses, such as forensic analysts. *Melendez-Diaz*, 557 U.S. at 313–21. But the rule's reach is nevertheless limited to statements by "witnesses"—that is, people. And

NCMEC's automated systems, not a person, entered the specific information into the report that Miller challenges. The rules of evidence, not the Sixth Amendment, govern the admissibility of this computer-generated information.

For these reasons and those that follow, we affirm Miller's convictions.

## I

### A

Many companies rely on hash-value matching to remove child pornography from their email, file-sharing, and similar internet services. *Amicus* Br. of Discord et al., at 4–5. "A hash value is a number that is often represented as a sequence of characters and is produced by an algorithm based upon the digital contents of a drive, medium, or file." 2017 Advisory Committee Note to Fed. R. Evid. 902(14). As a government witness explained, hash values can be created using common algorithms like SHA or MD5. Johnson Tr., R.106, PageID#1290. "You basically point this algorithm toward a file, and you get back this alphanumeric string, and that's a series of characters that are a fingerprint; the VIN number or the DNA, if you will, of that file." *Id.* Some algorithms assign a character to every pixel in an image, such that the hash value will change if a single pixel changes. *Id.*, PageID#1291. Other programs, like Microsoft's PhotoDNA, return the same value even if a file changes slightly. *Id.* After companies assign a "hash value" to a known image of child pornography, they can scan their services for files with the same value. When they get a "match," they know that the scanned file is a duplicate of the child-pornography image without opening and viewing the file. *Amicus* Br. of Discord et al., at 4–5.

Apart from commonly used hash algorithms, companies create their own unique programs. "[S]ince 2008," for example, "Google has been using its own proprietary hashing technology to tag confirmed child sexual abuse images." McGoff Decl., R.33-1, PageID#161. When a Google employee finds a child-pornography image on its services, Google gives this image a "hash" and adds it to its "repository of hashes of apparent child pornography as defined in 18 U.S.C. § 2256." *Id.* Google might also discover child pornography from a customer's complaint, but "[n]o hash is added to [its] repository without the corresponding image first having been visually confirmed by a Google employee to be apparent child pornography." *Id.*

Google's terms of service inform its customers that they may not use services like Gmail in violation of the law. *Id.* The terms indicate: "We may review content to determine whether it is illegal or violates our policies, and we may remove or refuse to display content that we reasonably believe violates our policies or the law. But that does not necessarily mean that we review content, so please don't assume that we do." Terms, R.33-1, PageID#164.

Consistent with these terms, Google's "product abuse detection system" scans some files that customers upload looking for hash-value matches with the files in its child-pornography repository. McGoff Decl., R.33-1, PageID#161–62. When this system detects a match, Google does one of two things. *Id.* An employee might view the file to confirm that it is child pornography. *Id.*, PageID#162. Or Google might just send an automated report with the file to the National Center for Missing and Exploited Children (NCMEC). *Id.* NCMEC, a nonprofit entity, "was created to help find

missing children, reduce child sexual exploitation, and prevent child victimization." Shehan Decl., R.33-6, PageID#193.

Companies like Google have business reasons to make these efforts to remove child pornography from their systems. As a Google representative noted, "[i]f our product is associated with being a haven for abusive content and conduct, users will stop using our services." McGoff Decl., R.33-1, PageID#161. Yet once "electronic communication services providers" become aware of child pornography on their services, federal law requires them to report it to NCMEC. 18 U.S.C. §§ 2258A(a), 2258E(6). NCMEC operates a "CyberTipline" that allows companies to securely disclose child pornography. Shehan Decl., R.33-6, PageID#194–95.

Companies use a standardized "CyberTipline Report" to send images to NCMEC. A company will complete the report's "Section A" by identifying, among other things, the date that the company discovered the file and the IP address that uploaded it. Rep., R.33-2, PageID#169–71. After a company sends this information, NCMEC's systems run a search for the location of the IP address and input the results into "Section B" of the report. *Id.*, PageID#172. An analyst next might manually search public information to identify a suspect (for example, an analyst might look for information associated with the email address that sent the file). *Id.*, PageID#174–76. This analyst might also look at the image, depending on such factors as whether the inspection could identify the culprit. Shehan Decl., R.33-6, PageID#195. The analyst adds the search results to "Section C" of the report. Rep., R.33-2, PageID#174–77. NCMEC sends the completed report to the law-enforcement agency in the area of the IP address. Shehan Decl., R.33-6, PageID#196.

B

This case concerns Gmail. On July 9, 2015, the email address "miller694u@gmail.com" attached two files to an email that had hash values matching images in Google's child-pornography repository. Rep., R.33-2, PageID#170–71. One file was named "young - tight fuck.jpg"; the other was named "!!!!!!Mom&son7.jpg." *Id.*, PageID#170. Google deactivated the account. The next day, it sent NCMEC an automated CyberTipline Report. *Id.*, PageID#169. No Google employee viewed the files. The report classified the images as "A1" under an industry-wide classification scheme, which meant that they were of prepubescent minors engaged in sex acts. *Id.*, PageID#170–72. Google listed two IP addresses associated with the Gmail account. From the first IP address, someone had uploaded the images into Gmail on July 9 and logged into the account several times during the prior month. From the second IP address, someone had registered the account on January 29, 2015. *Id.*

Once NCMEC received this report, its systems performed a "WhoIs lookup" for the IP addresses. This search identified their location as Fort Mitchell, Kentucky, and their internet service provider as Time Warner Cable. *Id.*, PageID#172. An analyst next searched for information connected to miller694u@gmail.com. *Id.*, PageID#174–77. This email was affiliated with a profile page of "Bill M." on the social-media website "Tagged." *Id.* The profile page included a picture of "Bill M." The analyst attached a printout of the page with the picture to the report. *Id.*, PageID#177. The analyst did not view the files. NCMEC sent the report and files to the Kentucky

State Police. The state police forwarded this information to the police department in Kenton County (the county encompassing Fort Mitchell).

On August 13, 2015, Detective Aaron Schihl with the Kenton County Police Department received the report. Schihl opened and viewed the two files and confirmed that they showed prepubescent children engaged in sex acts.

After subpoenaing Time Warner Cable, Schihl learned that the IP address that uploaded the child pornography was assigned to subscriber "Tania Miller" at a Fort Mitchell home address. He also learned that "William Jay Miller" had a driver's license that listed this address. Schihl obtained a warrant for the records that Google retained for this Gmail account. The records identified "Bill Miller" as the subscriber. Google provided about 4,000 emails and chat messages, as well as information in a file-storage account. Schihl found more child pornography in the file-storage account and in email exchanges from May 2015.

Schihl next got a warrant to search Miller's home. In October 2015, the police seized computers, flash drives, and hard drives. A forensic examination of an external hard drive turned up 571 child-pornography files (including the files from the July 9 email) organized in folders named things like "pre-teen." The IP address for Miller's laptop matched an IP address from the CyberTipline Report, and the laptop appeared to have been connected to the external hard drive. In an interview with Schihl, Miller admitted that his hard drive contained child pornography, but claimed that the images had been on the drive when he bought it at a yard sale a year earlier. A forensic

examination, in fact, showed that the child-pornography files had been created on the hard drive a week before the July 9 email.

The government indicted Miller on seven counts of knowingly receiving, distributing, or possessing child pornography. 18 U.S.C. § 2252(a)(2), (a)(4)(B). These counts corresponded to the email exchanges of child pornography from May 2015, the email containing the two files on July 9, and the files on the hard drive in Miller's home. Miller moved to suppress this evidence on the ground that the police learned of the child-pornography images attached to the July 9 email in violation of the Fourth Amendment. The district court denied his motion. *United States v. Miller*, 2017 WL 2705963, at *8 (E.D. Ky. June 23, 2017).

Miller stood trial. The government introduced the CyberTipline Report through the testimony of an NCMEC director. Miller raised a Confrontation Clause objection because this witness was not the analyst who had worked on the report. The district court overruled his objection.

As Miller's main defense, his counsel argued that he was not the person who had emailed child pornography or placed child pornography on the hard drive. Counsel highlighted that a few emails about a cellphone rebate sent to this Gmail account had been addressed to Miller's brother, Fred Miller. Miller's wife, mother-in-law, and daughter testified that Fred, whom they described as "strange" or "simple-minded," came to their house about once a week and sometimes used Miller's laptop.

The government sought to rebut Miller's attempt to shift blame to his brother. Detective Schihl went through many messages from the Gmail account

showing a person named "Bill" propositioning women using Miller's photos. Schihl also testified that the "Tagged" profile page connected to this Gmail account used a picture of Miller. The forensic examiner likewise explained that the hard drive with the child-pornography folders included a folder named "me" full of Miller's pictures. And it contained Skype messages requesting pictures of naked children using the display name "Bill Miller."

The jury convicted Miller on all counts. The district court sentenced him to 150 months in prison followed by 15 years of supervised release.

Miller appeals. He argues: (1) that the government violated his Fourth Amendment right against unreasonable searches; (2) that the district court violated his Sixth Amendment right to confront witnesses; and (3) that district court wrongly found sufficient evidence to convict him.

## II. Fourth Amendment

The Fourth Amendment provides in relevant part: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated[.]" U.S. Const. amend. IV. Miller asserts that the government committed two "unreasonable searches": the first when Google discovered the two files in Miller's email on July 9 and the second when Detective Schihl later opened and viewed those files.

### A. Did Google's has-value matching violate the Fourth Amendment?

Miller claims that Google conducted an "unreasonable search" by scanning his July 9 email for hash-

value matches. This claim faces an immediate (and ultimately insurmountable) obstacle: Google is a private entity. Like other constitutional rights, *see Manhattan Cmty. Access Corp. v. Halleck*, 139 S. Ct. 1921, 1928 (2019), the Fourth Amendment regulates only government action, *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). If, for example, a private party enters your home in search of incriminating papers, that party may have committed a trespass under state tort law, but the party has not engaged in an unreasonable search under the Fourth Amendment. *See Burdeau v. McDowell*, 256 U.S. 465, 475 (1921). Indeed, until it was incorporated against the states, the Fourth Amendment did not even apply to state officers (like Detective Schihl) who acted independently of federal officers. *See Byars v. United States*, 273 U.S. 28, 33–34 (1927); *cf. Elkins v. United States*, 364 U.S. 206, 215 (1960). And although the Fourteenth Amendment has now expanded the Fourth Amendment's reach to cover state actors, it too regulates only government action, not private action. *See Civil Rights Cases*, 109 U.S. 3, 17–18 (1883).

This "government" action most obviously exists when public employees perform public functions. *See West v. Atkins*, 487 U.S. 42, 49–50 (1988). But the Constitution does not compel governments to conduct their affairs through the "public employees" that they typically use today. *Spencer v. Lee*, 864 F.2d 1376, 1379 (7th Cir. 1989) (en banc). Historically, "[p]rivate citizens were actively involved in government work, especially where the work most directly touched the lives of the people." *Filarsky v. Delia*, 566 U.S. 377, 385 (2012). It was, for example, "a common practice in this country for private watchmen or guards to be vested with the powers of policemen, sheriffs or peace

officers to protect the private property of their private employers," but states considered them "public officers when performing their public duties." *NLRB v. Jones & Laughlin Steel Corp.*, 331 U.S. 416, 429, 431 (1947). And "[t]he Constitution constrains governmental action 'by whatever instruments or in whatever modes that action may be taken.'" *Lebron v. Nat'l R.R. Passenger Corp.*, 513 U.S. 374, 392 (1995) (quoting *Ex parte Virginia*, 100 U.S. 339, 346–47 (1880)).

This rule raises the key question: When should a private party's actions be "fairly attributable" to the government and trigger the Constitution's protections? *Lugar v. Edmondson Oil Co.*, 457 U.S. 922, 937 (1982). One approach to this constitutional "agency" question would be to review our legal traditions and consider situations in which our laws have historically imputed one person's conduct to another. After all, "traditional agency principles were reasonably well ensconced in the law at the time of the founding[.]" *United States v. Ackerman*, 831 F.3d 1292, 1301 (10th Cir. 2016) (Gorsuch, J.). Yet the Supreme Court has stated that "[w]hat is fairly attributable is a matter of normative judgment, and the criteria lack rigid simplicity." *Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n*, 531 U.S. 288, 295 (2001). It has adopted a fact-bound approach to this attribution question, one that uses "different factors or tests in different contexts." *Lugar*, 457 U.S. at 939. Sometimes, the Court uses a "function" test that asks whether a private party performs a public function. *Romanski v. Detroit Ent., L.L.C.*, 428 F.3d 629, 636 (6th Cir. 2005). Other times, the Court uses a "compulsion" test that asks whether the government compelled a private party's action. *Id.* Still other times, the Court uses a

"nexus" test that asks whether a private party cooperated with the government. *Id.*; *see Halleck*, 139 S. Ct. at 1928.

As the party seeking to suppress evidence, Miller must prove that Google's actions were government actions under one of these tests. *United States v. Ringland*, 966 F.3d 731, 735 (8th Cir. 2020); *cf. United States v. Baker*, 976 F.3d 636, 645 (6th Cir. 2020). He has fallen short.

1. *Did Google perform a public function?* The Supreme Court has held that some functions qualify as "government" functions no matter who performs them. *Halleck*, 139 S. Ct. at 1928–29. Yet few activities qualify. *Id.* at 1929. If a function is always a "government" action, it means that the government may not deregulate by allowing private parties to perform the action without becoming the "government" themselves. *See Spencer*, 864 F.2d at 1379. This test thus covers only those limited activities—for example, running a city—that have "traditionally *and* exclusively" been performed by the government. *Durante v. Fairlane Town Ctr.*, 201 F. App'x 338, 341 (6th Cir. 2006) (citing *Jackson v. Metro. Edison Co.*, 419 U.S. 345, 352 (1974)); *see Marsh v. Alabama*, 326 U.S. 501, 505–09 (1946). Most activities—such as providing electricity, operating a nursing home, or managing a public-access television station—will not qualify. *See Halleck*, 139 S. Ct. at 1929; *Blum v. Yaretsky*, 457 U.S. 991, 1011–12 (1982); *Jackson*, 419 U.S. at 352–53.

Miller has not shown that Google's hash-value matching satisfies this test. Admittedly, the investigation of a crime (like the possession of child pornography) has long been performed by the government. *Ackerman*, 831 F.3d at 1295. But it has also long been

performed by private parties protecting their property. Think of shopkeepers investigating theft by shoplifters or insurance companies investigating arson by claimants. *See Chapman v. Higbee Co.*, 319 F.3d 825, 833–34 (6th Cir. 2003) (en banc); *United States v. Howard*, 752 F.2d 220, 227–28 (6th Cir. 1985), *adopted en banc in relevant part* 770 F.2d 57, 62 (6th Cir. 1985). Only when a party has been "endowed with law enforcement powers beyond those enjoyed by" everyone else have courts treated the party's actions as government actions. *Ackerman*, 831 F.3d at 1296; *see Romanski*, 428 F.3d at 636–37. And Miller identifies nothing that gave Google any special police powers.

2. *Did Google act under compulsion?* Even if a private party does not perform a public function, the party's action might qualify as a government act if the government "has exercised coercive power or has provided such significant encouragement, either overt or covert, that the choice must in law be deemed to be that of the" government. *Blum*, 457 U.S. at 1004; *see Adickes v. S. H. Kress & Co.*, 398 U.S. 144, 170–71 (1970). When, for example, federal regulations *compelled* private railroads to conduct post-accident drug and alcohol testing of employees involved in train accidents, the Supreme Court held that the railroads were engaged in "government" searches. *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 614 (1989). Not only that, when other regulations merely *permitted* railroads to undertake this testing in other situations, the Court held that even these tests qualified as "government" searches. *Id.* at 611–12, 615. Several "features" of these regulations led the Court to treat the nonmandatory private testing as government action. *Id.* at 615. The regulations preempted conflicting

state laws and collective-bargaining terms, conferred on the government a right to receive test results, barred railroads from contracting away their testing rights, and prohibited employees from refusing to take tests. *Id.*

At the same time, private action does not become government action merely because the government authorizes or acquiesces in it. *See Flagg Bros., Inc. v. Brooks*, 436 U.S. 149, 164–65 (1978). Even extensive regulation of a private party will not turn its every action into government action. *See Am. Mfrs. Mut. Ins. Co. v. Sullivan*, 526 U.S. 40, 57–58 (1999). The Supreme Court thus refused to find "government" action when a utility disconnected a customer's electricity even though the utility had been subject to broad state oversight and the state had approved the utility's general disconnection practice. *See Jackson*, 419 U.S. at 352–58.

Miller has not shown that Google's hash-value matching falls on the "compulsion" side of this line. He cites no law that compels or encourages Google to operate its "product abuse detection system" to scan for hash-value matches. Federal law disclaims such a mandate. It says that providers need not "monitor the content of any [customer] communication" or "affirmatively search, screen, or scan" files. 18 U.S.C. § 2258A(f). Nor does Miller identify anything like the government "encouragement" that the Court found sufficient to turn a railroad's drug and alcohol testing into "government" testing. *See Skinner*, 489 U.S. at 615. In that context, regulations authorized the testing and barred railroads from contracting away their rights. *Id.* In this context, Miller identifies no regulations authorizing Google's hash-value matching or barring Google from changing its terms of service to

prohibit the practice. *See United States v. Richardson*, 607 F.3d 357, 365–67 (4th Cir. 2010). Google's decision to scan its customers' files is instead like the utility's decision to disconnect its customers' electricity: The "initiative" to take both actions "comes from" the private party, not the government. *Jackson*, 419 U.S. at 357.

Miller responds by identifying government compulsion for a different activity. Federal law requires "electronic communication service providers" like Google to notify NCMEC when they become aware of child pornography. 18 U.S.C. § 2258A(a). But this mandate compels providers only to *report* child pornography that they know of; it does not compel them to *search* for child pornography of which they are unaware. *Id.* § 2258A(f). And the Supreme Court's cases tell us to focus on "the specific conduct of which [a party] complains." *Sullivan*, 526 U.S. at 51 (quoting *Blum*, 457 U.S. at 1004). That conduct is Google's hash-value matching, not its reporting.

Precedent confirms this point. Many courts have found that a "reporting requirement, standing alone, does not transform [a service provider] into a government agent whenever it chooses to scan files sent on its network for child pornography." *Ringland*, 966 F.3d at 736 (quoting *United States v. Stevenson*, 727 F.3d 826, 830 (8th Cir. 2013)); *United States v. Cameron*, 699 F.3d 621, 637–38 (1st Cir. 2012); *United States v. Wolfenbarger*, 2019 WL 6716357, at *13–16 (N.D. Cal. Dec. 10, 2019) (citing cases). More generally, many laws require certain individuals, such as teachers or doctors, to report child abuse. In that context, too, courts have held that reporting mandates do not transform private parties into government actors for purposes of various constitutional provisions. *See,*

*e.g.*, *Mueller v. Auker*, 700 F.3d 1180, 1191–92 (9th Cir. 2012); *Brown v. Newberger*, 291 F.3d 89, 93–94 (1st Cir. 2002).

History also confirms the point. At common law, citizens had "a duty to raise the 'hue and cry' and report felonies" of which they were aware. *Branzburg v. Hayes*, 408 U.S. 665, 696 & nn.34–35 (1972). A person might commit a "misprision of felony" by failing to do so. *United States v. Caraballo-Rodriguez*, 480 F.3d 62, 71 (1st Cir. 2007); *see* Carl Wilson Mullis, *Misprision of Felony: A Reappraisal*, 23 Emory L.J. 1095 (1974). It would be odd to think that this reporting duty turned the entire populace into government actors. *Cf. Doe v. Rains Cnty. Indep. Sch. Dist.*, 66 F.3d 1402, 1411 (5th Cir. 1995). Indeed, English law imposed a harsher sentence on a "public officer" who failed to report a crime (as compared to a "common person"); it did not treat everyone as a government officer. 4 William Blackstone, *Commentaries on the Laws of England* *121. At the least, Miller has not shown that this common reporting duty turns private parties into public actors whenever they do something other than disclose a crime, such as voluntarily investigate it.

3. *Did Google have a nexus to government actors?* Private action might still be attributed to the government if "a sufficiently close nexus" exists between a private party and government actors. *Jackson*, 419 U.S. at 351; *cf. Byars*, 273 U.S. at 32–34. Our traditions can shed light on the required "nexus." *Cf. Ackerman*, 831 F.3d at 1301. At common law, for example, a conspirator's actions were imputed to coconspirators, so private action could be treated as government action if private and public actors conspired to violate constitutional rights. *Rudd v. City of Norton Shores*, 977 F.3d 503, 512–13 (6th Cir. 2020). Similarly, at

common law, an agency relationship was created through a "manifestation of consent by one person to another that the other shall act on his behalf and subject to his control, and consent by the other so to act." *Ackerman*, 831 F.3d at 1301 (quoting Restatement (Second) of Agency § 1 (Am. L. Inst. 1958)). In the search context, our cases have asked two questions to identify these constitutional agency relationships: What was the private party's intent in undertaking a search? And did the government acquiesce to the search? *See United States v. Bowers*, 594 F.3d 522, 525–26 (6th Cir. 2010).

Miller failed to show that Google acted as a government agent under this test. Consider Google's intent. Miller cites nothing suggesting that it intended to act as a police agent. Google instead sought to rid its virtual spaces of criminal activity for the same reason that shopkeepers have sought to rid their physical spaces of criminal activity: to protect their businesses. *See Chapman*, 319 F.3d at 834. Google does not want its services to become a "haven for abusive content" because customers will stop using them if that occurs. McGoff Decl., R.33-1, PageID#161; *see Stevenson*, 727 F.3d at 830–31. And Google "cooperated" with law enforcement in this case only by sending a report. Yet courts typically reject arguments that a private party's decision to call 911 or report a crime creates an "agency" relationship with the responding authorities. *See, e.g.*, *Moldowan v. City of Warren*, 578 F.3d 351, 399 (6th Cir. 2009).

Now consider the government's perspective. Miller again cites no evidence that Detective Schihl or any other law-enforcement officer influenced Google's decision to scan the files in the July 9 email for hash-value matches. *See Richardson*, 607 F.3d at 364–65.

Police got involved only after Google had performed that scan and uncovered the crime. *See Burdeau*, 256 U.S. at 474–75; *cf. United States v. Booker*, 728 F.3d 535, 540–45 (6th Cir. 2013).

Miller responds that Google has cooperated with NCMEC in other ways, including by participating in an NCMEC-led exchange of child-pornography hash values and by helping design NCMEC's standard report. Miller argues that these activities create a nexus with the government because he asks us to treat NCMEC, a private entity, as a government actor. The Tenth Circuit viewed NCMEC in that light. *Ackerman*, 831 F.3d at 1295–1300. We need not take a position on it. Even if NCMEC were a government actor, these activities do not show that Google acted as an NCMEC "agent" when engaging in the specific hash-value scanning at issue here. Google did not even scan for any NCMEC-provided hash values during the relevant time. McGoff Decl., R.33-1, PageID#162. And child pornography is tragically common. So it makes sense for providers that must report it to create a generic form for their "convenience," whether or not they have agreed with government actors to conduct searches. *See Gramenos v. Jewel Cos.*, 797 F.2d 432, 435–36 (7th Cir. 1986). Google's hash-value matching thus did not implicate the Fourth Amendment.

B. Was Detective Schihl's viewing of the images an "unreasonable search"?

Unable to rely on Google's private actions, Miller turns to Detective Schihl's public actions. Miller argues that Schihl conducted an illegal "search" when, without a warrant, he viewed the files that Google sent. In recent years, the Supreme Court has followed

two approaches to decide whether a Fourth Amendment "search" has occurred. *Taylor v. City of Saginaw*, 922 F.3d 328, 332 (6th Cir. 2019). Miller invokes both. Using the Supreme Court's primary definition of a "search," he argues that Detective Schihl invaded his "reasonable expectation of privacy" when viewing the files. Using an alternative property-based definition, Miller also argues that Schihl committed a "trespass" when viewing the files. We address each argument in turn.

1. Did Detective Schihl invade Miller's reasonable expectation of privacy?

When interpreting the Fourth Amendment over the last fifty years, the Supreme Court has typically not relied on the usual definition of the word "search" ("[t]o look over or through for the purpose of finding something"). *Kyllo v. United States*, 533 U.S. 27, 32 n.1 (2001) (quoting Noah Webster, *An American Dictionary of the English Language* 66 (1828) (reprint 6th ed. 1989)); *Morgan v. Fairfield Cnty.*, 903 F.3d 553, 570–72 (6th Cir. 2018) (Thapar, J., concurring). Since *Katz v. United States*, 389 U.S. 347 (1967), the Court has instead defined the word to mean a government intrusion into a person's "expectation of privacy that society is prepared to consider reasonable." *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010) (quoting *Jacobsen*, 466 U.S. at 113). This definition requires us to consider whether a person has an expectation of privacy in the space the government invaded and whether that subjective expectation is objectively reasonable. *Id.*

We thus must consider whether Miller had a reasonable expectation of privacy in the two files that De-

tective Schihl viewed. We begin, though, by identifying two questions that we need not consider. The first: Did Miller have a reasonable expectation of privacy in his Gmail account? Our court has held that individuals generally have reasonable expectations of privacy in the emails that they send through commercial providers like Google. *Id.* at 283–88. (Caselaw on this issue remains "surprisingly sparse" outside our circuit. 2 Wayne R. LaFave et al., Crim. Proc. § 4.4(c) (4th ed.), Westlaw (database updated Dec. 2019).) Yet Google's terms of service also permit it to view its customers' content for illegal items. *Warshak* added "that a subscriber agreement might, in some cases, be sweeping enough to defeat a reasonable expectation of privacy in the contents of an email account" (while suggesting that this outcome would be rare). 631 F.3d at 286. But here we need not consider whether Google's terms are of the "sweeping" sort and will assume that Miller had a reasonable expectation of privacy in his email.

The second: Did the hash-value matching "invade" Miller's reasonable expectation of privacy? According to the Supreme Court, binary searches that disclose only whether a space contains contraband are not Fourth Amendment "searches." *Illinois v. Caballes*, 543 U.S. 405, 408 (2005). The Court has held, for example, that the government does not invade a reasonable expectation of privacy when a police dog sniffs luggage for drugs. *United States v. Place*, 462 U.S. 696, 706–07 (1983). Yet the Court has also held that a thermal-imaging device detecting the heat emanating from a house invades such an expectation because it can show more than illegal growing operations (such as the "hour each night the lady of the house takes her daily sauna and bath"). *Kyllo*, 533 U.S. at 38. Which category does hash-value matching fall within? Is it

like a dog sniff? Or a thermal-imaging device? We also need not consider this question and will assume that hash-value searching counts as an invasion of a reasonable expectation of privacy. *Cf.* Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38 (2005).

We do not resolve these questions because Detective Schihl did not monitor the Gmail account. Google did. This case thus concerns another part of the Court's expectation-of-privacy test known as the "private-search doctrine." *See United States v. Lichtenberger*, 786 F.3d 478, 481–82 (6th Cir. 2015); *see also United States v. Reddick*, 900 F.3d 636, 637 (5th Cir. 2018). The Court has held that government conduct does not infringe a reasonable expectation of privacy (or qualify as a "search") if the conduct does not exceed the "scope" of an earlier private search. *Jacobsen*, 466 U.S. at 115. Two cases created this doctrine and illustrate its boundaries. *Id.* at 118–26; *Walter v. United States*, 447 U.S. 649, 653–59 (1980) (Stevens, J., opinion).

Start with *Jacobsen*. There, Federal Express employees opened a package for insurance reasons because it had been damaged in route. 466 U.S. at 111. Within this box, they discovered a tube "made of the silver tape used on basement ducts" covered by newspaper. *Id.* They cut open the tube and found bags with white powder. *Id.* The employees returned the bags to the tube and the tube to the box and called the police. *Id.* A DEA agent arrived and took everything back out. *Id.* The agent also conducted a field test of the powder to determine if it was cocaine. *Id.* at 111–12, 122. The Court rejected a Fourth Amendment challenge to the agent's actions. *Id.* at 113–26. It described the key question as whether those actions "exceeded the

scope" of the private search. *Id.* at 115. To answer this question, the Court divided the actions into two parts, separately analyzing the agent's decision to examine the box and test the powder. As for the examination, the Court held that the agent's conduct "infringed no legitimate expectation of privacy and hence was not a 'search'" because the employees had also searched the box and made it freely available. *Id.* at 118–20. As for the testing, the Court concluded that it exceeded the scope of the private search. *Id.* at 122. But it held that the testing was not a "search" for a different reason: because, like a dog sniff, it could reveal only whether the powder was (or was not) cocaine. *Id.* at 123.

Turn to *Walter*. There, packages containing boxes of films were delivered to the wrong company. 447 U.S. at 651 (Stevens, J., opinion). The company's employees opened the packages and discovered that the boxes had "explicit descriptions" suggesting the films were obscene. *Id.* at 652. After the employees called the FBI, agents watched the films to confirm their obscenity status. *Id.* In a fractured decision, the Court found a Fourth Amendment violation from the decision to watch the films without obtaining a warrant. *See Jacobsen*, 466 U.S. at 115–16. Justice Stevens's opinion reasoned that "the unauthorized exhibition of the films constituted an unreasonable invasion of their owner's constitutionally protected interest in privacy." 447 U.S. at 654 (Stevens, J., opinion). The private employees had seen only the labels, and watching the films was a "significant expansion" of that search. *Id.* at 657; *see also id.* at 661–62 (White, J., concurring in part and concurring in the judgment).

What rule emerges from these cases to decide when government actions "exceed[] the scope of the

private search"? *Jacobsen*, 466 U.S. at 115. *Jacobsen* suggested that the box "could no longer support any expectation of privacy" because "there was a virtual certainty" that the DEA agent would learn *nothing more* by reopening the box than what the FedEx employees had learned in their initial search of it. *Id.* at 119, 120 n.17, 121. *Walter* suggested that the films could support an expectation of privacy because the FBI agents would learn *much more* by watching the films than what the private employees had learned from viewing the labels alone, which permitted only "inferences about what was on the films." 447 U.S. at 657 (Stevens, J., opinion). Putting these outcomes together, we have held that the private-search doctrine requires a private actor's search to create a "virtual certainty" that a government search will disclose nothing more than what the private party has already discovered. *See Lichtenberger*, 786 F.3d at 488; *cf. United States v. Runyan*, 275 F.3d 449, 463–64 (5th Cir. 2001) (substantial-certainty test).

Applying this test, we must ask whether Google's hash-value search of the files using its digital eyes made it virtually certain that Detective Schihl would discover no more than what Google had learned when he viewed the images with his human eyes. *Jacobsen*, 466 U.S. at 119. We are helped in this endeavor by two thoughtful decisions applying the private-search doctrine in this new context. *Reddick*, 900 F.3d at 638–39; *Ackerman*, 831 F.3d at 1305–07.

In *Ackerman*, AOL matched one image in the defendant's email with a child-pornography hash value. AOL sent the email and its four images to NCMEC. 831 F.3d at 1294. An NCMEC analyst viewed the email and images. *Id.* In an opinion by then-Judge Gorsuch, the Tenth Circuit held that NCMEC's search

exceeded the scope of AOL's search. *Id.* at 1305–06. AOL learned only that a single image had a hash-value match, but the NCMEC analyst viewed the entire email. *Id.* The analyst's search thus disclosed a lot more information: whether the other images were child pornography and whether the email contained correspondence. *Id.* Yet *Ackerman* reserved whether its holding would change if the analyst had viewed *only* the one image. *Id.* at 1306.

In *Reddick*, the Fifth Circuit considered this reserved question. There, the defendant loaded images into a Microsoft account with hash values matching child pornography. 900 F.3d at 637–38. Microsoft sent the images to NCMEC, which shared them with a detective. *Id.* at 638. The court held that the detective's viewing did not exceed the scope of Microsoft's search. *Id.* at 639. It gave two reasons. Microsoft's hash-value matching allowed it to identify child pornography "with almost absolute certainty[.]" *Id.* (citation omitted). And the detective's viewing "was akin to the government agents' decision to conduct chemical tests on the white powder in *Jacobsen*." *Id.*

Our case is like *Reddick* rather than *Ackerman* because Detective Schihl viewed only files with hash-value matches. And we agree with *Reddick*'s holding that the private-search doctrine applies. But we opt not to rely on *Reddick*'s second reason: that the detective's viewing of the images was like the DEA agent's testing of the powder in *Jacobsen*. *Jacobsen* recognized that this testing "exceeded the scope" of the FedEx employees' search, so the Court held that it did not qualify as a "search" for a reason unrelated to the private-search doctrine. 466 U.S. at 122. The binary test revealed only "whether or not a suspicious white

powder was cocaine." *Id.* If the test came back negative, it would not disclose what the substance was—whether "sugar or talcum powder." *Id.* This logic does not cover Schihl's actions. If the files portrayed something other than child pornography, Schihl would have learned what they showed—whether an embarrassing picture of the sender or an innocuous family photo. His inspection (unlike the test) qualifies as the invasion of a "legitimate privacy interest" *unless* Google's actions had already frustrated the privacy interest in the files. *Id.* at 123; *cf. Riley v. California*, 573 U.S. 373, 401 (2014).

Rather than compare Schihl's viewing of the files to the agent's field test, we must compare Google's search of the files to the FedEx employees' search of the box. Did Google's "electronic" inspection create the same level of certitude as the FedEx employees' "manual" inspection that the later government search would reveal nothing more than what the private parties had already discovered? Recall what Google had learned. At some point, Google employees who are trained on the federal definition of child pornography viewed two images to confirm that they are illegal child pornography before adding them to its child-pornography repository. McGoff Decl., R.33-1, PageID#161. Google used its hashing technology to scan the images and give them hash values. *Id.*, PageID#161–62. It coded the files as prepubescent minors engaged in sex acts. *Id.*, PageID#162; Rep., R.33-2, PageID#170–72. Lastly, Google scanned the two files from Miller's July 9 email to confirm that those files had the same hash values and were duplicates of the images that its employees had previously viewed. McGoff Decl., R.33-1, PageID#161–62.

*Jacobsen* requires us to apply the public-search doctrine if there is a "virtual certainty" that Schihl's viewing of the files would disclose the same images that Google's employees had already viewed. *Lichtenberger*, 786 F.3d at 488. At bottom, then, this case turns on the question whether Google's hash-value matching is sufficiently reliable. Yet the caselaw leaves unclear how we should go about answering that question. Should we treat it as a legal issue subject to de novo review because it is more like a "legislative fact" (to be decided uniformly) than an "adjudicative fact" (to be decided anew by hundreds of district judges)? *Cf. A Woman's Choice-East Side Women's Clinic v. Newman*, 305 F.3d 684, 688 (7th Cir. 2002); Kenneth C. Davis, *An Approach to Problems of Evidence in the Administrative Process*, 55 Harv. L. Rev. 364, 402–10 (1942). Or should we treat it as a fact issue subject to clear-error review because it turns on historical facts about a technology's reliability? *Cf. Glossip v. Gross*, 576 U.S. 863, 881 (2015). This clear-error standard might at least govern subsidiary questions. Google, for example, used its own proprietary technology in this case, and presumably a defendant may challenge a specific program's reliability even if a general technology is foolproof when performed properly. *Cf. Florida v. Harris*, 568 U.S. 237, 247–48 (2013).

We leave these questions for another day. Miller, who bore the burden of proof, never "challenge[d] the reliability of hashing" in the district court. *United States v. Miller*, 2017 WL 2705963, at *5 n.2 (E.D. Ky. June 23, 2017); *see Baker*, 976 F.3d at 645. The magistrate judge, whose findings the district court adopted, found that the technology was "highly reliable—akin to the reliability of DNA." *United States v.*

*Miller*, 2017 WL 9325815, at *10 (E.D. Ky. May 19, 2017). The evidence in one cited case suggested that "[t]he chance of two files coincidentally sharing the same hash value is 1 in 9,223,372,036,854,775,808." *United States v. Dunning*, 2015 WL 13736169, at *2 (E.D. Ky. Oct. 1, 2015) (citation omitted). (That is 1 in 9.2 *quintillion* in case you were wondering.) Another cited source suggested that the common algorithms "will generate numerical identifiers so distinctive that the chance that any two data sets will have the same one, no matter how similar they appear, is less than one in one billion." Barbara J. Rothstein et al., *Managing Discovery of Electronic Information: A Pocket Guide for Judges* 38 (2d ed. Federal Judicial Center 2012). Miller points us to no contrary sources. This (unchallenged) information satisfies *Jacobsen*'s virtual-certainty test and triggers its private-search doctrine.

New technologies can cut in both directions when courts attempt the difficult task of applying fixed rules to them. If a private party manually searched just one bankers box, the police likely would exceed the scope of that search under *Jacobsen* if they manually searched many other nearby boxes. *Compare United States v. Richards*, 301 F. App'x 480, 483 (6th Cir. 2008), *with United States v. Williams*, 354 F.3d 497, 510 (6th Cir. 2003). Because a computer can hold substantially more information than a box, we held in a related context, a private search of *some* computer files does not give the government license to search the *entire* computer. *Lichtenberger*, 786 F.3d at 488–89. We reasoned that the latter search would reveal much more information and be equivalent to the search of the many other unopened boxes. *Id.*; *see* Orin

S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 541–43 (2005).

Here, by contrast, the information on which the district court relied suggests that a computer's "virtual" search of a single file creates more certainty about the file's contents than a person's "manual" search of the file. Most people who view images do not use a magnifying glass to undertake a pixel-by-pixel inspection. Common hash algorithms, by contrast, catalogue every pixel. Johnson Tr., R.106, PageID#1290–91. Suppose a private party gets only a quick view of a picture before concluding that it is child pornography and handing the picture to the police. *Cf. Bowers*, 594 F.3d at 524. Under *Jacobsen*, that inspection would likely trigger the private-search doctrine and allow the police to reexamine the picture "more thoroughly," *Runyan*, 275 F.3d at 464, despite the "risk of a flaw in the [person's] recollection," *Jacobsen*, 466 U.S. at 119. What sense would it make to treat a more accurate search of a file differently?

In response, Miller compares a hash value to the "explicit descriptions" on the film boxes that *Walter* found insufficient to permit the FBI's viewing of the films. 447 U.S. at 652 (Stevens, J., opinion). Miller would have a point if Google forwarded the image files to Schihl based on their names alone: "young - tight fuck.jpg" and "!!!!!!Mom&son7.jpg." Rep., R.33-2, PageID#170. But the hash-value searches revealed much more information than those descriptions. Google's technology "opened" and "inspected" the files, revealing that they had the same content as files that Google had already found to be child pornography.

An amicus supporting Miller next points out that the Google employees who add files to its child-pornography repository might mistake a lawful image for an illegal one. Yet that is not a type of error that matters under the private-search doctrine. Just because a private party turns out to be wrong about the legality of an item that the party discloses to police does not mean that the police violate the Fourth Amendment when they reexamine the item. If, for example, the powder in *Jacobsen* had tested negative for cocaine, that result would not have transformed the DEA agent's reexamination of the box into a Fourth Amendment "search." *See* 466 U.S. at 123. Nor would the police conduct a Fourth Amendment "search" if the pictures that a private party provides turn out not to be "child pornography" under 18 U.S.C. § 2256. *See Bowers*, 594 F.3d at 526. And Google employees trained on this federal definition are much more likely to accurately identify child pornography than a person who comes across one disturbing image.

Does *Carpenter v. United States*, 138 S. Ct. 2206 (2018), change things? It held that an individual has "a legitimate expectation of privacy in the record of his physical movements as captured" by cell-site location information—even though this information is kept by (and disclosed to) a third-party wireless carrier. *Id.* at 2217. The Court reasoned that the tracking of a person's cellphone "achieves near perfect surveillance" of the person over the many years that the carrier retains the data. *Id.* at 2218. We fail to see how this holding can help Miller. *Carpenter* may well confirm our prior decision that individuals have a reasonable expectation of privacy in their emails—even though those emails (like the cellphone data) are kept by third parties. *See id.* at 2222 (citing *Warshak*, 631 F.3d at

283–88); *id.* at 2262–63, 2269 (Gorsuch, J., dissenting). But *Carpenter* asked only whether the government engaged in a "search" when it compelled a carrier to search its records for certain information that the government demanded. *Id.* at 2222. *Carpenter* did not cite *Jacobsen*, let alone address its private-search doctrine. Here, moreover, the government did not compel Google's hash-value matching (unlike the carrier's subpoena-induced search of cell-site records). And Miller has no legitimate expectation of privacy in illegal contraband like child pornography (unlike cell-site records). *Jacobsen*, 466 U.S. at 123. In short, we agree with *Reddick*'s conclusion that *Jacobsen* controls this case. 900 F.3d at 637–39.

2. Did Detective Schihl conduct a search under a "trespass" approach?

Perhaps *Jacobsen* should not control. The Supreme Court recently clarified that the invasion of a "reasonable expectation of privacy" is not the only way to define a Fourth Amendment "search." "For much of our history, Fourth Amendment search doctrine was 'tied to common-law trespass' and focused on whether the Government 'obtains information by physically intruding on a constitutionally protected area.'" *Carpenter*, 138 S. Ct. at 2213 (quoting *United States v. Jones*, 565 U.S. 400, 405, 406 n.3 (2012)). Unlike the defendant in *Reddick*, Miller asks us to find that Detective Schihl engaged in a search under this alternative theory.

*Jones* recently reinvigorated the trespass approach. There, the police attached a GPS device to the defendant's car and tracked the car's movements for weeks. 565 U.S. at 402–03. The government argued that no search occurred because the defendant had no

reasonable expectation of privacy in his movements on public roads. *Id.* at 406. The Court disagreed, holding that the installation of the GPS device qualified as a "search" because the government "physically occupied private property for the purpose of obtaining information." *Id.* at 404. According to the Court, the expectation-of-privacy test can *expand* the scope of areas protected by the Fourth Amendment, but it cannot *eliminate* protection for areas that the traditional "trespass" definition of a search would cover. *Id.* at 405–08; *see also Taylor*, 922 F.3d at 332–33.

How might *Jones*'s property-based approach apply here? An obvious analogy helps Miller at the outset. The Fourth Amendment protects not just intrusions into a person's "house," but also invasions of the person's "papers" and "effects." *See* U.S. Const. amend. IV. From before the founding, therefore, judges recognized that "[t]he protection of private property extended to letters, papers, and documents." Laura K. Donohue, *The Original Fourth Amendment*, 83 U. Chi. L. Rev. 1181, 1198 (2016). The famous English cases that drove the Fourth Amendment's adoption involved government trespasses to rummage through a person's letters and private documents. *See Entick v. Carrington*, 95 Eng. Rep. 807, 807–08, 817–18 (K.B. 1765); *Wilkes v. Wood*, 98 Eng. Rep. 489, 491, 498–99 (C.P. 1763). And there can be no better "analogy from principle to new technology" than from yesterday's mail to today's email. *Ackerman*, 831 F.3d at 1308. As our court has explained, "[e]mail is the technological scion of tangible mail, and it plays an indispensable part in the Information Age." *Warshak*, 631 F.3d at 286.

*Jones* thus leads us to consider how courts treated mailed items at the time of the founding or, perhaps

more importantly given Schihl's status as a state officer, at the time of the Fourteenth Amendment. This inquiry again helps Miller at first blush. In *Ex parte Jackson*, 96 U.S. 727 (1877), the Court noted that the right "against unreasonable searches and seizures extends to" "letters" and "sealed packages" "closed against inspection, wherever they may be." *Id.* at 733. A governmental opening of sealed mail required a warrant, confirming that this intrusion was a "search" under a historical understanding. *Id.* This conclusion comported with a long tradition. Before then, Thomas Cooley had opined that any "proposition to permit letters to be opened at the discretion of a ministerial officer, would be met with general indignation." Thomas M. Cooley, *A Treatise on the Constitutional Limitations Which Rest upon the Legislative Power of the States of the American Union* 306–07 n.2 (1868). And the first Congress had made it a crime for postal employees to "unlawfully" "open[] any letter, packet, bag or mail of letters[.]" Act of Feb. 20, 1792, § 16, 1 Stat. 232, 236. Here, moreover, the files in Miller's email might be analogized to "sealed" letters—such that Schihl's "opening" of the files could be characterized as a "trespass to chattels" and an illegal "search." *See Ackerman*, 831 F.3d at 1307–08. After all, "[o]utside of a few narrow exceptions," federal law prohibits providers from disclosing emails to third parties without the "consent of one of the communicating parties[.]" William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 Harv. L. Rev. 1821, 1875–76 (2016).

Yet Miller's reliance on *Jones*'s property-based approach encounters trouble when we consider *who* committed any trespass (and so any "search") in this case. The rule that the Fourth Amendment does not protect

against private searches precedes the expectation-of-privacy test applied in *Jacobsen* by decades, so the Court was using the earlier "common-law trespass" approach when it adopted this rule. *See Jones*, 565 U.S. at 405; *Burdeau*, 256 U.S. at 475. And the rule applied even when a private party committed a trespass. In *Burdeau*, for example, parties had illegally "blown open" the safes in which a suspect had kept his private letters and documents and given these papers to the government. 256 U.S. at 473–74. Although the Court suggested that this suspect had "an unquestionable right of redress against those who illegally and wrongfully took his private property," it found that the government's use of his papers did not violate the Fourth Amendment (with nary a suggestion that the government needed a warrant to view them). *Id.* at 475. Even *Jackson*, while acknowledging the need for a warrant, recognized that the government could obtain evidence about sealed mail in other ways, such "as from the parties receiving the letters or packages, or from agents depositing them in the post-office, or others cognizant of the facts." 96 U.S. at 735. Here then, if Google's hash-value matching is akin to a party "opening" a letter, Google might be the one that engaged in the trespass. And the government's later review of the already opened files might not be considered a search—or at least not an unreasonable one. *Cf. Morgan*, 903 F.3d at 571–72 (Thapar, J., concurring); Restatement (First) of Torts § 253 (Am. L. Inst. 1934).

At day's end, *Jacobsen* does not permit us to consider this subject further. If Detective Schihl's viewing of the files would qualify as a "search" under *Jones*'s trespass approach, the DEA agent's examination of

the box in that case would also qualify. The Tenth Circuit suggested that, after *Jones*, the Supreme Court might today "find that a 'search' *did* take place" in *Jacobsen*. *Ackerman*, 831 F.3d at 1307. But the fact remains that *Jacobsen* held that a search did *not* occur. 466 U.S. at 118–26. *Ackerman*'s facts were sufficiently far afield of *Jacobsen*'s that the Tenth Circuit found itself unbound by *Jacobsen*'s rule. 831 F.3d at 1307. Our facts, by contrast, are on all fours with *Jacobsen*'s (when updated for this new technology). *Reddick*, 900 F.3d at 637–39. No matter how this case should be resolved under a trespass approach, then, our instructions from the Supreme Court are clear: "[I]f a precedent of this Court has direct application in a case, yet appears to rest on reasons rejected in some other line of decisions, the Court of Appeals should follow the case which directly controls, leaving to this Court the prerogative of overruling its own decisions." *Agostini v. Felton*, 521 U.S. 203, 237 (1997) (citation omitted). We must follow *Jacobsen*'s legal rule here.

* * *

One last point. The Fourth Amendment does not just prohibit unreasonable "searches"; it also prohibits unreasonable "seizures." Miller raises no separate claim that Schihl engaged in an unreasonable "seizure" through his "assertion of dominion and control over" the digital files sent by Google. *Jacobsen*, 466 U.S. at 120. (Schihl presumably had a right to seize the files if his viewing of them did not violate the Fourth Amendment because police may confiscate items that "are evidence of a crime or contraband." *Soldal v. Cook County*, 506 U.S. 56, 68 (1992).) We thus need not consider how the Fourth Amendment's seizure rules should extend to digital information that "can be copied repeatedly, instantly, and freely,"

"zipped around the world in a split second," and "stored anywhere and without cost." Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1014 (2010).

## III. Sixth Amendment

Miller next argues that the district court violated the Sixth Amendment's Confrontation Clause by admitting NCMEC's CyberTipline Report into evidence. He may be correct that the admission of certain portions of this report violated the Confrontation Clause. But his claim fails because he challenges only automated portions that did not.

### A

The Confrontation Clause gives "the accused" in "all criminal prosecutions" the right "to be confronted with the witnesses against him[.]" U.S. Const. amend. VI. This clause prohibits the government from introducing some out-of-court statements by individuals who do not testify at trial and whom the defendant has not had the opportunity to "confront." *See Crawford v. Washington*, 541 U.S. 36, 50–54 (2004). Yet the clause does not bar the use of all such hearsay. Its text gives the defendant a right to cross-examine "witnesses," not "speakers." A "witness" is one who provides "[t]estimony," that is, "[a] solemn declaration or affirmation made for the purpose of establishing or proving some fact." *Id.* at 51 (quoting 2 Noah Webster, *An American Dictionary of the English Language* (1828)). The nature of an out-of-court statement thus determines whether the clause gives the defendant a right to cross-examine the person who made it. If an out-of-court statement is akin to "testimony," the clause prohibits the government's use of the statement unless the person who made it is unavailable to

testify and the defendant has had a prior opportunity for cross-examination. *See id.* at 52, 68. If an out-of-court statement is not akin to testimony, the clause falls to the side and leaves the statement's admissibility to the rules of evidence. *See Ohio v. Clark*, 576 U.S. 237, 244–45 (2015).

The constitutional dividing line between admissible and inadmissible hearsay thus turns on the difference between "testimonial" and "nontestimonial" statements. To distinguish between these two types of statements, the Supreme Court has adopted a "primary-purpose" test. *See Davis v. Washington*, 547 U.S. 813, 822 (2006). The Court has described this test in varying ways. It has sometimes noted that a statement made during an out-of-court conversation is testimonial when, "in light of all the circumstances, viewed objectively, the 'primary purpose' of the conversation was to 'creat[e] an out-of-court substitute for trial testimony.'" *Clark*, 576 U.S. at 245 (quoting *Michigan v. Bryant*, 562 U.S. 344, 358 (2011)). It has other times noted that an out-of-court statement is testimonial if it has "a 'primary purpose' of 'establish[ing] or prov[ing] past events potentially relevant to later criminal prosecution.'" *Bullcoming v. New Mexico*, 564 U.S. 647, 659 n.6 (2011) (quoting *Davis*, 547 U.S. at 822). Either way, the prime example of this sort of out-of-court testimony is a person's statement to the police about a crime during a formal interrogation. *See Crawford*, 541 U.S. at 53. Conversely, a person does not give "testimony" when, for example, the person calls 911 to request help during an emergency. *See Davis*, 547 U.S. at 827–29. The "primary purpose of [that] interrogation is to enable police assistance to meet an ongoing emergency," not to establish a prior fact or create trial evidence. *Id.* at 822.

This dividing line extends to statements made in reports. On the one hand, a formal report created for the purpose of proving a fact at trial is testimonial, and a defendant has the right to cross-examine the report's author. *See Bullcoming*, 564 U.S. at 657–58. Laboratory reports made for trial are good examples of these "testimonial" reports. In a drug-trafficking trial, the Supreme Court held that the government could not introduce an analyst's sworn report asserting that a substance connected to the defendant was cocaine. *See Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 309–11 (2009). And in a drunk-driving trial, the Court held that the government could not use an analyst's formal, signed certificate asserting that a blood-alcohol test showed the defendant's blood-alcohol level. *See Bullcoming*, 564 U.S. at 658–65.

On the other hand, a report written for a purpose unrelated to creating evidence or proving past events is generally nontestimonial. Business records are the best examples of these reports. Those records are generally admissible without cross-examination of their authors because they are "created for the administration of an entity's affairs and not for the purpose of establishing or proving some fact at trial[.]" *Id.* at 659 n.6 (quoting *Melendez-Diaz*, 557 U.S. at 324). Even some lab reports might fall on this nontestimonial side of things. *See Williams v. Illinois*, 567 U.S. 50, 58 (2012) (plurality opinion). In *Williams*, a fractured Supreme Court found nontestimonial a report that contained "a male DNA profile produced from semen taken from [the vaginal] swabs" of a rape victim. *Id.* at 59. A four-Justice plurality reasoned that the report was nontestimonial because its primary purpose was "to catch a dangerous rapist who was still at large," not to prove a fact for trial. *Id.* at 84. Justice

Thomas relied on a different rationale. He reasoned that this DNA report (unlike the reports in *Bullcoming* and *Melendez-Diaz*) was nontestimonial because it lacked sufficient solemnity. *Id.* at 111–12 (Thomas, J., concurring in the judgment). Although signed by reviewers, the report nowhere "attest[ed] that its statements accurately reflect[ed] the DNA testing processes used or the results obtained." *Id.* at 111.

B

Miller challenges the admission of the CyberTipline Report under these rules. Recall that this report had three sections with three "authors." In Section A, Google identified the date that the Gmail account uploaded the child-pornography files and the IP addresses used to access this account. Rep., R.33-2, PageID#169–71. Section A describes itself as an "Automatic Report," *id.*, PageID#169, and Miller does not dispute the government's claim that no Google employee manually entered information into this section. Lindsey Olson, the NCMEC director who oversees the CyberTipline program, added that NCMEC could not change anything in this section. Olson Tr., R.105, PageID#1088. In Section B, NCMEC's systems automatically recorded the results of an automated search for the location of the Google-provided IP addresses. Rep., R.33-2, PageID#172–73. This section listed Fort Mitchell as the location of the IP addresses, included the same longitude and latitude coordinates for both IP addresses, and identified Time Warner Cable as the internet service provider. *Id.* In Section C, an NCMEC analyst recorded the results of a manual search for public information connected to the Gmail account. *Id.*, PageID#173–77. The analyst also attached a printout of a profile page with a picture of

"Bill M" from the social-media website "Tagged." *Id.*, PageID#177.

Miller argues that the admission of this report violated the Confrontation Clause because it was testimonial and he did not have the opportunity to cross-examine the NCMEC analyst about the location information in Section B. Miller may well be correct that the NCMEC analyst's statements were testimonial, but he is wrong in concluding that this fact gave him a right to cross-examine the analyst about statements that the analyst did not make.

Start with the analyst's statements in Section C describing the results of the analyst's manual searches. Were they testimonial? It might depend on which of the Supreme Court's varied "primary-purpose" tests we apply. As noted, sometimes the Court has described a testimonial statement as one made with the general "purpose of establishing or proving some fact." *Melendez-Diaz*, 557 U.S. at 310 (quoting *Crawford*, 541 U.S. at 51). When the test is defined this way, Miller has good grounds to conclude that the analyst's statements qualify. The analyst knew that a child-pornography crime likely had been committed and was searching public information to establish the identity of the suspect who had used the incriminating Gmail account. When the analyst noted that this email was associated with a profile page on a social-media site, the analyst made that statement "for the purpose of establishing" that very fact—that this email address was connected to "Bill M." on "Tagged." *Id.* And, considered objectively, the analyst well knew that this information would be shared with investigating police. For essentially these reasons, the First Circuit held in a similar case that Yahoo reports sent to

NCMEC and NCMEC reports sent to police both are testimonial. *See Cameron*, 699 F.3d at 642–52.

Yet the Supreme Court has sometimes defined the primary-purpose test more narrowly. It has noted that a statement is testimonial if it is made with the specific "purpose of creating an out-of-court substitute for trial testimony." *Clark*, 576 U.S. at 250–51 (quoting *Bryant*, 562 U.S. at 358). The analyst's statements might not satisfy this narrower definition. In two ways, the statements also resemble the report containing a DNA profile that *Williams* found nontestimonial. The first way: Like the technicians in *Williams*, the analyst did not have a specific target in mind when undertaking the searches. *See* 567 U.S. at 84–85 (plurality opinion). So the analyst might have made the statements "not to accuse [Miller] or to create evidence for use at trial," but "to catch" the at-large person who had sent child pornography. *Id.* at 84. The second way: In terms of their solemnity, the analyst's statements are more like the informal report in *Williams* than the sworn statements in *Melendez-Diaz* or the signed certificate in *Bullcoming*. The analyst did not sign the report or certify its accuracy. Rep., R.33-2, PageID#174–77. And the report disclaims its trustworthiness, noting that the "CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report." *Id.*, PageID#174. Justice Thomas's separate interpretation thus might also suggest that the statements are nontestimonial. *See Williams*, 567 U.S. at 111–12 (Thomas, J., concurring in the judgment).

All of this shows that the Supreme Court may one day need to clarify its primary-purpose test. Ulti-

mately, however, we need not resolve how this test applies to the NCMEC analyst's *own* statements. That is because Miller raises no objection to his inability to cross-examine the analyst about the statements in Section C. Rather, Miller objects that he could not cross-examine the analyst about the information identifying the location of the Google-provided IP addresses in Section B. Miller's claim that he had a right to confront the analyst about Section B's information contains both a factual error and a legal one. Factually, the NCMEC analyst was not the "speaker" who made the statements in Section B. As Olson testified, NCMEC's systems automatically generated this information once NCMEC received the report. Olson Tr., R.95, PageID#541–42.

Legally, the admissibility of this information turns on the rules of evidence, not the Confrontation Clause. The clause limits its reach to "witnesses." U.S. Const. amend. VI. The word "witness" has a common meaning covering "[o]ne" (i.e., a person) "who gives testimony." Webster, *supra*, *American Dictionary*; *see* 2 T.E. Tomlins, *The Law Dictionary* 986 (1810). The backdrop against which the clause was enacted also confirms that it existed to prevent the use of a *person*'s out-of-court statements to convict the defendant. *Crawford*, 541 U.S. at 43–50. This text and history show that the clause encompasses statements by people, not information by machines. A computer system that generates data and inputs the data into a report cannot be described as a "witness" that gives "testimony." If the system were the witness, how would the government make it available for cross-examination? Would it have to be asked questions in computer code?

Unsurprisingly, courts have agreed that the Confrontation Clause does not apply to information generated by machines. *See United States v. Summers*, 666 F.3d 192, 202–03 (4th Cir. 2011); *United States v. Lamons*, 532 F.3d 1251, 1263–65 (11th Cir. 2008); *United States v. Moon*, 512 F.3d 359, 362 (7th Cir. 2008). Relatedly, they have recognized that machine-generated information does not qualify as "hearsay" under the rules of evidence because the information is not a statement by a person. *See* Fed. R. Evid. 801(a)–(c); *see, e.g.*, *United States v. Channon*, 881 F.3d 806, 810–11 (10th Cir. 2018); *United States v. Lizarraga-Tirado*, 789 F.3d 1107, 1109–10 (9th Cir. 2015). This precedent extends to the data produced by NCMEC's systems.

Perhaps Miller could respond that the computer coder who developed the program that performs these functions should be subject to cross-examination about the program's reliability. *Bullcoming*, for example, rejected the argument that the "machine" performing the blood-alcohol test was the "speaker" when the analyst himself stated that he had performed the test on the machine and described the results. *See* 564 U.S. at 659–61. And the Eighth Circuit has noted that "[m]achine-generated records . . . can become hearsay when developed with human input." *United States v. Juhic*, 954 F.3d 1084, 1089 (8th Cir. 2020). But neither *Bullcoming* nor *Melendez-Diaz* can be extended as far as Miller needs. Both cases held only that an analyst who used a machine to perform a test and who made statements about the results must be subject to cross-examination over the statements. *Melendez-Diaz* disclaimed any broader notion that the Confrontation Clause reached everyone "whose testimony may be relevant in establishing the . . . accuracy of the

testing device" used in a case. 557 U.S. at 311 n.1. And *Bullcoming* nowhere suggested that the clause gave the defendant the right to cross-examine the creator of the "gas chromatograph machine" (the machine that tested the blood-alcohol level). 564 U.S. at 654.

The same logic applies here. The Confrontation Clause does not give Miller a right to cross-examine the individuals who created NCMEC's systems. And Miller identifies no other individuals like the analysts in *Bullcoming* and *Melendez-Diaz* who performed specific tests and made statements about their results. Here, the systems automatically performed the "search" (or "test") for the location of the IP addresses. And they automatically recorded the results (or "statements") in Section B. This case involved no "human input" because the NCMEC analyst undertook neither the search nor the recording. *Juhic*, 954 F.3d at 1089. Miller thus had no Confrontation Clause right to cross-examine the analyst about the information in Section B.

C

In response, Miller does not challenge the legal point that data from computers are not "testimony" from "witnesses." Rather, he challenges the factual point that NCMEC's systems automatically imported the location information into Section B. According to Miller, the record leaves "entirely unclear" whether the NCMEC analyst helped. Not so. As Miller's support, he cites Olson's background testimony that when NCMEC receives a report, "the analysts may add additional value to" it and "may review the information that's been provided and try to locate or provide a location." Olson Tr., R.105, PageID#1080. Yet Olson clarified that the analysts historically had to search

for the geographic area of IP addresses, but that Section B was "basically automating" "a lot of those things that [analysts] used to do" manually. *Id.*, PageID#1092. She went on: "[T]he system is able to take the IP address, [and] use publicly available tools to geo locate the IP address." *Id.*, PageID#1093. Another NCMEC witness at an earlier stage of the case confirmed that "NCMEC systems performed a publicly-available WhoIs lookup related to the [two] IP addresses reported by Google." Shehan Decl., R.33-6, PageID#196. Section B itself shows that it contained automated information. The report's table of contents describes "Section B" as "Automated Information Added by NCMEC Systems." Rep., R.33-2, PageID#168, 172. Section B then notes: "The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems." *Id.*, PageID#172. The record is clear: NCMEC's systems automatically produced the information about which Miller complains.

That this information was automated dooms Miller's reliance on the First Circuit's decision in *Cameron*. As noted, *Cameron* held that statements in reports that Yahoo provided to NCMEC and that NCMEC provided to the police were testimonial. 699 F.3d at 642–52. But *Cameron* made clear that the Yahoo reports "were made by a *person* with knowledge of their contents"; they were not made by a computer system. *Id.* at 642 (emphasis added). And *Cameron* made clear that an "NCMEC employee" had prepared the CyberTipline Reports at issue. *Id.* at 651.

That this information was automated also dooms Miller's claimed prejudice from the lack of cross-examination. He argues that he was harmed by his inability to cross-examine the analyst about the information

in Section B because some of this information may have been exculpatory. Specifically, Miller's counsel used the identified longitude and latitude coordinates to do his own manual "geolocation," and counsel's research allegedly revealed that the coordinates pinpointed to a location other than Miller's home. Appellant Br. 26 & Ex. A. Miller argues that the analyst's failure to testify barred him from engaging in any inquiry on this critical subject. Yet again, the analyst did not input these coordinates into Section B, so Miller had no Confrontation Clause right to cross-examine the analyst about statements the analyst did not make. And nothing prevented Miller from cross-examining NCMEC's director (Olson) about the accuracy of its systems or how those systems chose these coordinates. The district court indicated that it would have allowed Miller's counsel to pursue this line of questioning with Olson. Tr., R.97, PageID#902.

Miller's counsel decided against this cross-examination not because the analyst failed to testify but for a strategic reason: Olson did not mention the coordinates or suggest that they identified Miller's home. *Id.* Yet the government unfairly undermined this strategy, Miller rightly notes, when its counsel argued during closing that the longitude and latitude coordinates had been "[t]he defendant's house." *Id.*, PageID#891. The government concedes that this statement had no basis in evidence. But the Confrontation Clause does not regulate an improper closing argument. That is the domain of the Due Process Clause (or our general supervisory powers). *See Donnelly v. DeChristoforo*, 416 U.S. 637, 642–45 (1974). And Miller asserted no due-process or prosecutorial-misconduct challenge to the government's argument until his reply brief. That

came too late. *See Island Creek Coal Co. v. Wilkerson*, 910 F.3d 254, 256 (6th Cir. 2018).

## IV. Sufficiency of the Evidence

Miller ends with the claim that the government presented insufficient evidence to convict him. To succeed on this claim, Miller must show that no "rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *United States v. Potter*, 927 F.3d 446, 453 (6th Cir. 2019) (citation omitted). Miller does not dispute that a rational jury could have found that *someone* committed the essential elements of the charged child-pornography offenses beyond a reasonable doubt. He asserts only that no rational jury could have found that *he* committed those offenses given the other evidence implicating his brother—Fred Miller.

This argument misunderstands our standard of review. We readily agree that Miller presented *some* evidence pointing to his brother Fred. A few emails sent to the Gmail account, for example, were addressed to Fred about a cellphone rebate, and Fred visited Miller's home once a week or so. But simply because another jury might have harbored doubt based on this evidence does not allow us to overturn the jury's verdict that Miller was the guilty party. On a sufficiency-of-the-evidence challenge, we consider only whether "the government's case was so lacking that it should not have even been submitted to the jury." *Musacchio v. United States*, 136 S. Ct. 709, 715 (2016) (citation omitted). That "limited review" bars us from reweighing the evidence or deciding for ourselves whether Miller or the government put on the more convincing case. *United States v. Maya*, 966 F.3d 493, 499 (6th Cir. 2020) (quoting *Musacchio*, 136 S. Ct. at 715). We

ask merely whether Miller's jury behaved irrationally in concluding beyond a reasonable doubt that he rather than Fred committed these crimes, drawing all reasonable inferences in the government's favor. *See United States v. Braswell*, 704 F. App'x 528, 539–40 (6th Cir. 2017).

The government more than met its burden under these rules. Substantial evidence pointed to Miller rather than Fred as the person who committed the child-pornography offenses. Consider the emails. Google's records listed the subscriber for the Gmail account as "Bill Miller." Many emails and messages sent from this account also propositioned women using the same story. A person named "Bill" would, among other things, allege that his wife "Tania" had died (Tania is the name of Miller's wife), and would send personal photos of Miller (not his brother). This account was also connected to a "Tagged" social-media profile that included Miller's picture. And the IP address for the July 9 email matched a Time Warner Cable subscription from Miller's house, not Fred's.

Next consider the external hard drive with the child-pornography files. It was found at Miller's house, not Fred's. In an interview with Detective Schihl, Miller admitted that he owned the hard drive and that it contained child pornography (although he claimed that it had been on the drive when he bought it a year earlier). That hard drive, which had child pornography neatly catalogued in file folders with names like "incest" or "pre-teen," contained a file folder named "me" with pictures of Miller. And it had Skype messages asking for child pornography using the display name "Bill Miller." A forensic examination also revealed that the child-pornography folders were

created on the hard drive just a week before the July 9 email, not a year before as Miller had claimed.

Against this evidence, Miller cites *United States v. Lowe*, 795 F.3d 519 (6th Cir. 2015). There, the government learned that an IP address at the home of the defendant, James Lowe, was sharing child pornography over a peer-to-peer network. *Id.* at 520. Lowe lived at this home with his wife and an adopted child. *Id.* The police searched the home and found a laptop that contained substantial child pornography. *Id.* at 521. After a jury convicted Lowe of various child-pornography offenses, we held that the evidence was insufficient to prove that Lowe had knowingly downloaded the child-pornography onto the laptop. *Id.* at 523. We relied on the fact that Lowe "shared his home with two other people, both of whom could access" the laptop and the peer-to-peer file-sharing program without entering passwords. *Id.* Critically, no circumstantial evidence—for example, the laptop's browser history—suggested that it was Lowe rather than the others who had used this laptop to download child pornography. *Id.* at 523–24.

"Simply put, this case is not at all like . . . *Lowe*." *United States v. Niggemann*, 881 F.3d 976, 981 (7th Cir. 2018). The circumstantial evidence here, unlike the circumstantial evidence there, sufficed for a rational jury to exclude Fred beyond a reasonable doubt. *See United States v. Clingman*, 521 F. App'x 386, 395–96 (6th Cir. 2013). In other cases rejecting sufficiency challenges like Miller's, courts have pointed to such circumstantial evidence as the fact that the incriminating account (like the Gmail account) was registered to the defendant. *See Niggemann*, 881 F.3d at 980. These cases have also pointed to the fact that a

profile page of a relevant account included the defendant's picture (like the "Tagged" account) or the fact that the emails sent from a relevant account included "identifying photographs" and used the defendant's name (like many of the emails from the Gmail account). *See United States v. Woerner*, 709 F.3d 527, 536–37 (5th Cir. 2013); *see also United States v. Farnum*, 811 F. App'x 18, 20 (2d Cir. 2020) (order). And these cases have pointed to the defendant's own statements that he possessed the child pornography (like the statements that Miller made to Detective Schihl). *Woerner*, 709 F.3d at 537.

We affirm.

**APPENDIX B**

**UNITED STATES DISTRICT COURT**
**EASTERN DISTRICT OF KENTUCKY**
**NORTHER DIVISION**
**AT COVINGTON**

**CRIMINAL ACTION NO. 16-47-DLB-CJS**

**UNITED STATES OF AMERICA PLAINTIFF**

**vs. MEMORANDUM ORDER ADOPTING REPORT AND RECOMMENDATION**

**WILLIAM MILLER DEFENDANT**

* * * * * * * * * * * * * *

## I. Introduction

This matter concerns the role of electronic service providers (ESPs) in identifying and reporting images of child pornography sent using their services and the constitutionality of law enforcement's subsequent review of those images. Defendant's Motion to Suppress two images of apparent child pornography attached to an email in his Google account is before the Court on the Report and Recommendation (R&R) of Magistrate Judge Candace J. Smith, who recommends that the Court deny the Motion. (Doc. # 41). Defendant has filed objections to the R&R (Doc. # 44), and the R&R and objections are now ripe for the Court's review. For the reasons that follow, the objections are **overruled**, and the motion to suppress is **denied**.

## II. Factual Background

On July 9, 2015, someone using the Google email (Gmail) account miller694u@gmail.com uploaded two images as attachments to an email. (Doc. # 33-2 at 3-

4). Google's product abuse detection system recognized those images as apparent child pornography using its proprietary "hashing" technology. (Doc. # 33-1 at ¶¶ 4-8, 10-13). Hashing is "the process of taking an input data string [from an electronic image, for example] and using a mathematical function to generate a (usually smaller) output string." Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38, 38-39 (2005). The output string, called the hash value, is a "digital fingerprint" shared by any duplicate of the input data string. (Doc. # 33-1 at ¶ 4). Hashing is not unique to images of child pornography–the process can be used to derive hash values for many different kinds of data sets, "including the contents of a DVD, USB drive, or an entire hard drive." Salgado, *supra*, at 39. Importantly, hash values are uniquely associated with the input data, meaning that "if an unknown file has a hash value identical to that of another known file, then you know that the first file is the same as the second." *Id.* at 39-40; *see also* Doc. # 33-1 at ¶ 4.

Google has been using its proprietary hashing technology since 2008 to identify "confirmed child sexual abuse images." (Doc. # 33-1 at ¶¶ 4-8). After an image of child sexual abuse is viewed "by at least one Google employee," the image "is given a digital fingerprint ('hash')" and is "added to [Google's] repository of hashes of apparent child pornography as defined in 18 U.S.C. § 2256." *Id.* at ¶ 4. Although the company also receives tips from users who "flag suspicious content," Google confirms that "[n]o hash is added to [its] repository without the corresponding image first having been visually confirmed by a Google employee to be apparent child pornography." *Id.* at ¶ 5.

When Google "encounters a hash that matches a hash of a known child sexual abuse image," it does one of two things. *Id.* at ¶ 5. In some cases, Google does not view the image again, but instead automatically reports the user to the National Center for Missing and Exploited Children (NCMEC), a non-profit organization authorized by Congress to "operate a cyber tipline to provide [ESPs] an effective means of reporting . . . child pornography." *Id.*; 42 U.S.C. § 5773(b)(1)(P). "In other cases, Google undertakes a manual, human review, to confirm that the image contains apparent child pornography before reporting it to NCMEC." *Id.* Google is required by law to report apparent child pornography to NCMEC through the CyberTipline when it becomes aware of it. 18 U.S.C. § 2258A.

In this case, when Google's product abuse detection system identified two images in miller694u@gmail.com's email account as having hash values matching hash values contained in Google's repository of apparent child pornography, Google "submitted an 'automatic report' to NCMEC" in compliance with its reporting obligations. (Doc. # 41 at 2 n.2). A Google employee did not re-view the images or the content of the email before submitting the report to NCMEC. (Doc. # 33-1 at ¶ 11). However, Google did provide NCMEC with "the email address used, the IP address associated with the email in question, classification of the images ['A1' under the industry classification system, meaning the image contained a depiction of a prepubescent minor engaged in a sexual act], the file names listed with the images and the two uploaded image files." (Doc. # 41 at 3).

Upon receiving the images, NCMEC's staff "did not open or view the two uploaded files contained in the report." *Id.* Instead, NCMEC "located publicly

available social network profiles" associated with the email account, verified the IP address reported by Google, and learned it to be associated with a Time Warner Cable account having a potential geographic location of Fort Mitchell, Kentucky." *Id.* That information was sent to the Kentucky State Police and the Kenton County Police Department. *Id.*

Detective Aaron Schihl of the KCPD received NCMEC's CyberTipline report on August 13, 2015. *Id.* at 4. "Detective Schihl opened the attachments and viewed the images, which he confirmed to be child pornography." *Id.* He sought a grand jury subpoena for the subscriber information for the Time Warner account and then sought and obtained a search warrant for the contents of the miller694u@gmail.com account. *Id.* Detective Schihl then obtained search warrants for Defendant's home and the electronic devices seized from his home, which yielded additional evidence of "receipt, possession, and distribution of child pornography." *Id.*

Now, Defendant seeks to suppress all evidence obtained by Detective Schihl, arguing that both Google's initial search and Detective Schihl's subsequent search violated the Fourth Amendment. In her R&R, Magistrate Judge Smith concluded that Google's initial review of the files did not implicate the Fourth Amendment because Google is a private actor, not a government agent. She also concluded that Detective Schihl's actions in viewing the images did not implicate the Fourth Amendment because his actions did not exceed the scope of the prior private search by Google.

In his objections, which the Court reviews *de novo*, Defendant makes three specific arguments. First, he

argues that Google is a government actor because of its "close relationship and collaborative crime fighting efforts" with NCMEC, which the R&R assumes without deciding is a government actor. (Doc. # 44 at 2). As a result, Defendant argues, the fruits of Google's warrantless search should be suppressed. Second, Defendant argues that, even if Google is not a government actor, Detective Schihl's subsequent review of the images exceeded Google's private search, meaning that the detective violated the Fourth Amendment because Defendant had a reasonable interest in the privacy of his email attachments. Finally, Defendant argues that Detective Schihl's actions were a search pursuant to traditional trespass doctrine because the email attachments were sealed virtual containers.

For the reasons set forth herein, the Court finds that Defendant's arguments are unavailing, **overrules** his objections, and **adopts** Magistrate Judge Smith's R&R as the Opinion of the Court.

## III.Analysis

### A. Google is not a government actor.

Defendant's first objection is to Magistrate Judge Smith's conclusion that Google is not a government actor. (Doc. # 44 at 2-4). Whether Google is a government actor is significant because the Fourth Amendment protects individuals from "unreasonable searches and seizures" by the government, not private entities. U.S. Const. amend. IV. Indeed, the Fourth Amendment "is wholly inapplicable" to searches and seizures by "a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official." *United States v. Jacobsen*, 466 U.S. 109, 113-14 (1984) (internal quotation marks omitted).

The Sixth Circuit uses a two-part test to determine whether a private entity is a government agent for the purposes of the Fourth Amendment. "In the context of a search, the defendant must demonstrate two facts: (1) Law enforcement 'instigated, encouraged or participated in the search' and (2) the individual 'engaged in the search with the intent of assisting the police in their investigative efforts.'" *United States v. Hardin*, 539 F.3d 404, 419 (6th Cir. 2008) (quoting *United States v. Lambert*, 771 F.2d 83, 89 (6th Cir. 1985)). If the defendant cannot show both of these facts, the private actor is not a government agent. Here, Magistrate Judge Smith correctly concluded that Google is not a government agent when it voluntarily scans email attachments for apparent child pornography and sends reports to NCMEC.

The Sixth Circuit has not yet determined whether NCMEC itself is a government agent. (Doc. # 41 at 6). The Tenth Circuit recently concluded that it is, which means that NCMEC's actions implicate the Fourth Amendment to the extent they constitute "searches" or "seizures." *United States v. Ackerman*, 831 F.2d 1292, 1294-1304 (10th Cir. 2016 (Gorsuch, J.) (concluding that NCMEC is a government entity and a government agent). Magistrate Judge Smith assumed without deciding that NCMEC acted as a government agent in this case (Doc. # 41 at 6), and the Court sees no reason to disturb that assumption. However, that assumption does not extend to ESPs (like Google) that voluntarily scan emails for child pornography and report apparent child pornography to NCMEC.[1] In fact,

[1] In *Ackerman*, the Tenth Circuit concluded that NCMEC exceeded the scope of the ESP's search in any event, so the status of the ESP was not at issue in that case. *Ackerman*, 831 F.2d at 1306-07.

every court to have addressed the question (including the First, Fourth, and Eighth Circuits) has determined that, in situations like this one, the ESP is not a government agent. (Doc. # 41 at 6-8 (collecting cases)).

Defendant argues that Google's "close and collaborative relationship" with NCMEC, a government agent, makes Google a government agent too. (Doc. # 44 at 2-3). According to Defendant, a statutory scheme that involves "mandatory reporting requirements and penalties for failure to report" and a "requirement to preserve evidence" ties Google to NCMEC and makes it a government agent for purposes of the Fourth Amendment. (Doc. # 41 at 2); 18 U.S.C. §§ 2258A(a), (e), (f).

The statutory reporting requirements are not sufficient to transform Google into a government agent under this test. The Supreme Court's leading Fourth Amendment agency case, *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602 (1989), held that a regulatory scheme evidenced the government's "encouragement, endorsement, and participation" of a search when it "removed all legal barriers" for breath, blood, and urine testing of railroad operators, "mandated that the railroads not bargain away the authority to perform [such] tests," required employers to remove employees who refused to submit to the tests from service, and conferred the right to receive the results of the test on the government. *Skinner*, 489 U.S. at 615-16. The Court held that the regulatory scheme rendered otherwise private railroads agents of the government because it belied the idea that "tests conducted by private railroads . . . will be primarily the result of private initiative." *Id.*

Here, by contrast, there is ample evidence that Google's scanning is still the result of its private initiative, not government pressure. Unlike the regulations at issue in *Skinner*, the statutory scheme for reporting child pornography does not purport to authorize or remove "legal barriers" to ESP email scanning, or "prescribe consequences for [an ESP's] users should they refuse to submit" to the scanning. *United States v. Stevenson*, 727 F.3d 826, 829-30 (8th Cir. 2013). In fact, the statute explicitly disclaims a scanning or monitoring requirement, 18 U.S.C. § 2258A(f), and mandates only reporting of apparent images of child pornography that the ESPs are aware of, § 2258A(a). The penalties for failure to report do not compel ESPs to monitor their subscribers as a practical matter, either–in fact, "the converse is just as likely to be true," because ESPs "might just as well take steps to avoid discovering reportable information" to avoid penalties for failure to report. *United States v. Richardson*, 607 F.3d 357, 367 (4th Cir. 2010). Unlike the regulatory scheme at issue in *Skinner*, nothing prevents the ESPs from doing just that, and there is no evidence that NCMEC imposes obligations on Google that the statutory scheme does not. As a result, the statutory reporting requirements do not transform Google into a government agent.

Defendant also argues that Google and NCMEC's collaborative relationship "supports a finding that NCMEC has intimate knowledge of Google's searching activities, and encourages them." (Doc. # 44 at 3). Defendant explains that Google and NCMEC share hash values (though he acknowledges that they did not do so in this case, *id.* at 3 n.3), that NCMEC gives Google awards for its collaboration, and that Google makes public statements about its collaboration with

and support for NCMEC. *Id.* at 3. But acknowledgment of Google's voluntary activities is not the same as government participation in or encouragement of the search activities themselves. Whether Google has made itself a "willful participant" (Doc. # 27 at 6) in NCMEC's child-protective policies is not dispositive where, as here, Defendant has not met the second prong of the test–that Google's intention in searching is to provide the government with evidence for its criminal investigations.

Defendant failed to show that Google monitors image attachments for apparent child pornography with the intent of assisting police investigative efforts. Instead, Google presented evidence that it scans email attachments and uses its proprietary hashing technology for its own business purposes. Google explains that it "independently and voluntarily take[s] steps to monitor and safeguard [its] platform" because if it "is associated with being a haven for abusive content and conduct, users will stop using [Google's] services." (Doc. # 33-1 at ¶ 3). In particular, "[r]idding [its] products and services of child abuse images is critically important to protecting [Google's] users, product, brand, and business interests." *Id.*

Other than reflecting a general societal consensus that images of child pornography are harmful, Google's business interests are "entirely independent of the government's intent to collect evidence for use in a criminal prosecution." *United States v. Bowers*, 594 F.3d 522, 526 (6th Cir. 2010) (internal quotation marks omitted). Even without a statutory obligation to report its findings to NCMEC, it seems likely that Google would screen its platform for images of child pornography because doing so is good business practice.

For all those reasons, the Court agrees with Magistrate Judge Smith that the evidence does not compel a finding that the government participates in Google's activities to such a degree that Google's search is the government's search. Defendant's objection is **overruled**.

### B. Detective Schihl's actions did not exceed Google's private search.

Because Google's actions are not attributable to the government, Detective Schihl's subsequent review of the images will not violate the Fourth Amendment if that review does not exceed the scope of the prior private search. *Jacobsen*, 466 U.S. at 115. "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." *United States v. Lichtenberger*, 786 F.3d 478, 485-86 (6th Cir. 2015) (citing *Jacobsen*, 466 U.S. at 119-20). With respect to child pornography, the Sixth Circuit has held a government search permissible on the grounds that "the officers in question had near-certainty regarding what they would find and little chance to see much other than contraband," "learned nothing that had not previously been learned during the private search," and "infringed no legitimate expectation of privacy." *Id.* (internal quotation marks omitted).

**1. This case is not like *Walter* because the images have been previously viewed by Google and the hash value is not a mere label.**

Defendant's core objection is that Detective Schihl's actions are broader in scope and different in type from the actions taken by Google because Detective Schihl opened Defendant's email attachments to view the images, while Google merely looked at the hash values. (Doc. # 44 at 6). That distinction, Defendant argues, makes *Walter v. United States*, 447 U.S. 649 (1980) the proper analog to this case, and Defendant cites *United States v. Keith*, 980 F. Supp. 2d 33 (D. Mass. 2013), in support.

The Court disagrees. Defendant's argument is based on two flawed premises contradicted by the evidence and case law. The first flawed premise is that the images attached to his emails are akin to a sealed container that has never been opened. The second flawed premise is that the hash values associated with those images are analogous to the labels in *Walter*.

In *Walter*, the Supreme Court found a Fourth Amendment violation where private individuals mistakenly received shipments of films in boxes with labels that alluded to the obscene content of the films. *Walter*, 447 U.S. at 651. One individual held the film up to the light, but could not see anything. *Id.* at 652. None of the private individuals watched the films. *Id.* Instead, they called the FBI, who watched the films without a warrant. *Id.* Two justices wrote that watching the film exceeded the scope of the prior search, two justices concurred in the result but wrote that watching the film would exceed the scope of the

prior search even if the private individuals had held their own private screening because the private screening would not have exposed the film to plain view, and one justice concurred in the judgment without discussion. *Walter*, 447 U.S. at 658-62. Even the dissenting justices agreed that "[t]he additional invasions of respondents' privacy by the Government agent must be tested by the degree to which they exceeded the scope of the private search." *Jacobsen*, 466 U.S. at 115.

Defendant's argument that the images in this case are akin to the films in *Walter* that were not viewed in the private search is inconsistent with the evidence. Google's practice is to register hash values for images that Google has already physically viewed. (Doc. # 33-1 at ¶¶ 4-5). There is no evidence that Google departed from that practice in this case (and Defendant has abandoned his argument to the contrary (Doc. # 44 at 2 n.1)). After viewing the images at issue here, Google used its hashing technology and included the hash value in its registry. When Defendant attached the images to his email, Google noted a match in the hash values, conveyed that information to NCMEC, and NCMEC passed the information and the images along to Detective Schihl. (Doc. # 33-1 at ¶¶ 11). The argument that Detective Schihl, like the FBI agents in *Walter*, viewed the images when the private searchers did not is therefore not supported by the facts.[2]

---

[2] To the extent that Defendant's argument relies on a distinction between the file previously viewed by Google and the file Defendant attached to his email, that is a distinction without a difference. The two files were matched by hash values—a digital fingerprint. (Doc. # 33-1 at ¶ 4). Defendant does not challenge

Contrary to Defendant's suggestion, the hash value is not a label like what was written on the boxes in *Walter*. A hash value, unlike a label, has no inherent meaning–it gains meaning only when it matches with a hash value in the child pornography repository and therefore reminds Google that it has seen this image before. Indeed, a closer analog to the *Walter* case would be if Google had flagged the images in Defendant's email as apparent child pornography *merely because of their file names*, without having ever looked at the images to verify their content. If that were the situation, Detective Schihl's subsequent examination of the files would present a different, and much more difficult, question of scope.

For the same reasons outlined above, the Court departs from the district court's analysis in *United States v. Keith*, 980 F. Supp. 2d 33 (D. Mass. 2013). That court found that "matching the hash value of a file to a stored hash value is not the virtual equivalent of viewing the contents of the file." *Id.* at 43. "What the match says is that the two files are identical; it does not itself convey any information about the contents of the file. It does say that the suspect file is identical to a file that someone, sometime, identified as containing child pornography, *but the provenance of that designation is unknown*." *Id.* (emphasis added). Based on the evidence before the *Keith* Court, it was not clear *who* performed the initial private search—the court noted it was "possible that the hash value of a suspect file was initially generated by another provider and then shared with AOL." *Id.* at 37 n.2. The court also concluded from

---

the reliability of hashing, and as the R&R notes, "it appears well established that it is, in fact, reliable." (*See* Doc. # 41 at 21).

testimony at the evidentiary hearing that it is "indisputable that AOL forwarded the suspect file only because its hash value matched a stored hash value, not because some AOL employee had opened the file and viewed the contents." *Id.* at 42- 43; *see also id.* at 37 ("[n]othing is known about how the file came to be originally hashed and added to the flat file database, except that it was AOL's practice to hash and add to the database either the hash value of any file that was identified by one of its graphic file analysts as containing child pornography or a hash value similarly generated by a different ESP or ISP and shared with AOL").

Here, by contrast, the evidence indicates that Google itself had already viewed the images and identified them as apparent child pornography to Detective Schihl before he ever conducted his search. (*See* Doc. # 33-1 at ¶¶ 4-5 ("[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")). Defendant's efforts to analogize this case with searches violative of the Fourth Amendment in *Walter* and *Keith* fail because this case is distinguishable on a key point—the evidence shows that Google previously viewed the images at issue and tagged them as apparent child pornography.

Detective Schihl also avoids the pitfall the Tenth Circuit identified in *Ackerman*, where NCMEC (acting as a government agent) viewed images that the ESP had not even hashed. As Magistrate Judge Smith explains, in *Ackerman*, AOL's email filter identified one image out of four attachments to an email that matched the hash value of an image AOL had previously deemed to be child pornography.

*Ackerman*, 831 F.3d at 1294. Like Google did here, AOL sent a report to NCMEC. *Id.* But unlike here, NCMEC viewed more than just the image matching AOL's hash values—it also viewed the contents of the email and the other three attachments, which AOL had never examined. *Id*. The *Ackerman* Court determined that by "opening the email itself" and the three additional attachments, NCMEC "exceeded rather than repeated" AOL's private search. *Id.* at 1306. The Tenth Circuit did not need to address the constitutionality of the situation presented here, where the government looks only at the material that had previously been examined. *Id.* at 1306.

**2. *Jacobsen* and *Bowers* support the conclusion that Detective Schihl's search did not exceed the scope of Google's.**

Contrary to Defendant's argument, the scope of Detective Schihl's search in this case is more like the narrowly drawn searches that the Supreme Court and Sixth Circuit upheld in *Jacobsen* and *Bowers*. *Jacobsen*, the case that marks the origin of the private search doctrine, began with FedEx employees examining the contents of a damaged package. *Jacobsen*, 466 U.S. at 111. Inside the cardboard container, they discovered a ten-inch tube made of duct tape which, when the employees cut it open, revealed four plastic bags filled with white powder. *Id.* FedEx called the DEA and put the tube and its contents back in the box. *Id.* The DEA agent inspected the partially open container, removed the plastic bags, and field-tested them for cocaine. *Id.* at 112. The Supreme Court held that the DEA agent's inspection of the plastic bags and testing of the powder remained within the scope of FedEx's prior search because

"there was a virtual certainty that nothing else of significance was in the package and that a manual inspection of the tube and its contents would not tell him anything more than he had already been told." *Id.* at 119. Moreover, the field test "could disclose only one fact previously unknown to the agent—whether or not a suspicious white powder was cocaine"—a fact in which the defendant had no legitimate expectation of privacy. *Id.* at 122-24.

The Sixth Circuit applied the logic of *Jacobsen*'s private search doctrine to depictions of child pornography in *Bowers*. *Bowers*, 594 F.3d at 526. In that case, a private search by the defendant's housemate uncovered a physical photo album that contained child pornography. *Bowers*, 594 F. 3d at 524. The housemate alerted the FBI, who later looked at the same photo album and confirmed that it likely contained child pornography. *Id*. The Sixth Circuit held that the FBI's actions did not exceed the scope of the housemate's private search and affirmed the denial of the motion to suppress because "the agents 'learn[ed] nothing that had not previously been learned during the private search' and 'infringed no legitimate expectation of privacy.'" *Id.* at 526 (quoting *Jacobsen*, 466 U.S. at 119-20). *See also United States v. Richards*, 301 F. App'x 480, 483 (6th Cir. 2008) (the "government's confirmation of prior knowledge learned by the private individuals does not constitute exceeding the scope of a private search" in a case where storage unit employee notified police of child pornography found in a suitcase in defendant's storage unit).

Defendant argues that the "virtual certainty" test of *Jacobsen* does not apply unless there has been a "previous search of the actual container in question."

(Doc. # 44 at 6). As explained above, Google's practice of only hashing files its employees have viewed indicates that Google *did* previously view the images attached to Defendant's email. In this case, as in *Bowers*, a private party viewed the images, believed that they were child pornography, and alerted the authorities, who then viewed the same images. The difference between *Bowers* and this case is that the images here are made of pixels, not photo paper, and that Google identified the images as ones it had previously viewed by using hash values instead of human memory. Despite the relation to legitimate and "extensive privacy interests at stake in . . . modern electronic device[s]," *Lichtenberger*, 786 F.3d at 485, those differences do not require a different result in this case because the "virtual certainty" standard is met.

In *Lichtenberger*, the Sixth Circuit applied *Jacobsen* to an officer's search of a defendant's laptop for child pornography, holding that, in order for the government's search to be within the scope of the earlier private search, the government official "had to proceed with 'virtual certainty' that the 'inspection of the [laptop] and its contents would not tell [him] anything more than he had already been told'" by the defendant's girlfriend, the private searcher. *Lichtenberger*, 786 F.3d at 488. The court ruled that the officer did not have "virtual certainty" that what he viewed would be the same child pornography the girlfriend reported because it was not at all clear that she showed him the same images she had previously looked at. There was "a very real possibility," the court concluded, that the detective "could have discovered something *else* on Lichtenberger's laptop that was private, legal, and unrelated to the allegations prompt-

ing the search—precisely the sort of discovery the *Jacobsen* Court sought to avoid in articulating its beyond-the-scope test." *Id.* at 488-49.

There is no such possibility here. As discussed earlier, the digital fingerprints produced by hashing provide "virtual certainty" that the images will be the same as those seen on a prior search. And because Google's CyberTip report "did not include any email body text or header information associated with the reported content" (Doc. # 33-1 at ¶ 10), or any images that Google had not previously viewed, Detective Schihl had "little chance to see much other than contraband." *Lichtenberger*, 786 F.3d at 486. *Compare with Ackerman*, 831 F.3d at 1294 (NCMEC viewed email content and three attachments that the ESP had not viewed). That distinguishes this case from ones involving laptops and cell phones where privacy interests are high because of the large amount of information on those devices. There was no likelihood here, as there was in *Lichtenberger* or similar cases, that the attachments would "contain 1) many kinds of data, 2) in vast amounts, and 3) corresponding to a long swath of time." *Lichtenberger*, 786 F.3d at 488. The key question for the test under *Jacobsen* is whether the government official "saw the exact same images" the private searcher saw. *Id.* at 490. In this case, the evidence reveals that Detective Schihl and Google saw the same images—no more and no less.

Finally, Defendant argues that applying *Jacobsen* to find that Defendant's Fourth Amendment rights were not violated is a dramatic expanse of doctrine that allows "modern technology utilized by the private party" to "frustrate a citizen's reasonable expectation of privacy in the contents of a citizen's

sealed container." (Doc. # 44 at 6-7). This is not so. Google's hash-value matching—in the words of the R&R, its "virtual eye"—does not reveal anything about an image that Google does not already know from the regular eyes of its employees. Put another way, hashing is not a futuristic substitute for a private search—it is merely a sophisticated way of confirming that Google already conducted a private search. Google's use of hash values has no more effect on Defendant's reasonable expectation of privacy than Google's initial private search does (and because Google is not a government agent, the Fourth Amendment is "wholly inapplicable" to its searches, even "unreasonable one[s]," *Jacobsen*, 446 U.S. at 113-14).

For all those reasons, Defendant's objection that Detective Schihl's search exceeded the scope of Google's private search is **overruled**.

### C. Traditional trespass analysis does not apply.

Defendant's last objection is that Detective Schihl's search "was illegal when viewed through the lens of the traditional trespass test." (Doc. # 44 at 7-8) (citing *Ackerman*, 831 F.3d at 1308 (citing *United States v. Jones*, 565 U.S. 400 (2012))). Defendant also argues that Google did not open the attachments, which he refers to as "sealed virtual containers." *Id.* Once again, Defendant's attempt to distinguish between the image uploaded to his email account and the image Google previously viewed is unavailing—these particular attachments are not "sealed virtual containers" because the matching hash values indicate that Google has previously viewed them. Moreover, as Magistrate Judge Smith explains in the

R&R, the "traditional trespass" test does not apply when the government action is within the scope of a previous private search, because the Fourth Amendment does not apply to private individuals. (Doc. # 41 at 26 n.10). Therefore, this objection is overruled.

**IV.Conclusion**

Upon *de novo* consideration of the R&R and the objections thereto, the Court concludes that Magistrate Judge Smith's factual findings are clearly supported by the record. The Court further agrees with Magistrate Judge Smith's analysis and recommended disposition of Defendant's motion to suppress. Accordingly,

**IT IS ORDERED** as follows:

(1) Defendant's objections to the Magistrate Judge's Report and Recommendation

are **overruled**;

(2) The Magistrate Judge's factual findings are **adopted** as the factual findings of

the Court;

(3) The Magistrate Judge's analysis and conclusions of law are **adopted** as the Court's conclusions of law, as supplemented herein;

(4) Defendant's Motion to Suppress evidence (Doc. # 27) is **denied**; and

(5) The time period from January 31, 2017 through the date of this Order, totaling 143 days, is deemed excludable time from the Speedy Trial Act pursuant to 18 U.S.C. § 3161(h)(1)(F).

This 23rd day of June, 2017.

**Signed By:**

***David L. Bunning*** **DB**

**United States District Judge**

## APPENDIX C

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
NORTHER DIVISION
COVINGTON

| | |
|---|---|
| UNITED STATES OF AMERICA,<br>Plaintiff,<br><br>v.<br><br>WILLIAM MILLER,<br>Defendant. | Criminal Case No. 16-47-ART-CJS<br><br>**Report and Recommendation** |

*** *** *** ***

This matter is before the Court on the Defendant's Motion to Suppress. (R. 27). The Government has filed its Response, to which Defendant filed a Reply. (R. 33; R.37). The Motions have been referred to the undersigned for preparation of a Report and Recommendation pursuant to 28 U.S.C. § 636(b)(1)(B). (*See* R. 6). While Defendant requested an evidentiary hearing in his Motion filing, he withdrew that request in his Reply and instead requested the Court set the matter for oral argument. (*See* R. 27, at 11; R. 37, at 1). The Court heard oral argument on the Motion (*see* R. 38; R. 39), and the matter is now ripe for consideration. For the reasons set forth below, it will be recommended that Defendant's Motion to Suppress be **denied**.

## I. Factual Background

On July 9, 2015, an individual using Google email (Gmail) account miller694u@gmail.com uploaded two images of apparent child pornography to an email, which may or may not have been sent. (R. 33-2, at 3-4). Google was alerted to these images through use of its proprietary "hashing" technology. (R. 33-1, at 1-2, 4-10 ¶¶ 4-8, 10-13). A representative from Google explains:

> 4. . . . [S]ince 2008, Google has been using its own proprietary hashing technology to tag confirmed child sexual abuse images. Each offending image, after it is viewed by at least one Google employee, is given a digital fingerprint ("hash") that our computers can automatically recognize and is added to our repository of hashes of apparent child pornography as defined in 18 U.S.C. § 2256. Comparing these hashes to hashes of content uploaded to our services allows us to identify duplicate images of apparent child pornography to prevent them from continuing to circulate on our products.
>
> 5. We also rely on users who flag suspicious content they encounter so we can review it and help expand our database of illegal images. No hash is added to our repository without the corresponding image first having been visually confirmed by a Google employee to be apparent child pornography.
>
> . . .
>
> 7. When Google's product abuse detection system encounters a hash that matches a hash

> of a known child sexual abuse image, in some cases Google automatically reports the user to [the National Center for Missing and Exploited Children] NCMEC without reviewing the image. In other cases, Google undertakes a manual, human review, to confirm that the image contains apparent child pornography before reporting it to NCMEC.
>
> 8. When Google discovers apparent child pornography, Google files a report with . . . NCMEC in the form of a CyberTip. . . .

(R. 33-1, at 1 ¶¶ 4-8).[1]

Here, the parties do not dispute that Google's product abuse detection system hit on two images attached to an email in Defendant's Gmail account that matched hash values in Google's repository of hashes of apparent child pornography. (R. 27, at 1-2; R. 33, at 1-3; R. 33-1, at 2, ¶¶ 10, 11; R. 37, at 2-3). In response, Google submitted an "automatic report" to NCMEC– which Google is required to do by law, via a CyberTipline report.[2] (R. 33-1, at 1-2 ¶¶ 7, 8, 10; R. 33-2, at 3).

---

[1] In his Motion to Suppress Defendant stated he believed NCMEC provided Google with the hash values to use in its searching process. However, during oral argument counsel withdrew this statement, acknowledging the Affidavit of the Google executive explained that was not the case in this circumstance. (*See* R. 33-1, at ¶ 9).

2 Google's Senior Manager of Law Enforcement and Information Security stated that "[w]hen Google's product abuse detection system encounters a hash that matches a hash of a known child sexual abuse image, in some cases Google automatically reports the user to NCMEC without a manual re-review of the image. (R. 33-1, at 1-2, ¶ 7). Here, the report states it is an "automatic report." (R. 33-2, at 3).

Google's employees did not manually view the content of the email or the images prior to submitting the report to NCMEC. (R. 33-1, at ¶¶ 10-11). The CyberTipline report did not contain the content of the email or header information, but did include the email address used, the IP address associated with the email in question, classification of the images,[3] the file names listed with the images and the two uploaded image files. (R. 33-1, at ¶¶ 10-11; R. 33-2, at 1-5; R. 33-6, at 4 ¶ 14). In addition, on or about the time it submitted the CyberTipline report, Google disabled the associated Gmail account. (R. 33-1, at ¶¶ 10-11).

When NCMEC received the CyberTipline report, its staff did not open or view the two uploaded files contained in the report. (R. 33-6, at 4 ¶ 15). Instead, a member of NCMEC's staff queried publicly-available sources related to the "miller694u@gmail.com" email address and located publicly-available social network profiles associated with that account. (*Id.*). NCMEC also verified the IP address reported by Google and learned it appeared to be associated with a Time Warner Cable account having a potential geographic location of Fort Mitchell, Kentucky. (*Id.* at ¶ 16). NCMEC, either by automated processes or its staff, provided the information in Sections B and C of the CyberTipline report and specifically noted in the report: "[p]lease be advised that NCMEC has not opened or viewed any uploaded files submitted with this report and has no information concerning the con-

[3] The CyberTipline report noted the images had been classified as A1 under the industry classification system, which indicates that the content of the associated image contained a depiction of a prepubescent minor engaged in a sexual act. (R. 33-1, at 2 ¶ 10; R. 33-2, at 4).

tent of the uploaded files other than information provided in the report by the ESP [electronic service provider]." (*Id*. at ¶¶ 16-17; R. 33-2, at 8). NCMEC made the CyberTipline report available to Kentucky State Police and the Kenton County Police Department. (R. 33-6, at ¶¶ 16, 17).

On August 13, 2015, Detective Aaron Schihl of the Kenton County Police Department received this CyberTipline report from NCMEC. (R 33-3, at 1). Detective Schihl opened the attachments and viewed the images, which he confirmed to be child pornography. (*Id*. at 1-2). Detective Schihl requested a grand jury subpoena for the subscriber information for the Time Warner Cable account associated with the IP address provided in the report. (*Id*. at 1). Time Warner responded to the request, identifying Tania Miller of 2271 Mercury Street, Fort Mitchell, Kentucky, 41017 as the subscriber for the requested IP address and provided contact information for the account. (*Id*.). Detective Schihl sought and obtained a search warrant for the contents of the miller694u@gmail.com account. (R. 33-3). In his Affidavit, Detective Schihl states he received a CyberTipline report, he provides the information learned regarding the IP and email addresses, and he describes the images based on his review of them. (R. 33-3, at 1-2). After review of the contents of the Gmail account, Detective Schihl obtained a search warrant for Defendant's home, followed by a search warrant for the electronic devices seized from Defendant's home. (R. 33-4; R. 33-5). The fruits of these three searches yielded additional evidence of the receipt, possession, and distribution of child pornography. (*See* R. 33-3; R. 33-4; R. 33-5). Defendant seeks to suppress all evidence obtained in this case.

## II. Analysis

The Fourth Amendment provides in relevant part that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV. Fourth Amendment protections attach when a "search" occurs. A "search" occurs when the government infringes on an expectation of privacy that society is prepared to consider reasonable, *see United States v. Jacobsen*, 466 U.S. 109, 115 (1984), or where the government physically intrudes on a constitutionally protected area for the purpose of obtaining information, *see United States v. Jones*, 565 U.S. 400, 407-08 (2012). Fourth Amendment protections do not apply to a private search. *Jacobsen*, 466 U.S. at 113. Nor do they apply if the government merely replicates a prior private search. *Id*. at 115.

In the pending Motion, Defendant challenges two warrantless searches as having violated his Fourth Amendment rights against unreasonable searches and seizures. He first contends that Google's use of its hashing technology to search his email account without a warrant constituted a search implicating the Fourth Amendment because Google acted as a state actor in conducting the search. Defendant also challenges Detective Schihl's actions of opening and viewing the attachments to his email, which he argues no one had previously opened and viewed, without first obtaining a warrant. For the reasons discussed below, Defendant's challenges to these searches fail.

### A. Google is not a government actor

Defendant challenges Google's conduct of searching his email account for child pornography by utilizing hashing technology and then seizing two images

attached to an unsent email. (R. 27, at 3-7). The Sixth Circuit has held that a person has a reasonable expectation of privacy in the content of his emails. *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010). The Fourth Amendment, however, applies only to government action and does not constrain private parties "not acting as an agent of the Government or with the participation or knowledge of any governmental official." *Jacobsen*, 466 U.S. at 113 (quoting *Walter v. United States*, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting)). Defendant argues that because of Google's nexus with NCMEC, an entity Defendant argues qualifies as a state actor, Google is also a state actor for purposes of the Fourth Amendment. (R. 27, at 5-6).

Defendant acknowledges that the Sixth Circuit has yet to consider whether NCMEC is a state actor. However, he notes that the Tenth Circuit has recently considered the issue and found that it is. *See United States v. Ackerman*, 831 F.3d 1292, 1296 (10th Cir. 2016) (finding NCMEC to be a governmental entity and an agent of the government). For purposes of this Motion, the Court will assume without deciding that NCMEC is a governmental entity or an agent of the Government such that the Fourth Amendment applies to its searches.

In his Motion, Defendant argues Google's conduct of searching his email account implicates the Fourth Amendment because there is a sufficiently close nexus between NCMEC and Google's search such that Google's conduct is fairly treated as that of NCMEC. (R. 27, at 5-6) (citing *Lansing v. City of Memphis*, 202 F.3d 821, 830 (6th Cir. 2000)). He also argues that Google is a government actor because it is a willful

participant in NCMEC's policy of searching for and finding child pornography. (*Id*.).

To support his argument, Defendant points to statutory reporting requirements that require Google to report child pornography to NCMEC and preserve the suspected file or be subject to significant monetary penalties for failing to adhere to the reporting requirements. (R. 27, at 6) (citing 18 U.S.C. § 2258A). Defendant also argues that while Google is not statutorily required to search its products for child pornography, it presumably does so because of its relationship with NCMEC. Specifically, Defendant explains that Google and NCMEC are "entwined based on shared governmental policies and their combined actions reflect a joint effort and commitment to work together" to combat child pornography. (*Id.* at 7).

As the parties acknowledge, the Sixth Circuit has not yet addressed the issue of whether ESPs, such as Google, act as an agent of the government when they scan files on their network for child pornography and, pursuant to the reporting requirement contained in 18 U.S.C. § 2258A, report findings of apparent child pornography to NCMEC. However, the cases that have considered the issue have uniformly held that such conduct does not transform an ESP into a government actor. *See United States v. Stevenson*, 727 F.3d 826, 831 (8th Cir. 2013) ("A reporting requirement, standing alone, does not transform an [i]nternet service provider into a government agent whenever it chooses to scan files sent on its network for child pornography."); *United States v. Cameron,* 699 F.3d 621, 638 (1st Cir. 2012) (finding Yahoo! was not acting as an agent of the government in conducting a search of defendant's account and reporting its findings to

NCMEC, stating "if Yahoo! chose to implement a policy of searching for child pornography, it presumably did so for its own interests."); *United States v. Richardson*, 607 F.3d 357, 366 (4th Cir. 2010) (holding that AOL's scanning of email communications for child pornography and reporting discoveries to NCMEC did not trigger the Fourth Amendment's warrant requirement because no law enforcement officer or agency asked the provider to search or scan the defendant's emails); *United States v. Stratton*, No. 15-40084, 2017 WL 169041, at **4-5 (D. Kan. Jan. 7, 2017) (finding Sony was not acting as government agent when it monitored its users' accounts for child pornography because it was acting to protect its own interest in providing a safe online gaming community); *United States v. Miller*, No. 8:15-cr-172, 2015 WL 5824024, at *4 (D. Neb. Oct. 6, 2015) ("Google did not become a state actor by providing the reports required by law."); *United States v. Keith*, 980 F. Supp. 2d 33, 44 (D. Mass. 2013) (finding AOL, motivated by its own wholly private interests in monitoring emails for child pornography, was not acting as a government agent in searching its network for child pornography and reporting any findings to NCMEC). In fact, defense counsel stated during oral argument that his research revealed no authority, either in this circuit or elsewhere, where an ESP has been held to be a government actor in a similar circumstance.

While Defendant argues Google is a state actor because of its nexus relationship to NCMEC, the Sixth Circuit has explained the appropriate considerations when determining whether a private party is acting as an agent of the government in conducting a search such that the Fourth Amendment is implicated:

> [A] private party's search is attributable to the government only "if the private party acted as an instrument or agent of the Government." *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 614, 109 S. Ct. 1402, 103 L. Ed.2d 639 (1989); *see, e.g., United States v. Clutter*, 914 F.2d 775, 778 (6th Cir. 1990). That "necessarily turns on the degree of the Government's participation in the private party's activities." *Skinner*, 489 U.S. at 614, 109 S. Ct. 1402. In the context of a search, the defendant must demonstrate two facts: (1) Law enforcement "instigated, encouraged or participated in the search" and (2) the individual "engaged in the search with the intent of assisting the police in their investigative efforts." *United States v. Hardin*, 539 F.3d 404, 419 (6th Cir. 2008) (quoting *United States v. Lambert*, 771 F.2d 83, 89 (6th Cir. 1985)).

*United States v. Shepherd*, 646 F. App'x 385, 388 (6th Cir. 2016); *see also United States v. Bowers*, 594 F.3d 522, 525-26 (6th Cir. 2010) ("in determining whether a private party is acting as an agent of the government such that the Fourth Amendment applies" the Sixth Circuit uses a two-factor analysis: "(1) the government's knowledge or acquiescence to the search, and (2) the intent of the party performing the search.") (quoting *Hardin*, 539 F.3d at 418) (internal quotations omitted). "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.'" *Bowers*, 594 F.3d at 526 (quoting *Hardin*, 539 F.3d at 418 (internal quotation marks and emphasis omitted)).

Defendant's argument that Google's reporting obligations under 18 U.S.C. § 2258A render Google an agent of NCMEC is not persuasive. As Defendant acknowledges, § 2258A does not require Google to search for child pornography. In fact, the statute specifically states that it does not impose such a requirement: "[n]othing in this section shall be construed to require an electronic communication service provider . . . to – (1) monitor any user, subscriber, or customer of that provider; (2) monitor the content of any communication of any person described in paragraph (1); or (3) affirmatively seek facts or circumstances described in sections (a) and (b)." 18 U.S.C. § 2258A(f). Instead, the statute merely requires that when an ESP discovers apparent child pornography, it comply with its reporting requirements. Thus, Defendant's pointing to the statute does not establish that Google conducted its search because of any directive or encouragement by the government.

Further, while the Sixth Circuit has not addressed the specific issue at hand, several other circuit courts have considered the issue and have consistently held that the reporting requirement set forth in 18 U.S.C. § 2258A, or its predecessor statute, "does not transform an [i]nternet service provider into a government agent whenever it chooses to scan files sent on its network for child pornography." *Stevenson*, 727 F.3d at 829-30; *see also Cameron*, 699 F.3d at 637-38 (rejecting argument that statutory reporting obligations demonstrated government control over Yahoo!, stating "the statute did not impose any obligation to *search* for child pornography, merely an obligation to *report* child pornography of which Yahoo! became aware") (emphasis original); *Richardson*, 607 F.3d at 367 (distinguishing the reporting scheme in *Skinner*,

noting nothing in the statute requires the electronic communication services to actively seek evidence of child pornography nor prescribes the procedures for doing so). These persuasive authorities support the conclusion in this case that Google's obligation to report known facts or circumstances of apparent child pornography to NCMEC does not transform Google's voluntary decision to use its own proprietary hashing technology to search its products for child pornography into conduct of a government actor where the statute does not impose a duty to conduct a search.

Nor does the Court find merit in Defendant's argument that Google's willful participation in NCMEC's policy of searching for and finding child pornography demonstrates Google was acting as a government actor. The question of whether Google served as an agent of the government in performing its search of Defendant's email account for hash value matches "necessarily turns on the degree of the Government's participation in [Google's] activities." *Shepherd*, 646 F. App'x at 388 (quoting *Skinner*, 489 U.S. at 614).

Here, Defendant has not presented any evidence that NCMEC or law enforcement "instigated, encouraged or participated in the search" of Defendant's Gmail account. *Shepherd*, 646 F. App'x at 388. Defendant does not contend that NCMEC or law enforcement asked Google to perform the search of his emails or that either had any role in instigating or participating in the search. Even assuming NCMEC may have been aware that Google routinely monitors its platforms for illegal usage, and submits reports of any illegal activity found, there is no evidence that NCMEC or law enforcement compelled or encouraged Google to routinely monitor its platforms. Nor does Defendant

present evidence to suggest that NCMEC or law enforcement were aware of the existence of Defendant or the miller694u@gmail.com account prior to Google's search in this case. *Cameron,* 699 F.3d at 638 (finding no evidence that the government instigated the search, participated in the search, or coerced the ESP to conduct the search at issue).

In fact, the Affidavit of Cathy A. McGoff, Google's Senior Manager of Law Enforcement and Information Security, provides that Google has no records to suggest, prior to submitting the CyberTipline report, that Google was aware of any law enforcement investigation pertaining to the user associated with the report. (R. 33-1, at 2 ¶ 12). Thus, evidence in the record does not establish that NCMEC or law enforcement "instigated, encouraged or participated" in Google's search.

Nor is there evidence that Google "engaged in the search with the intent of assisting the [government] in their investigative efforts." *Shepherd*, 646 F. App'x at 388. Other than referencing the statute requiring Google to report (but not search for) discoveries of child pornography to NCMEC, the only other evidence Defendant points to as suggesting a relationship between Google, NCMEC and/or law enforcement are website citations to a number of articles on Google's website and blog. (R. 27, at 6 n.3). In these articles, Google expresses its commitment to protecting children online, discusses its goal of finding, removing and reporting child pornography on its products, and discusses its involvement/collaboration with other "tech industry companies" and NCMEC to combat child pornography by participating in various coalitions and programs. (*Id.*). While Defendant argues this evidence demonstrates Google is collaborating

with NCMEC and has "made itself a willful participant in NCMEC's policy of searching out and finding child pornography," these articles only establish that Google and NCMEC have a shared goal of eradicating the online sharing of child pornography. "Sharing a goal with the Government is insufficient to transform [an ESP] from a private actor into a Government agent." *United States v. Stevenson*, No. 3:12-cr-5, 2012 WL 12895560, at *3 (S.D. Iowa June 20, 2012), *affirmed,* 727 F.3d 825 (8th Cir. 2013).

Here, as in *Stevenson*, Defendant has offered no evidence that the Government, through NCMEC or law enforcement, participated in or encouraged Google's search of Defendant's email account. In fact, there is no evidence that NCMEC or law enforcement were even aware of the search of Defendant's emails prior to their receipt of the CyberTipline report. Nor is there evidence Google performed the search for the purpose of assisting the Government in its investigative efforts. Instead, the Government provided the Affidavit of Ms. McGoff that explains Google's reasons for its decision to monitor its platform for child pornography:

> 3. Google has a strong business interest in enforcing our terms of service and ensuring that our products are free of illegal content, and in particular, child sexual abuse material. We independently and voluntarily take steps to monitor and safeguard our platform. If our product is associated with being a haven for abusive content and conduct, users will stop using our services. Ridding our products and services of child abuse images is critically important to protecting our users, our product, our brand, and our business interests.

> 4. Based on these private, non-government interests, since 2008, Google has been using its own proprietary hashing technology to tag confirmed child sexual abuse images. Each offending image, after it is viewed by at least one Google employee, is given a digital fingerprint ("hash") that our computers can automatically recognize and is added to our repository of hashes of apparent child pornography as defined in 18 U.S.C. § 2256. Comparing these hashes to hashes of content uploaded to our services allows us to identify duplicate images of apparent child pornography to prevent them from continuing to circulate on our products.

(R. 33-1, at 1 ¶¶ 3-4). This evidence demonstrates Google's actions in this case were motivated by business interests that are separate from a desire to assist law enforcement. (*Id.*). Other courts have found such evidence sufficient to demonstrate the ESP operated its file-scanning programs independently of the government, and thus were held not to have acted as agents of the government in operating their scanning programs. *Stevenson*, 727 F.3d at 830-31; *Cameron,* 699 F.3d at 638 (stating that the fact child pornography is a government interest does not mean that an ESP "cannot voluntarily choose to have the same interest").

Thus, the evidence before the Court in the present case demonstrates that Google was not acting as an agent of NCMEC or law enforcement, but as a private entity pursuing its own business interests. Therefore, Google's use of its hashing technology to search Defendant's email account did not implicate the Fourth Amendment.

### B. Detective Schihl's actions did not exceed Google's private search

Defendant also argues that even if Google's search and seizure was not government action, Detective Schihl exceeded Google's private search by opening and viewing the email attachments and thereby violated his Fourth Amendment rights. This raises questions about the private search doctrine and the application of the doctrine to the circumstances here.

The private search doctrine permits a government agent to verify the illegality of evidence discovered during a private search provided the agent stays within the scope of the private search. *United States v. Lichtenberger*, 786 F.3d 478, 481-83 (6th Cir. 2015) (citing *Jacobsen*, 466 U.S. at 119-20). A government agent's invasion of a defendant's privacy "must be tested by the degree to which [the agent] exceeded the scope of the private search." *Jacobsen*, 466 U.S. at 115 (citing *Walter*, 447 U.S. 649); *Lichtenberger,* 786 F.3d at 482. The Supreme Court has explained that "[o]nce frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information." *Jacobsen*, 466 U.S. at 117.

The private search doctrine originates from the Supreme Court's decision in *Jacobsen*, 466 U.S. at 109. In *Jacobsen*, Federal Express ("FedEx") employees discovered a damaged package and proceeded to examine its contents, which was consistent with company policy involving insurance claims. *Jacobsen,* 466 U.S. at 111. The container itself was made of cardboard packaging, but inside of it were crumpled newspapers concealing a 10-inch tube made of silver duct tape. *Id.* The employees proceeded to cut open the

tube, and discovered four zip-lock bags filled with an unidentified white powder. *Id.* FedEx notified the Drug Enforcement Agency ("DEA") of their discovery, and placed the tube and its contents back in the cardboard container. *Id.* Upon arrival, a DEA agent discovered the partially opened container, and observed a slit in the duct tape tube. He then removed the zip-lock bags, took a sample from each, and field-tested it. The test positively identified the substance as cocaine. *Id.* at 112.

The Supreme Court analyzed whether the DEA agent's after-occurring warrantless search had exceeded the scope of the FedEx employees' initial private search of the package. The Court found that the agent's removal of the cocaine from the package remained within the scope of the private search because "there was a virtual certainty that nothing else of significance was in the package and that a manual inspection of the tube and its contents would not tell him anything more than he already had been told." *Id.* at 119. As for the chemical test, the Court held that the field test "could disclose only one fact previously unknown to the agent–whether or not a suspicious white powder was cocaine." *Id.* at 122. The Court concluded that no search occurred because the defendant did not have a legitimate expectation of privacy in whether the powder was contraband and the test could not disclose any other arguable private fact. *Id.* at 123-24.

Here, Defendant argues Detective Schihl exceeded Google's private search when he opened and viewed the email attachments because Google had not conducted a manual review of the two attached images before submitting them to NCMEC. (R. 33-1, at 2 ¶ 11). Instead, Google reported the attachments to NCMEC because its hashing technology indicated

they were images that matched hash values of images its employees had previously viewed and found to be apparent child pornography. (R. 33-1, at 2 ¶¶ 4, 7, 10-11). NCMEC, without opening the attachments or otherwise viewing the images, forwarded the CyberTipline report to law enforcement.[4] (R. 33-6, at 4 ¶15). It is undisputed that Detective Schihl was the first person to manually open and view the attachments to Defendant's email. (R. 33-3, at 2; R. 33-6, at 4 ¶ 15). Thus, Defendant argues that because Google did not manually open and view the attachments, Detective Schihl opened and viewed unopened virtual containers, i.e., the attachments, thereby exceeding the scope of Google's search.

The Sixth Circuit has explained that "[u]nder 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 reexamines the evidence and, relatedly, how certain it is regarding what it will find." *Lichtenberger*, 786 F.3d at 485-86 (citing *Jacobsen*, 466 U.S. at 119-20). Thus, to determine whether the Fourth Amendment is implicated by Detective Schihl's opening and viewing of the attachments sent via the CyberTipline report, the

---

[4] Defendant finds of import that the CyberTipline report noted that NCMEC had "no information concerning the content of the uploaded files other than information provided in the report by [Google]," and that NCMEC classified the files as "Child Pornography (Unconfirmed-Files Not Reviewed by NCMEC). (R. 27, at 10) (quoting R. 33-2, at 8). However, the fact that NCMEC did not review the image files reported by Google does not affect the Court's determination of whether Officer Schihl's actions fell within the scope of Google's private search.

Court must determine whether Detective Schihl was virtually certain that his "inspection of the [attachments] . . . would not tell [him] anything more than he already had been told [by Google via the CyberTipline report]." *Lichtenberger*, 786 F.3d at 488 (citing *Jacobsen*, 466 U.S. at 119).

Defendant looks to the Tenth Circuit's *Ackerman* decision to support his argument that Detective Schihl's conduct was unconstitutional. *Ackerman*, 831 F.3d at 1292. Defendant contends the facts here are analogous to those the *Ackerman* court found exceeded the ESP's private search. (R. 27, at 8). In *Ackerman*, the defendant sent an email containing child pornography. *Id.* at 1294. But before the email reached its intended recipient, AOL's automated filter identified the email as containing one image that matched the hash value of an image an AOL employee had previously viewed and deemed to be child pornography. *Id.* AOL automatically stopped the email's delivery and without manually viewing the email or its attachments, it reported the email to NCMEC and provided the email and its four attachments (not just the one attachment containing the image AOL's filter found matched the hash value of a known image of child pornography). *Id.*

A NCMEC analyst opened the email, viewed each of the four attached images and confirmed all four images appeared to be child pornography. *Id.* In reaching its decision that NCMEC, a governmental entity or agent, had exceeded AOL's private search, the *Ackerman* court found of import that NCMEC opened and viewed information beyond the one image that was the target of AOL's hash value match. *Id.* at 1306. Notably, the *Ackerman* court asked, but left unresolved the following questions:

> What if NCMEC hadn't opened Mr. Ackerman's email but had somehow directly accessed (only) the (one) attached image with the matching hash value? Could the government have argued that, in that case, NCMEC's actions didn't risk exposing any private information beyond what AOL had already reported to it? Or might even that have risked exposing new and protected information, maybe because the hash value match could have proven mistaken (unlikely if not impossible) or because the AOL employee who identified the original image as child pornography was mistaken in his assessment (unlikely if maybe more possible)?

*Id.* at 1306 (citing Salgado, Fourth Amendment Search and the Power of the Hash, 119 Harv. L. Rev. F. 38, 38-40 (2005)). The court left these questions unresolved because it found the undisputed facts indicated that NCMEC exceeded AOL's private search when it opened the email as well as all four images, rather than solely viewing the one attachment that was the target of AOL's private search. The Court found that NCMEC's conduct of opening the email and viewing the three attachments that had not been identified by AOL as having a hash value match "was enough to risk exposing private, noncontraband information that AOL had not previously examined." *Ackerman*, 831 F.3d 1306-07.

The facts of this case are distinguishable from *Ackerman*. Most significantly, there is no evidence or allegation that Google sent anything to NCMEC other than the files of the two images having a hash value match to two images Google's employees had previously identified as being apparent child pornography.

(R. 33-1, at 2 ¶¶ 10, 11; R. 33-2, at 4-5). Thus, the reasoning of the *Ackerman* court in finding the search exceeded the scope of AOL's private search is not applicable. Instead, the issue is whether Detective Schihl's opening and viewing of the two attachments that Google's private search detected as matching the hash values of images previously identified as apparent child pornography risked exposing any private information beyond what Google had reported.

Defendant contends the answer to this inquiry is yes, and argues the circumstances at hand are similar to those in *Walter v. United States*, 447 U.S. 649 (1980). In *Walter*, a private mail carrier mistakenly delivered 12 packages containing 871 boxes of 8-millimeter film to the wrong address. *Id.* at 651. Employees of the company that received the packages opened them, finding the boxes of film. The boxes contained drawings and descriptions that alluded to the obscene content of the films. *Id.* at 652. One employee attempted to view portions of at least one film by holding it up to the light, but was unsuccessful. *Id.* Soon after, the employees contacted the FBI, and an agent picked up the packages. *Id.* The FBI agents–without obtaining a warrant–proceeded to screen the films through a projector. *Id.*

The Supreme Court did not issue a majority opinion in *Walter*.[5] Justice Stevens, joined by Justice Stewart, announced the judgment of the Court, and found

[5] While a majority opinion did not issue, five Justices agreed that the warrantless projection of the films constituted a search that infringed the defendant's Fourth Amendment interests. Justices Stevens and Stewart found that the officers had violated the Fourth Amendment because they exceeded the scope of the private search. *Walter*, 447 U.S. at 653-60. However, Justice White, with whom Justice Brennan joined, wrote separately stating that

that "the Government may not exceed the scope of the private search unless it has the right to make an independent search." *Id.* at 657. Justice Stevens found that despite the descriptive nature of the labels on the films' packaging, the private party had not actually viewed the films and "prior to the [g]overnment screening one could only draw inferences about what was on the films." *Id.* at 656-57. He thus concluded that the viewing of the films was a "significant expansion" of the private search, requiring it be characterized as a separate search. *Id.* at 657-59.

Here, Defendant Miller contends the hash values of the images Google located in its search are analogous to the descriptive labels on the films in *Walter*. Detective Schihl's conduct of opening and viewing the attachments, argues Miller, is akin to the FBI agents' unconstitutional conduct in *Walter* of viewing the films without a warrant. (R. 37, at 4). Defendant points to a decision of the United States District Court in the District of Massachusetts as supporting the

---

even if there had been a private screening of the films, the agents still needed a warrant because the private search would not have exposed the content of the films to plain view. Justice Marshall concurred in the judgment without discussion.

Justices Blackmun, with whom Chief Justice Burger, Justice Powell and Justice Rehnquist joined, dissented in the judgment, but agreed the legality of the government's actions must be tested by the scope of the private search that preceded them. *See Jacobsen*, 466 U.S. at 115-16 (discussing the various opinions in *Walter*). Justice Blackmun explained that because the private search in *Walter* exposed the labels describing the nature of the films, there was no remaining expectation of privacy in the contents of the films. He found the subsequent viewing of the films by the agents did not "change the nature of the search," and therefore their view ng did not constitute an additional search subject to the warrant requirement. *Walter*, 447 U.S. at 663-64.

comparison of the facts at hand to those in *Walter*. *See United States v. Keith*, 980 F. Supp. 2d 33 (D. Mass. 2013).

In *Keith*, AOL was alerted to an email on its system containing a file that had a positive hash value match to an image AOL had previously determined to be child pornography. *Keith,* 980 F. Supp. 2d at 37. Much like Google, AOL maintains a database of hash values that is "essentially a catalog of files that have previously been identified as containing child pornography." *Id.* at 36. Upon detecting a hash value match in defendant's email, AOL forwarded the file (unopened) to NCMEC via the CyberTipline. *Id.* A NCMEC analyst opened and inspected the file and determined it contained child pornography. The file was then forwarded to local law enforcement. *Id.*

The defendant in *Keith* moved to suppress this evidence, arguing that by opening and viewing the image NCMEC exceeded AOL's private search.[6] *Id*. The district court agreed, finding that the hash value provided by AOL, much like the labels on the films in *Walter*, likely would have furnished the requisite probable cause for a warrant, but did not justify viewing the contents without a warrant. The court also distinguished *Jacobsen*, 466 U.S. at 109, stating it is "indisputable that AOL forwarded the suspect file only because its hash value matched a stored hash value,

---

[6] Defendant also argued that both AOL and NCMEC were acting as government agents under the circumstances, and thus their searches violated his Fourth Amendment rights. *Keith*, 980 F. Supp. 2d at 39. The district court dismissed the notion that AOL had a sufficient enough connection with the government to be treated as a government actor, but held NCMEC to be an agent of the government and subject to Fourth Amendment constraints. *Id*. at 40-42.

not because some AOL employee had opened the file and viewed the contents." *Keith*, 980 F. Supp. 2d at 42-43. The court found *Walter*, not *Jacobsen*, was the better analog to the facts of its case. *Id.* at 43. The court further stated:

> In this regard it is worth noting that matching the hash value of a file to a stored hash value is not the virtual equivalent of viewing the contents of the file. What the match says is that the two files are identical; it does not itself convey any information about the contents of the file. It does say that the suspect file is identical to a file that someone, sometime, identified as containing child pornography, but the provenance of that designation is unknown. So a match alone indicts a file as contraband but cannot alone convict it. That is surely why a CyberTipline analyst opens the file to view it, because the actual viewing of the contents provides information additional to the information provided by the hash match. This is unlike what the Court found the case to be in *Jacobsen*, where the subsequent DEA search provided no more information than had already been exposed by the initial FedEx search. *Jacobsen* is inapposite.

*Id.* Thus, the court found that by opening the previously unopened email image file, NCMEC exceeded the scope of the private search. *Id.*

Defendant Miller's reliance upon the *Keith* court's rejection of *Jacobsen* and acceptance of *Walters* to the circumstances in that case raises additional questions for this Court. In applying the Supreme Court's holding in *Jacobsen*, the Sixth Circuit has explained that

the relevant inquiry for determining if government action exceeds the scope of a private search is to determine how much information the government stood to gain when it conducted the search and, relatedly, how certain it was regarding what it would find. *Lichtenberger,* 786 F.3d at 485-86 ("We have held a government search permissible–that is, properly limited in scope–in instances involving physical containers and spaces on the grounds that the officers in question had near-certainty regarding what they would find and little chance to see much other than contraband");[7] *Bowers*, 594 F.3d at 526 ("based on [defendant's roommate's] statements that the album contained child pornography, the agents were justified in opening the album to view the potentially incriminating evidence. . . . In doing so, the agents 'learn[ed] nothing that had not previously been learned during the private search' and 'infringed no legitimate expectation of privacy.'") (quoting *Jacobsen*, 466 U.S. at 120); *United States v. Richards*, 301 F. App'x 480, 483 (6th Cir. 2008) ("the government's confirmation of prior knowledge learned by the private individuals does not constitute exceeding the scope of a private search.").

Importantly, Defendant Miller does not question the reliability of hashing technology, and it appears well established that it is, in fact, reliable. *Ackerman*

---

[7] The *Lichtenberger* court further explained that when the item searched is an electronic device, the privacy interests at stake are increased because of the amount of information that is stored in such devices. *Lichtenberger,* 786 F.3d at 488. The court found that given the amount of data that can be stored in a laptop, "'there was absolutely no virtual certainty that the search of [defendant's] laptop would have' revealed only what Officer Huston had already been told." *Id*.

contains language, albeit *in dicta,* indicating the reliability of hash value matching, stating it is "unlikely if not impossible" that a hash value match could have proven a mistake. *Ackerman,* 831 F.3d at 1306 (citing Salgado, Fourth Amendment Search and the Power of the Hash, 119 Harv. L. Rev. F. 38, 45-46 (2005)). In *Ackerman*, the court explained hash values as "a short string of characters generated from a much larger string of data (say, an electronic image) using an algorithm–and calculated in a way that makes it highly unlikely another set of data will produce the same value. Some consider a hash value as a sort of digital fingerprint." *Id*. at 1294.

In addition, other courts, including our own, have found hash values to be highly reliable–akin to the reliability of DNA. *See United States v. Dunning*, No. 7:15-04-DCR, 2015 WL 5999818, at *3 (E.D. Ky. Oct. 15, 2015) (noting in a probable cause analysis that "as Magistrate Judge Atkins observed, hash values 'boast a reliability and accuracy akin to DNA: 99.99%.'") (citing *United States v. Wellman*, 663 F.3d 224, 226 n.2 (4th Cir. 2011) (also citing the 99.99% probability statistic); *see also United States v. Cartier*, 543 F.3d 442, 446 (8th Cir. 2008)). The Federal Judicial Center, in a guide for federal judges, has defined "hash value" as follows:

> hash value: A unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. The most commonly used algorithms, known as MD5 and SHA, will generate numerical values so distinctive that the chance that any two data sets will have the same hash value, no matter how similar they appear, is

> less than one in one billion. "Hashing" is used to guarantee the authenticity of an original data set and can be used as a digital equivalent of the Bates stamp used in paper document production.

Barbara J. Rothstein et al., Managing Discovery of Electronic Information: A Pocket Guide for Judges 24 (Federal Judicial Center 2007).

> Even the court in *Keith* acknowledges the reliability of hashing technology, explaining:
>
> A hash value is an alphanumeric sequence that is unique to a specific digital file. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Consequently, once a file has been "hashed," a suspect copy can be determined to be identical to the original file if it has the same hash value as the original, and not to be identical if it has a different hash value.

*Keith*, 908 F. Supp. 2d at 36-37.

Given the function of the hash value, the *Keith* court's analogy of the hash value to the labels at issue in *Walter* seems misplaced. A label, such as those in *Walter,* is not mathematically derived, nor is it intended to have unique identification features that permit one to know with near certainty that a container containing the exact label will have identical contents to that of another containing the same label. Further, the content in labeled containers can be removed or altered without changing the label. A hash value, on the other hand, is derived from an algorithm and is a unique identifier that confirms that two digital files

are the same or different (often discussed as being similar to a digital fingerprint or DNA). *See supra*. In addition, changes to the contents of a digital file will change the hash value. Thus, a label, such as those at issue in *Walter*, is not only created differently than a hash value, but serves an entirely different purpose.

Instead of merely describing what may be in the attachments, Google's search of the attachments using hashing technology revealed they contained images that were duplicates of images a Google employee had previously identified as apparent child pornography. (R. 33-1, at 1 ¶ 4). Accordingly, when Detective Schihl opened and viewed the two images Google identified as matching the hash values of images it previously identified as apparent child pornography, he was virtually certain to view an exact duplicate of the original image and was merely confirming what Google had told him–that the attachments contained apparent child pornography. The virtual certainty that Detective Schihl would see only images of apparent child pornography is what distinguishes this case from *Walter*.

Similarly, *Lichtenberger* is also distinguishable on this basis. *Lichtenberger*, 786 F.3d 478 (6th Cir. 2015). In *Lichtenberger,* Defendant's girlfriend, without his permission, hacked into his laptop and found a number of images of child pornography. The girlfriend called the police and told them of the child pornography images she found. An officer came to the home and directed the girlfriend to access the laptop and open the files. She testified that she showed the officer a few pictures from the computer files she had found, but she was not sure if they were the same images she had seen in her original search. *Id.* at 481. The Sixth Circuit held the police officer's warrantless search of

defendant's laptop computer exceeded the scope of defendant's girlfriend's search because it was not virtually certain that the officer's review would be limited to the images the girlfriend had previously viewed.[8] *Id.* at 485-88. Specifically, the court noted:

> Considering the extent of information that can be stored on a laptop computer–a device with even greater capacity than the cell phones at issue in *Riley [v. California* ___ U.S. ___ , 134 S. Ct. 2473 (2014)]–the "virtual certainty" threshold in *Jacobsen* requires more than was present here. When Office Huston arrived, he asked Holmes to show him what she had found. While the government emphasizes that she showed Officer Huston only a handful of photographs, Holmes admitted during testimony that she could not recall if these were among the same photographs she had seen earlier because there were hundreds of photographs in the folders she had accessed. And Officer Holmes himself admitted that he may have asked Holmes to

---

[8] *Bowers* also supports the Court's finding. *Bowers*, 594 F.3d at 524-26. In *Bowers*, the boyfriend of defendant's roommate discovered a photo album containing what he believed to be child pornography in the defendant's bedroom. *Bowers*, 594 F.3d at 524. When the summoned authorities arrived at the defendant's home, his roommate directed them to the dining room table where they had placed the album. The agents opened the album to view the potentially incriminating evidence. *Id.* at 524-25. The Sixth Circuit upheld the search of the photo album by agents because the roommate had already described the contents of the album. *Id.* at 526. The agents therefore knew the album contained child pornography, "learn[ed] nothing that had not previously been learned during the private search," and "infringed no legitimate expectation of privacy." *Id.* (quoting *Jacobsen*, 466 U.S. at 120) (internal quotation marks omitted).

> open files other than those she had previously opened. As a result, not only was there no virtual certainty that Officer Huston's review was limited to the photographs from Holmes's earlier search, there was a very real possibility Officer Huston exceeded the scope of Holmes's search and that he could have discovered something else on Lichtenberger's laptop that was private, legal, and unrelated to the allegations prompting the search–precisely the sort of discovery the *Jacobsen* Court sought to avoid in articulating its beyond-the-scope test.
>
> All the photographs Holmes showed Officer Huston contained images of child pornography, but there was no virtual certainty that would be the case. The same folders–labeled with numbers, not words–could have contained, for example, explicit photos of Lichtenberger himself: legal, unrelated to the crime alleged, and the most private sort of images. Other documents, such as bank statements or personal communications, could also have been discovered among the photographs. So, too, could internet search histories containing anything from Lichtenberger's medical history to his choice of restaurant. The reality of modern data storage is that the possibilities are expansive.

*Lichtenberger*, 786 F.3d at 488-89.

Here, on the other hand, Defendant Miller does not dispute that only the two images Google's private search identified as matching previously tagged images of apparent child pornography were attached to the CyberTipline report. Thus, there was little to no possibility that Detective Schihl's review of the two

image files would reveal other information beyond what the private search revealed–the two image files contained images of apparent child pornography.

Further, Defendant's argument that the "virtual certainty" language in *Jacobsen* is not applicable because Detective Schihl did not "re-examine" the attachments but rather opened "an unopened virtual container" is not persuasive. (R. 37, at 2-6). The evidence establishes that Google used its digital or virtual eye to search the contents of Defendant's email account looking for images it had previously viewed and tagged as apparent child pornography. Once it located two images within Defendant's email account having hash values that matched images it had previously viewed and tagged as apparent child pornography, it knew from its electronic viewing or examination of the attachments that they contained apparent contraband. Accordingly, because hashing technology identifies files that are exact matches to images containing the same hash value, Google's private search of the attachments, using its digital or virtual eye, frustrated Defendant's expectation of privacy in those attachments. Simply put, Google's private search "compromised the integrity of the [attachments]." *Jacobsen*, 466 U.S. at 120 n.17. Therefore, contrary to Defendant's argument, the principles articulated in *Jacobsen* apply to determine whether Detective Schihl's actions exceeded the scope of Google's private search.

As discussed above, Detective Schihl's opening and viewing of the images Google's private search identified as having hash values that matched that of known images of apparent child pornography was virtually certain to reveal only the images Google previously viewed and tagged. As in *Jacobsen*, there was a

virtual certainty that nothing else of significance except suspected contraband, i.e. apparent child pornography, would be found in the attachments, and a manual inspection of the attachments would reveal nothing more than what Google's private search revealed– the attachments contained apparent child pornography.[9] Therefore, Detective Schihl's opening and viewing of the attachments to confirm Google's report of apparent child pornography falls within the private search doctrine, and no Fourth Amendment violation occurred. *See Jacobsen*, 466 U.S. at 115; *Lichtenberger*, 786 F.3d at 485-86; *Bowers*, 594 F.3d at 524-26.[10]

---

[9] As the Government notes, while the possibility exists that Google erred in its original determination that these images constituted child pornography, that possibility is no greater than any other circumstance where a private person reports apparent child pornography. *Cf. Bowers*, 594 F.3d at 526 ("based on the [roommate's] statements that the album contained child pornography, the agents were justified in opening the album to view the potentially incriminating evidence. . . . In doing so, the agents 'learn[ed] nothing that had not previously been learned during the private search' and 'infringed no legitimate expectation of privacy.'") (quoting *Jacobsen*, 466 U.S. at 120).

[10] Defendant also briefly argues in Reply that while the Government suggests Detective Schihl's opening of the two email attachments was not a physical trespass, his conduct does, in fact, constitute a search under the traditional trespass test. (R. 37, at 9) (citing *Ackerman*, 831 F.3d at 1308) (citing *United States v. Jones*, 565 U.S. 400 (2012)). Defendant specifically references the finding in *Ackerman* that NCMEC's opening of the email and its attachments in that case constituted a search under both the reasonable expectation of privacy test discussed by the Supreme Court in *Jacobsen*, *Walter* and *Katz v. United States*, 389 U.S. 347 (1967) and the traditional trespass test discussed in *Jones*. However, *Jones* and *Ackerman* are distinguishable from this case. *Jones* did not involve the application of the private search doctrine; and *Ackerman* involved a finding that the Government

## III.Conclusion and Recommendation

Google's use of its hashing technology to search Defendant's email account does not implicate the Fourth Amendment because it was a private search. Further, Detective Schihl's actions of opening the email attachments did not exceed the scope of Google's private search because it was virtually certain his actions would reveal nothing more than already reported by Google–that the images were apparent child pornography.

Accordingly, **IT IS RECOMMENDED** that Defendant's Motion to Suppress (R. 27) be **DENIED.**

Specific objections to this Report and Recommendation must be filed within **fourteen (14) days** of the date of service or further appeal is waived. 28 U.S.C. § 636(b)(1)(C); Fed. R. Crim. P. 59(b)(2); *Thomas v. Arn*, 728 F.2d 813, 815 (6th Cir. 1984), *aff'd*, 474 U.S. 140 (1985); *United States v. Walters*, 638 F.2d 947 (6th Cir. 1981).

Dated this 19th day of May, 2017.

---

exceeded the scope of AOL's private search by opening the email and all four attachments, not just the one attachment with the hash value match. As discussed above, the Fourth Amendment only prohibits governmental action; it is 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 (quoting *Walter*, 447 U.S. at 662) (Blackmun, J., dissenting). Given the Court's finding that the private search doctrine is applicable to the case at bar and the lack of any appreciable development of a trespass argument by Defendant, this argument will not be considered further.

**Signed By:**

***Candace J. Smith*** **CJS**

**United States Magistrate Judge**