RECOMMENDED FOR PUBLICATION
Pursuant to Sixth Circuit I.O.P. 32.1(b)

File Name: 20a0376p.06

UNITED STATES COURT OF APPEALS

FOR THE SIXTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

WILLIAM J. MILLER,

Defendant-Appellant.

No. 18-5578

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

Argued: December 11, 2019

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 hash-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 Detective 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. Ultimately, 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.