FILED
United States Court of Appeals
Tenth Circuit

February 20, 2024

Christopher M. Wolpert
Clerk of Court

PUBLISH

UNITED STATES COURT OF APPEALS

FOR THE TENTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

v.

DONALD ALVIN TOLBERT,

Defendant - Appellant.

No. 22-2085

Appeal from the United States District Court
for the District of New Mexico
(D.C. No. 1:14-CR-03761-JCH-1)

Todd B. Hotchkiss, Albuquerque, New Mexico, for Defendant-Appellant Donald Alvin Tolbert.

Alexander M.M. Uballez, U.S. Attorney, and Kristopher N. Houghton, Assistant U.S. Attorney (with him on the brief), Albuquerque, New Mexico, for Plaintiff-Appellee United States of America.

Before **HARTZ**, **EBEL**, and **CARSON**, Circuit Judges.

EBEL, Circuit Judge.

In this direct criminal appeal, Defendant Donald Alvin Tolbert challenges the district court's denial of his motion to suppress. In 2012, Tolbert sent seven emails

with attachments containing child pornography using three different America Online (AOL) accounts. AOL used software to screen these emails which detected suspected child pornography, so AOL submitted the emails and attachments, along with other information about the incident, in CyberTips to the National Center for Missing and Exploited Children (NCMEC). NCMEC analysts opened the emails and attachments and determined they likely contained child pornography. After further investigation by law enforcement—first by the state of New Mexico, then the federal government—Tolbert was charged with, and pled guilty to, receipt, distribution, and possession of child pornography, as well as committing a felony while registered as a sex offender. Before pleading guilty, Tolbert moved to suppress the evidence obtained as a result of NCMEC opening his emails and attachments. The district court denied that motion and Tolbert's subsequent motion to reconsider. Tolbert now appeals those decisions.

We conclude that the inevitable discovery exception to exclusion applies, and therefore we need not address whether NCMEC violated the Fourth Amendment by opening Tolbert's emails and attachments or whether the good faith exception to exclusion would apply. The evidence before the district court established by a preponderance of the evidence that the investigation into the CyberTips would inevitably have proceeded in the same manner even if the emails and attachments had not been opened by NCMEC. Based on the routine practices of analysts at NCMEC and the New Mexico Attorney General's Office (NMAGO), Internet Crimes Against Children (ICAC) division, we conclude, even if the emails and attachments had not

been opened, those agencies would have investigated the CyberTips using information unrelated to the examination of the emails and attachments—such as IP addresses and email addresses—to link the CyberTips to Tolbert at two addresses in Albuquerque, New Mexico, and to find other evidence which raised suspicion of child pornography. It was routine practice for NCMEC analysts to report such tips to law enforcement, which, in this case, led the tips to agents at NMAGO and Homeland Security Investigations (HSI). These agents used the information from the investigation, which was largely developed through open-source searches on public databases, to obtain search warrants. These warrants would have been obtained during the ongoing investigation even if the challenged emails and attachments had not been opened—as evinced by the fact that police later obtained a search warrant for computers used by Tolbert, without relying on the contents of the emails and attachments.

Therefore, we conclude that the government has established by a preponderance of the evidence that the evidence against Tolbert inevitably would have been discovered even if NCMEC had not opened Tolbert's emails and attachments without an authorizing warrant. Having jurisdiction under 28 U.S.C. § 1291, therefore, we AFFIRM the district court's denial of Tolbert's motion to suppress and motion to reconsider.

I. BACKGROUND[1]

a. The Investigation of Tolbert

Tolbert was convicted in 2006 in state court for criminal sexual contact of a child. He was released on probation and parole in 2009, reincarcerated after violating the terms of his probation and parole in 2010, then later released again on probation. Upon his second release, Tolbert agreed to various conditions as part of his probation. He was then a registered sex offender, which subjected him to further conditions. These conditions included: probation officers could visit his home or workplace at any time; probation officers could search him without a warrant if they reasonably suspected a probation violation; he had to provide his probation officer with his email addresses, usernames, and passwords; and any computer or electronic device used by Tolbert could be accessed and reviewed at any time for inappropriate content, including child pornography.

Between July and September 2012, Tolbert sent emails through three different accounts on America Online (AOL). AOL uses a system called "image detection filtering process" (IDFP) to detect suspected child pornography in users' emails. When emails are sent, AOL uses software to scan the emails and attachments and create a "hash value," or unique 32-character string of numbers and letters, for each photograph or video. AOL maintains a database of hash values generated from photographs or videos containing suspected child pornography, and it uses IDFP to

[1] These facts come from the district court's order denying Tolbert's motion to suppress. See (I R. 383-408).

detect emails with hash values matching those in its database. Utilizing this system, AOL detected suspected child pornography in seven emails sent by Tolbert.

For each email flagged through IDFP, AOL submitted the email and other information in a "CyberTip" to the National Center for Missing and Exploited Children (NCMEC).[2] The CyberTips included:

> (1) the email addresses of both the senders and the recipients of the emails,
> (2) the subjects of the emails, along with all of their attachments;
> (3) identification of the specific attachments which had been hash value matched as child pornography; and
> (4) the IP address corresponding to the email sender for all five emails.

(I R. 385). AOL's CyberTip process was automated, so no person at AOL viewed or opened the emails before the tips were submitted.[3] Additionally, AOL's software

---

[2] AOL was required by law to report the suspected child pornography to NCMEC. 18 U.S.C. § 2258A(a)(1)(A). NCMEC is a nonprofit entity endowed by statute with various law-enforcement-related duties. See 34 U.S.C. § 11293(b) (providing for funds to be granted annually to NCMEC to be used in various ways, including operating a tipline for reports of child pornography and reporting tips to law enforcement). NCMEC is statutorily authorized to receive and review child pornography, which allows NCMEC to fulfill its duty as a "clearinghouse" of child pornography tips. 18 U.S.C. § 2258A(a), (b)(4), (c).

We have held, in a case decided after the operative offense in this case, that the Fourth Amendment is implicated by NCMEC's conduct, either because NCMEC is a "governmental entity," or because it acts as the government's agent. United States v. Ackerman, 831 F.3d 1292, 1297, 1301 (10th Cir. 2016) ("Ackerman I"). In Ackerman I, we left open the question whether NCMEC's opening and viewing photos and videos constitutes a Fourth Amendment "search." Id. at 1304-05.

[3] The district court found that an AOL employee in fact opened and viewed the emails and attachments after AOL submitted the CyberTips. Tolbert argues there is no evidence to support this conclusion. Instead, the evidence before the district court merely established that it was AOL's general practice to open the emails after submitting CyberTips—not that the emails at issue here were actually opened by AOL. This fact does not affect our legal analysis in this case.

automatically prevented the emails from reaching the intended recipients, saved snapshots of the sender's account, and then terminated the sender's account.

AOL submitted the first CyberTip to NCMEC on July 18, 2012, which concerned a single email sent from the address "dat666@aol.com" with the affiliated username "Donnie T." (Id. at 385, 407). It submitted the second CyberTip on August 8, 2012, which concerned a single email from the address "abc123ddt@aol.com." (Id. at 407).[4] AOL then submitted CyberTips concerning five emails with fifteen total attachments sent on September 1 from the address "ddt123abc@aol.com." (Id. at 384). Three of the emails were sent to a separate address allegedly belonging to Tolbert, "donnieisagod@aol.com," while two were sent to an address not associated with Tolbert, "widd2703@web.de." (Id.).

On September 5, NCMEC, acting without a warrant, opened and viewed the five emails and respective attachments from September 1. By doing so, NCMEC determined the attachments appeared to contain child pornography. NCMEC then used information submitted by AOL in the CyberTips, such as the sender's IP address[5] and two of the email addresses—"ddt123abc@aol.com" (the sender's) and "donnieisagod@aol.com" (a

[4] It is not clear when NCMEC investigated the July 18 and August 8 CyberTips. Tolbert argues that these tips were not investigated by NCMEC until after the September emails were opened and confirmed to contain child pornography, and therefore the first two CyberTips were tainted by NCMEC's "search" of the September emails. The timing of the investigation of the July 18 and August 8 CyberTips does not affect our analysis, as we conclude that the investigations in this case would inevitably have proceeded in the same manner even if NCMEC never opened the emails in the September CyberTips.

[5] An IP address helps to identify the geographic location from which a computer accesses the internet. (I R. 385).

recipient's)—to search publicly available databases. These searches led NCMEC to discover the Albuquerque address of Margaret Tolbert—the Defendant's mother—and eventually to discover Tolbert's name, address, and date of birth.

After conducting its own investigations, NCMEC forwarded the tips, emails, attachments, and Tolbert's information to the New Mexico Attorney General's Office (NMAGO), Internet Crimes Against Children (ICAC) division. This division is the clearinghouse for CyberTips with a connection to New Mexico. An analyst at ICAC reviewed the CyberTips and images and searched open sources to determine that the sender's IP address was connected to a location in New Mexico. The analyst then referred this information to the Special Agent in Charge, who assigned the case to Special Agent Owen Pena at the NMAGO. Agent Pena conducted his own open-source searches to confirm the IP address was connected to a location in Albuquerque, New Mexico. He then used that information to obtain grand jury subpoenas duces tecum for information from CenturyLink regarding the IP address and from AOL regarding the two email addresses associated with Tolbert, "ddt123abc@aol.com" and "donnieisagod@aol.com." AOL provided information linking "donnieisagod@aol.com" with the name "Donald Tolbert" and an address in Albuquerque. CenturyLink provided information linking the IP address with the name "Margaret Tolbert" and an address in Albuquerque. Having connected the information in the CyberTips with Donald Tolbert, Agent Pena called Tolbert's probation officer and confirmed he was registered as a sex offender and on probation in New Mexico.

Through further investigation, Agent Pena found that an email address or the IP address in the CyberTips was associated with an account named "YUNGMUFFMAN" on IMGSRC, a Russian file uploading website. The account owner's name was listed as "Donnie," with the email address "ddt666abc@gmail.com." A statement on the account read, "I love girls between 8-15. Someone told on me got my other 2 email accounts cancelled. AOL has something that reads your emails." (Id. at 387-88) The account also contained pictures of young girls and naked adults.

Agent Pena met with Christina Altamirano, a Homeland Security Investigations (HSI) agent who specialized in internet crimes against children and sexual exploitation crimes, to review the evidence he had regarding Tolbert—information provided by CenturyLink, AOL, and NCMEC, including the emails and attachments. Agent Altamirano used this evidence to obtain search warrants for AOL regarding the "ddt123abc@aol.com" and "donnieisagod@aol.com" email addresses. Additionally, Agent Pena obtained warrants for Tolbert's residence and Tolbert's mother's residence. The AOL warrants contained subscriber information, IP addresses, and times and dates when the accounts were used. Police seized two computers from Tolbert's mother's residence, which were later examined and discovered to contain child pornography. Tolbert's mother told police that she and Tolbert were the only users of those computers.

After this court decided Ackerman I—which held that NCMEC is a "governmental entity" and subject to the requirements of the Fourth Amendment—police obtained a new search warrant for the computers without using the emails and

attachments. 831 F.3d at 1297. A subsequent search revealed child pornography on the computers.

On June 14, 2016, Tolbert was charged by superseding indictment with: notice and advertisement of child pornography in violation of 18 U.S.C. §§ 2251(d)(1)(A), (d)(2)(A), and (B), 2251(e), 2256, and 3359(e); receipt of child pornography in violation of 18 U.S.C. §§ 2252(a)(2), 2252(b)(1), and 2256; distribution of child pornography in violation of 18 U.S.C. §§ 2252(a)(2), 2252(b)(1), and 2256; possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(4)(B), 2252(b)(2), and 2256; and committing a felony while required to be registered as a sex offender in violation of 18 U.S.C. § 2260A.

b. Tolbert's Motion to Suppress

On October 27, 2017, Tolbert moved to suppress "any and all evidence obtained either directly or indirectly as a result of the illegal actions by NCMEC and law enforcement in the investigation of the emails and attachments involving email addresses 'ddt123abc@aol.com' and 'donnieisagod@aol.com' and any seizure of evidence related to or pursuant to those searches." (I R. 33). The district court held evidentiary hearings on the motion on April 24-25 and June 12, 2018.

The district court heard testimony from Gregory Phillips, who worked as a Senior Technical Security Investigator for AOL in 2012. Phillips explained AOL's use of IDFP: emails are scanned when sent, a unique hash value is created for images and videos, and the hash values of sent items are compared to the hash values in AOL's database of "apparent child pornography." (II R. 123-24, 128-29) (explaining when a sent item's hash

value matches a hash in the database, "[t]hat means that it is child pornography").[6] The database was created over years with hash values of images that were reviewed by graphics analysts at AOL and determined to be child pornography. Another AOL employee, Mark Ludlow, testified that the "ISP industry" has "come up collectively with a set of criterion (sic) that [it] use[s] to determine" if an image or video depicts child pornography, but that the determination has a "degree of subjectivity." (Id. at 398, 431). He testified that AOL's process of reviewing content and developing the database was not perfectly accurate, and he approximated that about eighty percent of images and videos in the database contained child pornography.[7]

John Shehan, the vice president of the Exploited Children's Division at NCMEC, testified about NCMEC's process regarding CyberTips. He testified that NCMEC analysts in 2012 had discretion when determining whether to conduct open-source searches using information in CyberTips. He also testified that when an IP address is included in a CyberTip, NCMEC analysts "try to use that information to help . . . determine a location." (Id. at 183). NCMEC makes every CyberTip available to law enforcement. If an IP address is included in a tip and NCMEC identifies the location of the reported activity, NCMEC sends that tip to the law enforcement agency responsible for that location. Shehan also testified about the specific process used by NCMEC with respect to the CyberTips at issue here: NCMEC analysts viewed the photo and video

[6] The second volume of the record is sealed.

[7] Ludlow was not responsible for reviewing images in 2012, and he was unfamiliar with the training received by those who reviewed images for AOL in 2012.

attachments, used publicly available sources to search the email addresses and discover information about Tolbert—including his address and registration as a sex offender in New Mexico—used publicly available sources to search the IP address, discovered the emails were likely sent from Albuquerque, New Mexico, and reported the information to law enforcement in New Mexico.

NMAGO ICAC Agent Pena testified about ICAC's practices regarding investigation of NCMEC CyberTips. When asked whether ICAC would have investigated the five September 1 CyberTips if they received "no information about NCMEC ever opening any image or the e-mail itself"—in other words, the tips would have indicated only that AOL identified a hash value match and provided the email addresses, IP address, and other header information—Pena answered affirmatively. (Id. at 347). He also testified that ICAC would have investigated the July 18 and August 8 CyberTips, even if the September 1 CyberTips did not exist and no photos or videos were opened. Agent Pena stated it is ICAC's current practice to pursue such tips, even when the photos and videos remain unopened. He testified that, now that it is known that NCMEC's conduct implicates the Fourth Amendment, if ICAC receives a tip with unopened photos or videos from NCMEC, ICAC obtains subpoenas and search warrants to authorize opening and viewing them. The district court found Agent Pena's testimony credible.

HSI Agent Altamirano testified about her process investigating the CyberTips. She testified that, if she had received the CyberTips without the information that the photos or videos had been opened—and even if she only received an IP address and

the fact that AOL identified a hash value match—HSI still would have investigated the tips.[8] When asked why, she stated:

> Because we are still required to investigate the case. So even if I just had an IP address and hash values, that is still enough for me to work with to continue on my case to get information from the Internet service provider for the IP address, it is still enough, you know, there is a hash value there so I just have some probable cause to believe that this person is either viewing or downloading child pornography, so I would continue to work my case from there.

(II R. 464).[9] Agent Altamirano then explained how she investigated the tips using the IP address and email addresses: she sought search warrants for AOL and CenturyLink regarding the email addresses and IP address in the tip; she received an Albuquerque address associated with the IP address from CenturyLink; she searched the address in a law enforcement database and found the names Margaret Tolbert and Donald Tolbert; and then she searched Donald Tolbert's name in a database and found his New Mexico criminal history and probation officer. The name "Donnie Tolbert" was also included in an attachment by NCMEC to the July 18 CyberTip, and Agent Altamirano testified that she used publicly available sources to search this name and to discover Tolbert was a registered sex offender in New Mexico—and would have done so even if the photos and videos had never been opened. Finally, Agent Altamirano testified that one of the tips she reviewed provided information about the "YUNGMUFFMAN" IMGSRC account, which she suspected could contain child pornography, and therefore she

---

[8] Agent Altamirano admitted that she had only ever received and investigated NCMEC tips where the photos and videos had previously been opened. (II R. 481).

[9] Agent Altamirano testified "[b]ased on training and experience" that an AOL hash value match indicates "child pornography or child erotica, known child exploitation evidence." (II R. 471).

investigated that account—and would have done so even if the photos and videos had never been opened. The district court found her testimony credible.

c. The district court's decisions

The district court denied Tolbert's motion to suppress. The district court did not initially decide whether NCMEC violated the Fourth Amendment by opening Tolbert's emails and attachments. Instead, the court concluded, "the evidence should not be suppressed because both the good faith and the inevitable discovery exceptions" to exclusion apply. (I R. 390).

Tolbert filed a motion to reconsider, which was denied by the district court. The court relied on the good faith exception to exclusion. The court also explained, in a footnote, that Tolbert lacked a reasonable expectation of privacy in his emails because he agreed to AOL's terms of service, which notified Tolbert that he was required to comply with the law and that AOL could take action to enforce those terms and report illegal activity to law enforcement. The court provided this as "an additional, alternate reason why Tolbert's motion to reconsider should be denied." (Id. at 448-49 n.3).

After the denial of his motions, Tolbert entered a conditional guilty plea, reserving his right to appeal the district court's denial of his motion to suppress and motion to reconsider. The district court sentenced Tolbert to 420 months in prison with 10 years of supervised release. Tolbert now appeals the denial of his motion to suppress and motion to reconsider.

II. STANDARD OF REVIEW

"When reviewing the district court's denial of a motion to suppress, we view the evidence in the light most favorable to the government and accept the district court's factual findings unless they are clearly erroneous." United States v. Grimmett, 439 F.3d 1263, 1268 (10th Cir. 2006). "We review legal questions de novo." United States v. Neugin, 958 F.3d 924, 929 (10th Cir. 2020).

III. DISCUSSION

Tolbert argues the district court erred in denying his motion to suppress because: 1. He had a reasonable expectation of privacy in his emails and attachments, and therefore the warrantless searches by NCMEC and law enforcement violated the Fourth Amendment; 2. The good faith exception to the exclusionary rule does not apply; and 3. The inevitable discovery exception to the exclusionary rule does not apply. We hold that the inevitable discovery exception applies, and therefore we need not address whether Tolbert had a reasonable expectation of privacy in his emails or whether the good faith exception applies.[10] The inevitable discovery

[10] The government argues Tolbert lacked a "reasonable expectation of privacy" in his emails, and therefore any access to his emails by NCMEC or law enforcement was not a "search" that implicated the Fourth Amendment. See Smith v. Maryland, 442 U.S. 735, 740 (1979) (explaining two-part inquiry to determine whether a Fourth Amendment "search" occurred: whether an individual has a subjective expectation of privacy in the thing searched; and whether that expectation is objectively reasonable) (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

First, the government argues Tolbert lacked a subjective expectation of privacy in his AOL emails, as he posted on his IMGSRC account, "[s]omeone told on me got my other 2 email accounts cancelled. AOL has something that reads your emails." (I R. 387-88). Second, the government argues any expectation of privacy would be objectively unreasonable because AOL's terms of service put Tolbert on notice that users could not

analysis that follows simply assumes, without deciding, that Tolbert's constitutional rights were violated.

a. Legal Standard

"Subject to a few exceptions, evidence obtained in violation of the Fourth Amendment will be suppressed under the exclusionary rule." United States v. Christy, 739 F.3d 534, 540 (10th Cir. 2014). However, under the inevitable discovery exception to exclusion, "illegally obtained evidence may be admitted if it 'ultimately or inevitably would have been discovered by lawful means.'" Id. (citing Nix v. Williams, 467 U.S. 431, 444 (1984) ("If the prosecution can establish . . . that the information ultimately or inevitably would have been discovered by lawful means . . . then the deterrence rationale has so little basis that the evidence should be received")). "The government bears the burden of proving by a preponderance of the evidence that the evidence would have been discovered without the Fourth Amendment violation." Id.

> Inevitable discovery analysis . . . requires the court to examine each of the contingencies involved that would have had to have been resolved favorably to the government in order for the evidence to have been discovered legally and to assess the probability of the contingencies having occurred. . . The more contingencies there are, and the lower the probability that each would have been resolved in the government's favor, the lower the probability that the evidence would have been found by lawful means.

---

use their email accounts for illegal purposes, that AOL could access and disclose the contents of a user's communications when AOL developed a "good faith belief" that the user was engaging in illegal activity, and that AOL would report illegal activity to law enforcement. (I R. 202-03). We need not resolve this issue here.

United States v. Souza, 223 F.3d 1197, 1205 (10th Cir. 2000).

While we have expressed "reluctan[ce] to apply the inevitable discovery exception in situations where the government fails to obtain a search warrant and no exception to the warrant requirement exists," we will apply the exception where "demonstrated historical facts" indicate "that an independent and untainted discovery would inevitably have occurred." Id. at 1206; United States v. Griffin, 48 F.3d 1147, 1151 (10th Cir. 1995) (quoting United States v. Terzado-Madruga, 897 F.2d 1099, 1114 (11th Cir. 1990) (citation omitted)). The government need not prove the existence of a second, distinct investigation that would have discovered the evidence absent the Fourth Amendment violation—it is sufficient to establish that "the first (and only) investigation would inevitably have discovered the contested evidence by lawful means." Christy, 739 F.3d at 541.

Where application of the inevitable discovery exception depends on whether an investigation would have continued if a prior unlawful search had not occurred, we have looked at whether the evidence establishes a routine practice of conducting such investigations under the circumstances. See United States v. White, 326 F.3d 1135, 1139 (10th Cir. 2003) (applying inevitable discovery exception where evidence established that it was officers' routine practice to check for outstanding warrants, and therefore officers would have run a warrant check even if they had not conducted the unlawful search and discovered illegal drugs before the check); see United States v. Cooper, 24 F.4th 1086, 1094 (6th Cir. 2022) (stating that the court will apply inevitable discovery exception based on "routine practices: that an airline would,

pursuant to its official policy, open the defendant's lost luggage . . . ; that police would follow standard procedure to inventory a vehicle before having it towed . . . ; or that upon arresting a suspect, police would routinely search his person, . . . or ask for his name" (citations omitted)).

b. Analysis

As noted previously, we assume without deciding that NCMEC violated the Fourth Amendment when its analyst opened Tolbert's emails and attachments without a warrant. Therefore, the emails, attachments, and evidence gathered as a result of their being viewed by NCMEC—including the computers seized from Tolbert's mother's home which contained child pornography—must be excluded unless an exception to exclusion applies.[11] We agree with the district court that the government has carried its burden to establish by a preponderance of the evidence that the challenged evidence would have been discovered absent the Fourth Amendment violation—and therefore the inevitable discovery exception to exclusion applies.

First, the government established that NCMEC would have investigated the information in the September 1 CyberTips from AOL, even if the accompanying emails and attachments were never opened. Shehan's testimony established it was routine

[11] Tolbert argues, "[e]verything that followed the search" of his emails and attachments "was undertaken only because of the illegal searches by NCMEC," and therefore all subsequently obtained evidence is "fruit of the poisonous tree" and must be excluded. (Aplt. Br. 42) (citing Wong Sun v. United States, 371 U.S. 471, 488 (1963)). Because we conclude that all challenged evidence would inevitably have been discovered without the allegedly unlawful "searches," we need not further address this argument.

practice for NCMEC analysts to use IP addresses in CyberTips to conduct open-source searches and attempt to "determine a location." (II R. 183). The September 1 CyberTips contained the IP address corresponding to the sender of the five reported emails. Therefore, based on Shehan's testimony, NCMEC analysts would have conducted open-source searches of the IP address to determine a corresponding geographic location, even if the emails and attachments were not opened. In fact, that happened in this case—NCMEC analysts conducted open-source searches of the IP address and discovered the corresponding geographic location of Albuquerque, New Mexico.

Additionally, Shehan testified, so long as time permits, NCMEC analysts run open-source searches of the email addresses and other information provided in CyberTips. (II R. 226-27) ("Certainly [the analysts] are always going to focus on more of the user or the person that's being reported."). The emails in the September 1 CyberTips were sent from the email address, "ddt123abc@aol.com." NCMEC analysts conducted open-source searches of this email address and discovered the suspicious "YUNGMUFFMAN" IMGSCR account, which included the name "Donnie" and the statement, "I love girls between 8-15." Open-source searches also led NCMEC to the name "Don Tolbert," which an analyst used to search a national sex offender public website.

Shehan testified that NCMEC makes all CyberTips available to law enforcement and, when NCMEC analysts can use an IP address to identify the geographic location of the reported activity, NCMEC sends those tips to law enforcement in the respective jurisdiction. NMAGO ICAC is the agency where

NCMEC sends tips with a connection to New Mexico. Here, since NCMEC was able to locate the IP address in Albuquerque, New Mexico, NCMEC sent the September 1 CyberTips, emails, attachments, and related information to NMAGO ICAC. Ultimately, NCMEC's routine practices of using IP addresses in CyberTips to determine a geographic location, conducting open-source searches of other information in CyberTips when time permitted, and forwarding tips and information with a connection to New Mexico to NMAGO ICAC are sufficient to establish by a preponderance of the evidence that NCMEC would have investigated the September 1 CyberTips and sent them to NMAGO ICAC, even if NCMEC never opened the emails and attachments.

Tolbert argues NCMEC analysts had discretion when determining whether to investigate the information in CyberTips, and it is impossible to know whether the analysts here would have exercised their discretion to investigate the September 1 CyberTips if they had not first opened the emails and attachments and confirmed they contained suspected child pornography. Therefore, in Tolbert's view, the conclusion that NCMEC would inevitably have investigated the CyberTips and reported them to NMAGO ICAC is too speculative to support the inevitable discovery exception. See United States v. Owens, 782 F.2d 146, 152 (10th Cir. 1986) (refusing to apply inevitable discovery exception "because of the highly speculative assumption of 'inevitability' that would be required"). While the inevitable discovery exception would be inapplicable if we had no insight into how NCMEC analysts exercised their discretion when investigating tips, there was evidence before the district court here that, in 2012, it

was the practice of NCMEC analysts to run open-source searches for all CyberTips—especially when those tips included an IP address.[12] Therefore, we disagree—it is not "highly speculative" to conclude that NCMEC analysts would have followed routine practice and conducted open-source searches of the information in the September 1 CyberTips, even if they had not opened the emails and attachments. See White, 326 F.3d at 1139 (applying inevitable discovery exception where district court found it unclear whether officers would have checked defendant's name for warrants, but evidence created a "solid implication that the officers routinely ran" such checks).

Further, the government established that NMAGO ICAC would have investigated the information provided by NCMEC relating to the September 1 CyberTips—even if the emails and attachments were never opened by anyone at NCMEC or ICAC. Agent Pena testified that ICAC would have investigated the information in the September 1 tips based solely on the fact that AOL found a hash value match. He testified that this is ICAC's current practice—after Ackerman I, neither NCMEC or ICAC opens photos or videos without a warrant, yet ICAC

[12] See (II R. 168-69) (Question: "Back in 2012, was it the practice then for analysts to be able to perform if the information is there for them to use open source queries and the like on every case that came through"; Answer: "Yes. Generally speaking they should have the time during that period to have been able to do that. They certainly were given discretion to make those decisions on when they wanted to conduct those types of queries, but yes, time was much more affordable [to investigate tips] then compared to now."); see also (II R. 183) ("So if there is an IP address we are going to try to use that information to help us determine a location.").

continues to investigate tips from NCMEC—even when no one has opened the photos or videos.[13]

We conclude that the government has established by a preponderance of the evidence that ICAC would have conducted the same investigation of the September 1 tips if the emails and attachments were never opened: an ICAC analyst reviewed the information from NCMEC and ran open-source searches of the IP address to confirm the emails were sent from New Mexico; the analyst referred the tips to the Special Agent in Charge, who then assigned the case to Agent Pena; Agent Pena used the IP address and email addresses in the tips to conduct open-source searches and determine a geographical connection to Albuquerque, New Mexico; Agent Pena used this information to obtain grand jury subpoenas duces tecum for information from CenturyLink and AOL, which revealed information linking one of the email addresses with "Donald Tolbert" at an address in Albuquerque, New Mexico, and linking the IP address with "Margaret Tolbert" at a different Albuquerque address; and Agent Pena, having discovered Tolbert's name, called Tolbert's probation officer and confirmed he was registered as a sex offender and on probation in New Mexico. This investigation relied entirely on information unrelated to the contents of the emails and attachments, and Agent Pena's testimony indicates that this investigation

[13] If previously opened by a private party, such as AOL, then it is NCMEC's practice to open images and videos. The Supreme Court has held that a warrantless "search" does not violate the Fourth Amendment when it merely reveals the same information previously discovered by a private party's search. United States v. Jacobsen, 466 U.S. 109, 119-20 (1984).

would have been pursued in the same manner if the emails and attachments had never been opened. The district court concluded, at this point, "NMAGO would have had ample evidence to support probable cause for a search warrant to open the emails and their attachments." (I R. 406). Agent Pena then used the information developed through this investigation to obtain search warrants for the residences of Tolbert and his mother.[14]

---

[14] Tolbert argues that, without all the evidence tainted by NCMEC's initial "search," there was insufficient evidence to support probable cause for the search warrants. He argues that there was no evidence before the district court establishing the reliability of AOL's hash value match. We reject this argument for three reasons.

First, as described throughout our analysis, the investigations by NCMEC and ICAC relied almost entirely on publicly available sources, and therefore the evidence supporting probable cause would have been discovered if the emails and attachments were not opened. There was ample evidence supporting probable cause, even after NCMEC's open-source investigations, such as Tolbert's name, which was searched and led to a "hit" on the national sex offender public website, Tolbert's Albuquerque address, a connection between the sender's IP address and Albuquerque, and the suspicious "YUNGMUFFMAN" IMGSRC account.

Second, there was evidence before the district court supporting the proposition that an AOL hash value match supports probable cause of child pornography: two AOL employees testified about the process used by AOL to build a database of suspected child pornography and detect hash value matches; AOL employee Ludlow testified that AOL employees used criteria developed by the ISP industry to identify suspected child pornography and add it to the database; and HSI Agent Altamirano testified based on training and experience that hash value matches indicated child pornography.

Third, after the search warrants were executed on the residences of Tolbert and his mother, we decided Ackerman I, which held that NCMEC is a government entity to which the Fourth Amendment applies. Ackerman I, 831 F.3d at 1297, 1301. Police had seized two computers from Tolbert's mother's residence. Given our decision in Ackerman I, police sought a new warrant to search the seized computers without reference to the contents of the opened emails and attachments. Police obtained the warrant and searched the computers, which revealed evidence of child pornography. This post-Ackerman I warrant supports our conclusion that Agent Pena could have, and would have, sought and obtained the search warrants in this case, even if the emails and attachments were not opened.

Tolbert argues that the conclusion that ICAC would have conducted the same investigation if the emails and attachments remained unopened is too speculative. He supports this argument by pointing to Agent Pena's testimony that the ICAC analyst who first investigated the tips from NCMEC had the power to decide whether an investigation should be "closed out." (II R. 313). Therefore, Tolbert suggests, it is impossible to know whether the analyst would have exercised his discretion to close out the investigation if no one had opened the emails and attachments. We reject this argument. Agent Pena testified that the analyst could not decide to withhold a tip from ICAC's investigation process—every tip had to be reported to the Special Agent in Charge. This testimony supports the conclusion that ICAC's investigation would have proceeded in the same manner if the emails and attachments were never opened.[15]

Tolbert also argues there is evidence that undermines the conclusion Agent Pena would have pursued the subpoenas duces tecum for information from CenturyLink and AOL if the emails and attachments were not opened—Agent Pena testified that opening the emails and attachments "was the crux for the subpoena."

---

[15] The government argues that Agent Pena's statement that the analyst could "close out" an investigation was taken out of context by Tolbert. While one of Agent Pena's statements does seem to suggest the analyst could "close out" an investigation, Agent Pena also testified that all tips had to go through the Special Agent in Charge, and that certain cases—involving registered sex offenders and juvenile victims—were given high priority by the analyst and reported to the Special Agent in Charge more quickly than other cases. Crucially, when asked specifically whether an analyst could decide "not to put a cyber tip through the [ICAC's investigative] process," Agent Pena stated, "[n]o, he cannot. Everything has to go through [the] Special Agent in Charge." (II R. 315-16).

(II R. 365). We reject this argument. Agent Pena testified that, had he only received from NCMEC the header information and the fact that AOL found a hash value match—and had no one at NCMEC or ICAC opened the emails and attachments—he still would have sought the subpoenas duces tecum to receive information from CenturyLink and AOL. He then would have used this information to obtain a search warrant to open the emails and attachments. Agent Pena testified that this is ICAC's current practice—obtaining subpoenas to gather information to support probable cause, then obtaining search warrants to authorize opening photos and videos. Therefore, Agent Pena's above statement does not undermine our conclusion that he would have obtained the subpoenas and continued his investigation if no one had opened the emails and attachments.

The government also established that HSI Agent Altamirano would have investigated the September 1 tips and obtained search warrants for the two AOL email addresses in the September 1 tips, even if the emails and attachments had never been opened. Agent Pena provided Agent Altamirano with information regarding the September 1 tips—including the names and addresses provided by CenturyLink and AOL in response to the subpoenas. Agent Altamirano testified that if she had only been given the IP address and the fact that AOL found a hash value match, she would have investigated the tips and sought search warrants "[b]ecause [HSI is] still required to investigate the case." (II R. 464). Also, as described above, the district court concluded that the information obtained through NCMEC's and ICAC's open-source investigations supported probable cause for a warrant to open the emails and attachments,

and the post-Ackerman I warrant—which did not rely on the contents of the emails and attachments—supports this conclusion. Therefore, even if the emails and attachments had not been opened by the time the tips reached Agent Altamirano, the evidence before the district court established that Agent Altamirano would still have pursued the investigation and obtained the search warrants.

Finally, Tolbert argues that there is insufficient evidence to support the conclusion that NCMEC, NMAGO ICAC, and HSI would have conducted the same investigation if the emails and attachments were not opened because the district court did not hear testimony from: the AOL employees who allegedly opened the emails and attachments after the CyberTips were sent to NCMEC; any of the NCMEC analysts who reviewed and investigated the CyberTips; and the NMAGO ICAC analyst who reviewed and investigated the tips. Instead, the district court relied on testimony from AOL employees who were not directly involved with the case, a vice president at NCMEC who did not directly investigate the CyberTips at issue here, and NMAGO Agent Pena, who did not receive the tips until after the ICAC analyst finished his investigation. This testimony, Tolbert argues, cannot support a conclusion that the individuals who investigated the CyberTips inevitably would have pursued the investigation in the same manner if the emails and attachments were not opened—in other words, Tolbert argues testimony from each link in the investigative chain was required. (Aplt. Br. 52) ("Given that the specific identifiable NCMEC analyst did not testify for each cyber tip, . . . there is no probable way to establish inevitability.").

We reject this argument. As described above, the evidence before the district court was sufficient to establish NCMEC analysts routinely used IP addresses in CyberTips to identify a location and send the tips to the corresponding law enforcement agency, and the ICAC analyst routinely reported all cases to the Special Agent in Charge. This was sufficient to establish by a preponderance of the evidence that the investigation would have proceeded in the same manner if the emails and attachments were not opened. Testimony from every link in the investigative chain is not required—we can instead infer that the individuals involved in the investigations at issue here would have acted consistent with their agencies' routine practices. See White, 326 F.3d at 1139 (applying inevitable discovery exception based on evidence of routine practice); United States v. Larsen, 127 F.3d 984, 985-86 (10th Cir. 1997) (relying on testimony by FBI agent that FDIC reports were routinely forwarded to the FBI and the FDIC report would have been sent to him in that case to support finding of inevitable discovery).

IV. CONCLUSION

We conclude that the inevitable discovery exception to exclusion applies to all evidence obtained through investigations by NCMEC, NMAGO ICAC, HSI, and the search warrants executed on Tolbert's residence, his mother's residence, and AOL.[16]

[16] Tolbert also argues that the "totality of the circumstances" and "special needs" exceptions to exclusion do not apply. (Aplt. Br. 68-71). Neither the government nor the district court relied on these exceptions, and, given our conclusion that the inevitable discovery exception applies, we need not address these other arguments.

We need not rely on speculation to reach this conclusion—we instead rely on the evidence before the district court establishing that, even if the emails and attachments in the September 1 CyberTips were never opened without a warrant, the routine practices of NCMEC, ICAC, and HSI would have led all of these agencies to conduct the same investigation, and gather the same evidence, that occurred in this case. Our precedents support reliance on routine practice when applying the inevitable discovery exception. See White, 326 F.3d at 1139; Larsen, 127 F.3d at 985-86. Therefore, we AFFIRM the district court's denial of Tolbert's motion to suppress and motion to reconsider.