FILED
United States Court of Appeals
Tenth Circuit

May 12, 2025

Christopher M. Wolpert
Clerk of Court

PUBLISH

UNITED STATES COURT OF APPEALS

FOR THE TENTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

v.

GUY ROSENSCHEIN,

Defendant - Appellant.

No. 23-2017

Appeal from the United States District Court
for the District of New Mexico
(D.C. No. 1:16-CR-04571-JCH-1)

Submitted on the briefs:*

Guy R. Rosenschein, New Mexico, pro se Defendant-Appellant.

Alexander M.M. Uballez, United States Attorney, and Tiffany L. Walters, Assistant United States Attorney, Albuquerque, New Mexico, for Plaintiff-Appellee.

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

EID, Circuit Judge.

---

* After examining the briefs and appellate record, this panel has determined unanimously that oral argument would not materially assist in the determination of this appeal. *See* Fed. R. App. P. 34(a)(2); 10th Cir. R. 34.1(G). The case is therefore ordered submitted without oral argument.

In 2016, an anonymous user uploaded images of child pornography to Chatstep, an internet chatroom service. Using a Microsoft product called PhotoDNA, Chatstep identified and reported the uploads to the National Center for Missing & Exploited Children ("NCMEC"). Based on location data derived from the IP address accompanying the files, NCMEC forwarded the reports to the Bernalillo County Sheriff's Office ("BCSO") in New Mexico. BCSO investigated the reports, identified the user as Guy Rosenschein, and obtained a warrant to search Rosenschein's home in Albuquerque. The search uncovered approximately 21,000 images and videos of child pornography on electronic devices in Rosenschein's possession.

A grand jury indicted Rosenschein on charges of possession and distribution of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2), 2252A(a)(5)(B), 2252A(b)(1), and 2256. Rosenschein filed three pre-trial motions in response. First, Rosenschein moved to suppress the evidence of his uploads, arguing that Chatstep's warrantless search of his files through PhotoDNA violated the Fourth Amendment. He also claimed that, as a result of that unlawful search, any evidence of child pornography found in his home should be suppressed under the exclusionary rule. Second, Rosenschein moved to dismiss the case, or, in the alternative, to compel the discovery of the computer programs used by Microsoft and NCMEC to generate reports of child pornography. And third, Rosenschein moved to compel the government to require expert reports for two of its witnesses before the suppression hearing.

The district court denied each of Rosenschein's motions. Rosenschein subsequently pleaded guilty to one count of possession of child pornography and seven counts of distribution of child pornography, reserving his right to appeal the district court's decision to deny his motions.

Exercising jurisdiction under 28 U.S.C. § 1291, we affirm the district court's denial of all three motions. First, because Chatstep and Microsoft were not acting as governmental agents, the Fourth Amendment does not protect Rosenschein from their conduct. Further, even if Chatstep and Microsoft were governmental agents, Rosenschein's Fourth Amendment claim fails because he had no reasonable expectation of privacy in images he uploaded to a reportable internet chatroom with strangers. Second, the district court did not abuse its discretion in denying Rosenschein's motion to require production of NCMEC's reporting system because Rosenschein had the opportunity to access that information through the examination of witnesses. Finally, the district court did not abuse its discretion in refusing to require expert reports for the government's witnesses because Rosenschein conceded that Federal Rule of Criminal Procedure 16(a)(1)(G)—which generally requires the government to produce expert reports for witnesses it intends to call during its case-in-chief—does not apply to suppression hearings.

I.

As part of its efforts to combat child victimization, NCMEC operates the CyberTipline, which functions as a "national online clearinghouse for tips and leads about child exploitation." Supp. R. Vol. IV at 71. Federal law requires electronic

service providers ("ESPs") to report to NCMEC any apparent child pornography of which they are aware. 18 U.S.C. §§ 2258A(a)(1), (f). It does not, however, compel ESPs to affirmatively search for child pornography. *Id.*

In July and August of 2016, Chatstep submitted two CyberTipline reports to NCMEC after detecting several uploads of pornographic images by a user named "Carlo." Chatstep uses a Microsoft program called PhotoDNA to scan the "hash values" of suspect files on its site and compare them to the list of hash values of known child pornography images already in circulation.[1] A "hash match" occurs when an uploaded image's hash value matches the hash value of a known image of child pornography.

Each of Chatstep's reports included the uploaded image and the IP address of the user. NCMEC investigated the reports and traced the IP address to a computer in Albuquerque, New Mexico, with CenturyLink as its internet service provider. NCMEC referred the information to the Internet Crimes Against Children ("ICAC") Task Force at the Office of the New Mexico Attorney General, which obtained grand jury subpoenas for CenturyLink. CenturyLink identified "rosenscheinguy" as the

[1] A "hash value" is "a short string of characters generated from a much larger string of data (say, an electronic image) using an algorithm—and calculated in a way that makes it highly unlikely another set of data will produce the same value." *United States v. Ackerman*, 831 F.3d 1292, 1294 (10th Cir. 2016). "Hash values have been used to fight child pornography distribution, by comparing the hash values of suspect files against a list of the hash values of known child pornography images currently in circulation." *United States v. Reddick*, 900 F.3d 636, 637 (5th Cir. 2018). "This process allows potential child pornography images to be identified rapidly, without the need to involve human investigators at every stage." *Id.*

subscriber for the IP address and gave ICAC the physical address associated with the account. BCSO obtained and executed a search warrant for Rosenschein's residence and recovered a thumb drive containing child pornography. The execution of subsequent search warrants at Rosenschein's home revealed several additional devices containing evidence of possession and distribution of child pornography. In total, law enforcement discovered devices containing over 19,000 images and 2,000 videos of child pornography.

Rosenschein was indicted by a grand jury for possession and distribution of child pornography in violation of 18 U.S.C. §§ 2252A(a)(2), 2252A(a)(5)(B), 2252A(b)(1), and 2256. Rosenschein moved to suppress all the evidence of child pornography. He alleged that Microsoft and Chatstep were acting as agents for NCMEC—and thus agents for the government, *see United States v. Ackerman*, 831 F.3d 1292, 1295–304 (10th Cir. 2016)—when they created and used PhotoDNA to scan the images uploaded to Chatstep without a warrant.

Rosenschein also moved to suppress the evidence under *Franks v. Delaware*, 438 U.S. 154 (1978). He argued that the search warrant affidavit contained materially false or misleading statements and omitted information intentionally or with reckless disregard for the truth. He further claimed that, without these false statements and omissions, the warrant to search his home could not have lawfully issued.

Beyond his suppression motion, Rosenschein moved to compel discovery of the computer algorithm used by NCMEC for CyberTipline reports from ESPs. He

also framed this motion as a motion to dismiss the case based on failure to produce evidence. Finally, he moved to require the government to disclose expert reports for the Microsoft and NCMEC witnesses it planned to call at the suppression hearing.

The district court denied each of Rosenschein's motions. Under a Rule 11(c)(1)(C) plea agreement, Rosenschein pleaded guilty to seven counts of distribution and one count of possession of child pornography. Rosenschein reserved his right to appeal the denial of his suppression motions, his motion to dismiss the case or compel discovery, and his motion for expert reports. The district court sentenced Rosenschein to 210 months' imprisonment, and Rosenschein timely appealed.

II.

We begin by addressing the district court's denial of Rosenschein's suppression motions. Following the denial of a motion to suppress evidence, we review the district court's legal determinations de novo and its factual findings for clear error. *United States v. Muhtorov*, 20 F.4th 558, 592 (10th Cir. 2021). A district court's factual finding is made in clear error only if "the error [is] pellucid to any objective observer," the finding is "without factual support in the record," or the panel is "left with a definite and firm conviction that a mistake has been made." *United States v. Madrid*, 713 F.3d 1251, 1256–57 (10th Cir. 2013) (quotations omitted). In conducting this review, "we view the evidence in the light most favorable to the government." *Muhtorov*, 20 F.4th at 592 (quotation omitted).

A.

Rosenschein first argues that Microsoft and Chatstep violated his Fourth Amendment right to be free from unreasonable searches and seizures when they created and used PhotoDNA to search his Chatstep uploads without a warrant. We disagree. Because Microsoft and Chatstep were not acting as governmental agents, their actions cannot implicate the Fourth Amendment. And even if they were governmental agents, Rosenschein's claim fails because he had no reasonable expectation of privacy in images he uploaded to a reportable internet chatroom with strangers.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures[.]" U.S. Const. amend. IV. Its protections do not apply against "private individual[s] not acting as [] agent[s] of the [g]overnment or with the participation or knowledge of any governmental official." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (quotation omitted); *see United States v. Koerber*, 10 F.4th 1083, 1114 (10th Cir. 2021) ("Fourth Amendment concerns [] are not implicated when a private person voluntarily turns over property belonging to another and the government's direct or indirect participation is nonexistent or minor." (quotation omitted)). Accordingly, the first step in a Fourth Amendment search claim is to determine the extent of the government's involvement in the search.

To determine whether a private party is acting as a governmental agent, we employ a two-pronged inquiry. *United States v. Souza*, 223 F.3d 1197, 1201 (10th

Cir. 2001). First, we ask "whether the government knew of and acquiesced in the [party's] intrusive conduct[.]" *Id.* (quotation omitted). Second, we consider "whether the party performing the search intended to assist law enforcement efforts or to further his own ends." *Id.* (quotation omitted). "Both prongs must be satisfied considering the totality of the circumstances before the seemingly private search may be deemed a government search." *United States v. Poe*, 556 F.3d 1113, 1123 (10th Cir. 2009).

Here, neither Chatstep nor Microsoft was a governmental agent because each "acted to further [its] own ends." *Souza*, 223 F.3d at 1201 (quotation omitted). As the district court noted, Chatstep began monitoring its site for child pornography out of concern that the presence of child pornography would hurt the company's reputation, drive away users, and violate advertisers' policies. Chatstep independently turned to PhotoDNA to automate the monitoring of child pornography; it was not directed by a government entity to use that product. Instead, Chatstep found PhotoDNA after conducting a web search and applied twice before receiving approval to use the product.[2]

[2] Rosenschein claims NCMEC improperly coerced Chatstep into registering for the CyberTipline, thus making Chatstep a governmental agent. But even after receiving multiple emails from NCMEC about the program, Chatstep waited approximately one year to register. And though Rosenschein correctly notes that Chatstep went beyond its legal obligations to assist law enforcement, Chatstep provided several independent business reasons for doing so. *See, e.g.*, R. Vol. III at 615 (noting Chatstep's decision to cooperate with the government to receive "free moderation" of child pornography on the site); *id.* at 288, 368–70, 614 (noting that providing the government with direct access to logs saved Chatstep time). Put differently, Chatstep's decision to involve the government advanced an independent

Microsoft's sole tie to the Rosenschein investigation was its creation of PhotoDNA. But Microsoft's independent creation of a product that assists both private and public parties in combatting the distribution of child pornography does not transform it into a governmental agent. *See United States v. Alexander*, 447 F.3d 1290, 1297 (10th Cir. 2006) (noting that "an agency relationship does not develop where the government is an incidental beneficiary of another party's actions"). And here, the record contains ample evidence showing that Microsoft created PhotoDNA to advance its independent business interests. *See, e.g.*, R. Vol. III at 741–42 ("Protecting our brand and our reputation means reducing illegal and harmful activities on our services."); *id.* at 100–02 (noting that Microsoft creates similar services and offers them to third-party platforms as part of its "vision in protecting customers more broadly," "purg[ing] the ecosystem of explicit material[,] . . . [and making] it a better environment for [Microsoft] to operate in").[3]

---

interest because, as previously noted, child pornography negatively affected business. *See United States v. Rosenow*, 50 F.4th 715, 735 (9th Cir. 2022) ("[A] private party's otherwise legitimate, independent motivation is not rendered invalid just because law enforcement may further its interests.").

[3] Rosenschein also challenges the district court's exclusion of Exhibit AD, which consists of documents from *Soto v. Microsoft*, No. 16-2-31049-4 (Super. Ct. Wash. 2016), a civil case. He contends the court should have taken judicial notice of Microsoft's "Policy Overview"—which discusses changes in how Microsoft handled reports of child sexual abuse material on its private services—because that document "concern[ed] Microsoft's understanding of both being an agent of the state and how to take actions to better assist law enforcement during criminal prosecutions." R. Vol. II at 286. We conclude the district court did not abuse its discretion in denying Rosenschein's motion for three reasons: (1) the documents dealt with Microsoft's policies for *private* services, while this case concerns Microsoft's licensing of PhotoDNA for the public; (2) the documents did not bear a direct relation to Rosenschein's case and their accuracy can be reasonably questioned; and (3) in any

Rosenschein claims our decision in *Ackerman* requires us to conclude that Chatstep and Microsoft were governmental agents. There, we held that NCMEC acted as a governmental agent when it opened an email and four attachments forwarded by AOL through the CyberTipline. *Ackerman*, 831 F.3d at 1295–300. We further noted that it is a "misreading" of precedent to suggest that "a private party who bears *any* private purpose cannot serve as a governmental agent." *Id.* at 1303. But *Ackerman* provides little guidance to us here because the key facts that led us to determine that NCMEC was a governmental agent are absent in this case. Unlike NCMEC, which receives its funding from Congress for the purpose of stopping the spread of child pornography and seeks tips "precisely because (at least in part) it intends to aid law enforcement," *id.* at 1302, Congress has expressly stated that ESPs—such as Chatstep and Microsoft—need not affirmatively search for child pornography, 18 U.S.C. § 2258A(f). Instead, unlike NCMEC, both Chatstep and Microsoft acted to protect their legitimate private business interests. *Cf. United States v. Sykes*, 65 F.4th 867, 877 (6th Cir. 2023) (concluding that Facebook was not a governmental agent where its search was motivated by "an independent business purpose for keeping its platform safe and free of child-exploitation content"). Thus,

---

case, judicial notice would not have changed the district court's ruling because the documents support the court's conclusion that Microsoft acted according to its independent business interests.

Rosenschein's Fourth Amendment claim fails under the second prong of the governmental-agent inquiry.[4] *Souza*, 223 F.3d at 1201.

Even if Chatstep and Microsoft were governmental agents, Rosenschein's Fourth Amendment claim falls short because he has not presented evidence sufficient to establish a Fourth Amendment search. The Supreme Court has identified two types of searches that give rise to a Fourth Amendment claim. First, "[w]hen an individual seeks to preserve something as private, and his expectation of privacy is one that society is prepared to recognize as reasonable, . . . [an] official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause." *Carpenter v. United States*, 585 U.S. 296, 304 (2018) (quotation and internal quotation marks omitted). Second, a Fourth Amendment search occurs where the government "physically occupie[s] private property for the purpose of obtaining information." *United States v. Jones*, 565 U.S. 400, 404–05 (2012).

On appeal, Rosenschein has not argued that the conduct in this case amounted to a physical trespass for the purpose of obtaining information. Accordingly, we

[4] Rosenschein also argues that the district court should have invalidated the entire PhotoDNA program based on NCMEC's alleged violation of an earlier version of 18 U.S.C. § 2258C(a)(1). Specifically, he argues that the court should have suppressed all the evidence because NCMEC was statutorily prohibited from including in its hash list any PhotoDNA hash values of images of unidentified children. We need not address this argument in depth. We have long held that suppression is available for a statutory violation only where the statute provides for such a remedy. *See United States v. Minjares-Alvarez*, 264 F.3d 980, 986 (10th Cir. 2001). The statute here does not.

deem that argument waived. *See United States v. Leffler*, 942 F.3d 1192, 1196 (10th Cir. 2019).

Rosenschein's claim that he had a reasonable expectation of privacy in his uploads also fails. The Fourth Amendment offers no protection for items "knowingly expose[d] to the public." *United States v. Miller*, 425 U.S. 435, 442 (1976). This principle is based on the common-sense understanding that "[t]hose who bring personal material into public spaces, making no effort to shield that material from public view, cannot reasonably expect their personal materials to remain private." *United States v. Barrows*, 481 F.3d 1246, 1249 (10th Cir. 2007). Here, several facts support the district court's conclusion that Rosenschein has not demonstrated an objectively reasonable expectation of privacy in the images he uploaded to Chatstep. For example, Chatstep is a free, publicly accessible website. Rosenschein understood that he was sharing child pornography with strangers online. And though Rosenschein claims his expectation of privacy was reasonable because the images were (or could have been) uploaded in a private, password-protected chatroom with a single recipient, he has offered no evidence to establish this fact.

Chatstep's inclusion of a "report image" function—which, when utilized, allowed users to view the IP address of the image's sender—further supports this conclusion. Chatstep created this feature "as a deterrent to Chatstep users sharing illegal photos because they would know that other users could report them" either to Chatstep or to law enforcement. R. Vol. II at 330. Thus, even in a small chatroom

with generally anonymous users, no reasonable user would have believed that images uploaded to Chatstep would remain private.

Both our precedents and several out-of-circuit cases also reaffirm what common sense makes clear: Individuals have no reasonable expectation of privacy in images they post to a reportable online chatroom with strangers. *See, e.g.*, *United States v. Morel*, 922 F.3d 1, 10 (1st Cir. 2019) (concluding that a defendant had no reasonable expectation of privacy in images uploaded to a publicly accessible image hosting website); *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers. . . . They may not, however, enjoy such an expectation of privacy in transmissions over the Internet or e-mail that have already arrived at the recipient."); *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001) (holding, in a non-criminal context, that "computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person—the system operator"); *United States v. Perrine*, 518 F.3d 1196, 1205 (10th Cir. 2008) (concluding that a defendant had no reasonable expectation of privacy in subscriber information given to an internet provider); *United States v. Charbonneau*, 979 F. Supp. 1177, 1185 (S.D. Ohio 1997) (concluding that a defendant had no reasonable expectation of privacy in statements made in AOL chatrooms in part because the defendant "ran the risk of speaking to an undercover agent"). Accordingly, we reject Rosenschein's first set of arguments for suppressing the evidence under the Fourth Amendment.

B.

Rosenschein next argues the district court should have suppressed the evidence found in his home under *Franks v. Delaware*, 438 U.S. 154 (1978). To establish a Fourth Amendment violation under *Franks*, a defendant must show that "(1) an officer's affidavit supporting a search warrant application contains a reckless misstatement or omission that (2) is material because, but for it, the warrant could not have lawfully issued." *United States v. Moses*, 965 F.3d 1106, 1110 (10th Cir. 2020) (quotation omitted). Because we identify no materially false statements or wrongful omissions in the search warrant affidavit, we affirm the district court's denial of Rosenschein's suppression motion.

Rosenschein challenges three statements as materially false or misleading. First, he argues the affidavit's claim that "using hash values is another common technique used to identify users and specific electronic files" is false because PhotoDNA identifies only images, and not users or other electronic files. Supp. R. Vol. IV at 43; Aplt. Br. at 30. But this statement refers to hash values generally—which can be used on usernames, passwords, and email addresses, or to determine what user saved or uploaded a file, *see* R. Vol. III at 471–72—and not merely to PhotoDNA's capabilities. Thus, the statement is accurate. Although it is not wholly applicable to PhotoDNA—the only product used in this case—it was not intentionally or recklessly misleading. *See id.* at 564–65 (explaining that the detective who authored the affidavit did not understand the precise differences between PhotoDNA's hash values and hash values generally).

Second, Rosenschein contends the affidavit's claim that "hash values are mathematical algorithms that produce a 25-character pattern that is specific to a single file" is false because hash values are the product of algorithms, and not themselves algorithms. Supp. R. Vol. IV at 43; Aplt. Br. at 30. But whether hash values are algorithms or products of algorithms is immaterial. As the affidavit makes clear, "the salient point for purpose[s] of a probable cause determination is that a hash value is unique to any given image and thus is a reliable way to identify an image." R. Vol. II at 368. And here, the government has provided ample evidence that hash values are a reliable way to identify an image. *See* R. Vol. III at 89–90 (describing PhotoDNA's error rate as one in fifty billion); *id.* at 166, 177 (explaining that PhotoDNA has an accuracy rate of over ninety-nine percent); *id.* at 91, 213 (stating that false positives—that is, matches that are not child pornography—are extremely rare).

Third, Rosenschein claims that the authoring detective's statement that "Chatstep provided the photograph . . . I reviewed it" was misleading. Supp. R. Vol. IV at 44–45; Aplt. Br. at 31. Specifically, he argues that the term "*re*view" may have misled the judge issuing the warrant to believe that Chatstep had also viewed the images. We agree with the district court that this language did not reasonably suggest that Chatstep had viewed the images. And even if the language was ambiguous, we conclude the mistake was immaterial because the affidavit correctly stated that a detective had viewed the images and confirmed that they contained child pornography before applying for the warrant.

Rosenschein also claims the affidavit omitted several key facts. First, he notes that the affidavit did not include a detailed description of PhotoDNA. But he does not explain how this omission negated probable cause. And in any event, the government has offered significant evidence showing that PhotoDNA is a reliable method of identifying child pornography. *See supra* p. 15. Thus, Rosenschein has not shown this omission was material.

Second, Rosenschein argues that the affidavit wrongly omitted information about NCMEC's role in the investigation. He also contends the affidavit was misleading because it did not disclose that the reported images were not viewed or verified by NCMEC. But the record directly contradicts these claims. The affidavit described in detail NCMEC's role in forwarding CyberTips to ICAC and explained that local law enforcement received information from ICAC. Further, as previously noted, the affidavit explained that a detective had viewed the images and described their content before applying for the warrant.

Third, Rosenschein contends that the district court should have suppressed all evidence from the search of his home because the affidavit used to obtain the search warrant did not inform the issuing judge that a detective had viewed the Chatstep uploads without obtaining a warrant. This omission is immaterial; as the district court correctly concluded, the detective did not need a warrant to view Rosenschein's uploads because they were posted to a reportable chatroom with strangers. *See supra* pp. 11–13. Further, Rosenschein has presented no evidence that suggests the omission was made to mislead the court.

Fourth, Rosenschein argues the affidavit wrongly omitted important information about the investigative process. For example, he notes that the affidavit did not state that law enforcement had corroborated the IP address listed in the CyberTips. This omission is immaterial. Rosenschein does not explain how the absence of a corroboration statement would have affected the judge's probable cause determination, particularly where law enforcement had no reason to believe the information in the CyberTips was unreliable.

Finally, Rosenschein argues that the affidavit's description of the images as "depict[ing] a child under 18 years old involved in a sex act" was conclusory and thus did not permit the judge to determine that there was probable cause to search Rosenschein's home. Supp. R. Vol. IV at 44–45; Aplt. Br. at 31–32. He contends that the affidavit should have described the particular sex act. This claim directly contradicts our precedents. We have previously held that generalized descriptions of child pornography sufficiently convey to the judge issuing the search warrant the type of evidence required to support probable cause. *United States v. Simpson*, 152 F.3d 1241, 1247 (10th Cir. 1998). Further, the affidavit's description aligns with the legal definition of child pornography. *See* 18 U.S.C. § 2256(8) (defining child pornography as "any visual depiction . . . of a minor engaging in sexually explicit conduct"). Thus, the affidavit's description of the images was adequate.

Rosenschein has not shown that the affidavit contained false statements or relevant omissions such that the warrant should not have issued. *See Franks*, 438 U.S. at 171–72. Accordingly, based on the information provided in the affidavit, the

district court correctly concluded that the government's evidence was sufficient to establish probable cause to justify the search of Rosenschein's home.

III.

Rosenschein next challenges the district court's denial of his motion to either dismiss the case or, in the alternative, to compel the discovery of the computer programs used by Microsoft and NCMEC to produce internal reports. To support his claim, he argues that Chatstep, Microsoft, and NCMEC conspired to destroy or withhold evidence as part of their effort to frame him for possessing and uploading images he never possessed.

We begin with Rosenschein's claim that the district court should have dismissed the case based on Chatstep's failure to preserve evidence of the uploaded images after they were reported to NCMEC. "[U]nless a criminal defendant can show bad faith on the part of the police, failure to preserve potentially useful evidence does not constitute a denial of due process of law." *Arizona v. Youngblood*, 488 U.S. 51, 58 (1988). Here, Rosenschein has not shown that Chatstep's alleged failure to preserve electronic records after it reported the images to NCMEC constitutes bad faith on the part of the government. As previously discussed, Chatstep is not a governmental agent. *See supra* pp. 8–11. Further, nothing in the record suggests that Chatstep destroyed evidence at the government's direction or request. To the contrary, Chatstep's loss of data also precluded the government from using that information to support its case. Thus, Chatstep's failure to preserve evidence is not a basis for dismissal of Rosenschein's criminal charges. *See United*

States v. Fernandez, 24 F.4th 1321, 1336–39 (10th Cir. 2022) (concluding the government was not responsible for a private party's failure to preserve evidence).

We next turn to Rosenschein's claim that the district court should have compelled discovery of the computer programs and hash values used by NCMEC to generate reports of child pornography. "We generally review for an abuse of discretion the district court's denial of a discovery request for documentary evidence." *United States v. Cates*, 73 F.4th 795, 811 (10th Cir. 2023) (quotation omitted). "[W]e will not disturb the district court's ruling unless we have a definite and firm conviction that the court made a clear error of judgment or exceeded the bounds of permissible choice in the circumstances." *Id.* (quotation omitted).

At the hearing discussing this motion, the government stated (1) that it had produced all the information NCMEC had regarding the images in this case; (2) that NCMEC would present testimony regarding its child pornography database; and (3) that it had provided the defense with an outline of NCMEC's expected testimony on the issue. The government further explained that it could not produce what Rosenschein was requesting because there was no electronic report capturing the hash values, and that the information would instead be provided through testimonial evidence. Because Rosenschein would have had the opportunity to access that information—albeit through the examination of witnesses, rather than a report—we conclude that the district court did not abuse its discretion in denying Rosenschein's motion to require production of a report.

IV.

Rosenschein next claims that the district court erred in denying his motion to require the government to provide expert reports for two witnesses—John Shehan, who served as the vice president of the Exploited Children Division of NCMEC, and Jeff Lilleskare, who worked as a group manager for security and online safety at Microsoft—before the suppression hearing. *See* Fed. R. Crim. P. 16(a)(1)(G) (requiring the government to produce, at the defendant's request, expert reports for witnesses it intends to call during its case-in-chief). He further argues that Shehan and Lilleskare "had no knowledge of the case whatsoever, disqualifying [them] as [] factual witness[es]." Aplt. Br. at 28.

Both claims fall short. First, Rosenschein concedes that the Federal Rules of Evidence and Federal Rule of Criminal Procedure 16(a)(1)(G) do not apply to suppression hearings. R. Vol. I at 456 ("As a technical matter that is true."). Although courts may, in certain cases, exercise their discretion to order expert reports in advance of a suppression hearing, nothing in this case suggests the district court was required to do so. Second, the witnesses' declarations and testimony—as well as their positions in NCMEC and Microsoft—establish a clear basis for their knowledge. Nothing in the record suggests that the district court should not have permitted these witnesses to testify at the suppression hearing. Accordingly, the district court did not abuse its discretion in denying Rosenschein's motion.

V.

For the foregoing reasons, we AFFIRM the district court's denial of Rosenschein's motions.