APPENDIX A

UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT

No: 19-2331

United States of America

Appellee

v.

Mark Ringland

Appellant

Google, LLC, et al.

Amici on Behalf of Appellee(s)

Appeal from U.S. District Court for the
District of Nebraska – Omaha
(8:17-cr-00289-LSC-1)

ORDER

The petition for rehearing en banc is denied. The petition for rehearing by the panel is also denied.

Judge Kelly did not participate in the consideration or decision of this matter.

October 06, 2020

Order Entered at the Direction of the Court:
Clerk, U.S. Court of Appeals, Eighth Circuit

_____

/s/ Michael E. Gans

APPENDIX B

UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT

No: 19-2331

United States of America,

Plaintiff - Appellee

v.

Mark Ringland,

Defendant - Appellant

Appeal from the United States District Court
for the District of Nebraska – Omaha

Submitted: May 12, 2020
Filed: July 16, 2020

Before COLLOTON and BENTON, Circuit Judges,
and WILLIAMS, District Judge.[1]

---

[1] The Honorable C.J. Williams, United States District Judge for the Northern District of Iowa, sitting by designation.

WILLIAMS, District Judge.

Mark Ringland was convicted of receipt of child pornography, in violation of Title 18, United States Code, Section 2252(a)(2). At trial, the government introduced evidence of child pornography found on Ringland's electronic devices. Law enforcement officers seized and searched Ringland's devices under authorized warrants based on information furnished by Google, Inc. ("Google") and the National Center for Missing and Exploited Children ("NCMEC"). On appeal, Ringland asserts the district court[2] erred in denying his motion to suppress this evidence because he contends Google, acting as a government agent, conducted unlawful warrantless searches of his email accounts. Alternatively, Ringland argues that NCMEC, acting as a government agent, also conducted unlawful warrantless searches of his email accounts by expanding Google's original searches. Finally, Ringland argues the good faith exception to the exclusionary rule does not apply to save the unlawful searches. Because we find the searches lawful, we affirm.

I.

Google is an electronic communication service provider ("ESP") offering a variety of services, including the email service gmail. To create a gmail account, users must agree to Google's terms of service, which includes Google's right to review content to ensure it complies with the law. Google monitors gmail accounts using automated systems employing a hash-

[2] The Honorable Laurie Smith Camp, United States District Judge for the District of Nebraska, adopting the findings and recommendation of the Honorable Michael D. Nelson, United States Magistrate Judge for the District of Nebraska.

comparison technology to detect unlawful content, such as child pornography. Federal law requires Google to report known child pornography violations to NCMEC through the CyberTipline Report system. *See* 18 U.S.C. § 2258A(a).

On March 20, 2017, Google sent a CyberTipline Report to NCMEC containing 784 files of child pornography from Ringland's email account mringland69@gmail.com ("mringland69"). Google discovered some of these files through its hashing technology. The report noted that it contained "over 700 files," with Google affirming it reviewed 231 of the files but providing no information on the other 553 files. NCMEC "reviewed the uploaded files and found" apparent child pornography. On March 21, 2017, Google sent a new report to NCMEC, after uploading 400 more files from Ringland's gmail account, stating it had reviewed 258 of the files but giving no information on the other 142. Between April 6, 2017, and April 19, 2017, Google reported and uploaded to NCMEC 32 more files from Ringland's gmail account, stating it had reviewed 13 of the files and giving no information on the other files. In sum, from March 20, 2017, to April 19, 2017, Google uploaded to NCMEC 1,216 files from the mringland69 gmail account. Of these files, Google viewed 502 and gave no information as to whether it viewed the rest. On April 17, 2017, and April 28, 2017, NCMEC forwarded all reports to the Nebraska State Police ("NSP").

Google continued to monitor Ringland's gmail accounts. On June 20, 2017, Google discovered the gmail account mringland65@gmail.com ("mringland65"), which appeared to be linked to mringland69. Google scanned and uploaded two files from this second gmail account to NCMEC. Google gave no information as to

its review. On June 21, 2017, NCMEC noted it had not reviewed the files and forwarded them to police officers in South Dakota.

On June 27, 2017, NSP Investigator C.J. Alberico ("Investigator Alberico") sought and received a warrant to search the email mringland69. In her application, Investigator Alberico noted that Google had reviewed only 502 of the 1,216 files found on the mringland69 account and that she had reviewed only the same 502 files. From searching this account, Investigator Alberico discovered that the email address mringland69 had sent child pornography images to the email address mringland65.

On July 13, 2017, Google uploaded two more files from a third email, markringland65@gmail.com ("markringland65"), with no information as to its review. On July 18, 2017, NCMEC linked the June 20 and July 13 reports and forwarded both to NSP. NCMEC noted it had not reviewed these files. On July 19, 2017, Google uploaded five more files from markringland65, but did not indicate its review. On July 21, 2017, NCMEC did not review the files but forwarded them to NSP.

Between August 1, 2017, and August 4, 2017, Google uploaded 1,109 more files from markingland65 across nine reports. Google indicated it reviewed 773 of the files and gave no information on the other files. In one of the nine reports, NCMEC noted it had "viewed the uploaded files and found" apparent child pornography. On August 4, 2017, NCMEC forwarded these reports to NSP.

On August 7, 2017, Investigator Alberico sought and received a warrant to search defendant's other

two gmail accounts, mringland65 and markringland65. As to mringland65, Investigator Alberico noted mringland69 had sent child pornography to that address. As to markringland65, Investigator Alberico relied on the nine reports from NCMEC as containing alleged contraband. Investigator Alberico noted Google had not reviewed all the files in the reports and she had not viewed them either.

On August 31, 2017, Investigator Alberico sought and received a warrant to track defendant's cell phone, which was identified in earlier reports.[3] On September 1, 2017, Investigator Alberico sought and received federal search and arrest warrants. That same day, officers arrested Ringland, who made incriminating statements and allowed officers to retrieve an iPad from his van. On September 5, 2017, Ringland made further incriminating statements to Investigator Alberico during a transfer.

Ringland moved to suppress evidence recovered from his mringland69, mringland65, and markringland65 gmail accounts. A United States Magistrate Judge held an evidentiary hearing and issued a Findings and Recommendation ("F&R"). The magistrate judge found that Google was not acting as a government agent. The judge also found that NCMEC did not view more files than Google. The judge further found that Investigator Alberico did not view more files than Google. Alternatively, the magistrate judge reasoned, the officers who executed the search relied in good faith on the signed warrants such that the good faith exception to the exclusionary rule applied under *United*

---

[3] From August 4, 2017, to August 31, 2017, Google uploaded 566 more files from markrigland65 to NCMEC, but none of this information went into anywarrant application.

States v. Leon, 468 U.S. 897 (1984). Ringland objected to the magistrate judge's F&R.

The district court judge overruled Ringland's objections to the magistrate judge's F&R. The district court judge found the magistrate judge's factual findings to be correct, and further found the magistrate judge did not omit any material facts. The district court judge agreed that Google did not act as a government agent and that Investigator Alberico did not view any more files than Google. The district court judge concluded it did not matter whether NCMEC viewed more files because Investigator Alberico only viewed those already viewed by Google. Finally, the district court judge agreed alternatively that the warrants were within the *Leon* good faith exception.

II.

When reviewing the denial of a motion to suppress, we review the district court's factual findings for clear error and its legal conclusions de novo. *United States v. Clay*, 646 F.3d 1124, 1127 (8th Cir. 2011).

"A warrantless search is presumptively unreasonable absent some exception to the warrant requirement[.]" *United States v. Hernandez Leon*, 379 F.3d 1024, 1027 (8th Cir. 2004). "The ordinary sanction for police violation of Fourth Amendment limitations has long been suppression of the evidentiary fruits of the transgression." *United States v. Fiorito*, 640 F.3d 338, 345 (8th Cir. 2011). The Supreme Court has also long held, however, that Fourth Amendment protection extends only to actions undertaken by government officials or those acting at the direction of some official. *See, e.g.*, *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 613-14 (1989); *Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971); *Burdeau v. McDowell*, 256 U.S.

465, 475 (1921). Thus, "the Fourth Amendment does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative" but it does "protect[] against such intrusions if the private party acted as an instrument or agent of the Government." *Skinner*, 489 U.S. at 614.

"Whether a private party should be deemed an agent or instrument of the government for Fourth Amendment purposes necessarily turns on the degree of the government's participation in the private party's activities, a question that can only be resolved in light of all the circumstances." *United States v. Wiest*, 596 F.3d 906, 910 (8th Cir. 2010) (quoting *Skinner*, 489 U.S. at 614). In this context, we have focused on three relevant factors: "[1] whether the government had knowledge of and acquiesced in the intrusive conduct; [2] whether the citizen intended to assist law enforcement or instead acted to further his own purposes; and [3] whether the citizen acted at the government's request." *Id.* "A defendant bears the burden of proving by a preponderance of the evidence that a private party acted as a government agent." *United States v. Highbull*, 894 F.3d 988, 992 (8th Cir. 2018). Further, "[w]hen a statute or regulation compels a private party to conduct a search, the private party acts as an agent of the government." *United States v. Stevenson*, 727 F.3d 826, 829 (8th Cir. 2013) (citation omitted). "Even when a search is not required by law, however, if a statute or regulation so strongly encourages a private party to conduct a search that the search is not 'primarily the result of private initiative,' then the Fourth Amendment applies." *Id.*

If a private party conducted an initial search independent of any agency relationship with the govern-

ment, then law enforcement officers may, in turn, perform the same search as the private party without violating the Fourth Amendment as long as the search does not "exceed[ ] the scope of the private search." *United States v. Miller*, 152 F.3d 813, 815 (8th Cir. 1998). This is because the private search already frustrated the person's legitimate expectation of privacy; thus, "an ensuing police intrusion that stays within the limits of the private search is not a search for Fourth Amendment purposes." *Id.*

III.

Here, the district court did not err when it found Google's search of Ringland's email accounts constituted a private search. Ringland argues Google acted as a government agent because it was coerced into reporting child pornography by statutory penalties imposed for failing to report such content. It is true that Title 18, United States Code, Section 2258A(a) requires an ESP to report to NCMEC any apparent violation of child pornography laws it discovers. Despite the reporting requirement, however, Section 2258A does not require ESPs to seek out and discover violations. 18 U.S.C. 2258A(f).

In *United States v. Stevenson*, the defendant sought to suppress child pornography discovered on his email by America Online ("AOL") through hashing. 727 F.3d at 828-29. AOL's hash-detection program automatically forwarded a report to NCMEC which was then relayed to law enforcement officers. There, we rejected the defendant's argument that Sections 2258A and 2258B amounted to state action like the railroad regulations in *Skinner v. Railway Labor Executives' Association*. *Id.*, at 829-30. We held these sections did

not authorize the scanning of emails, clear legal barriers for preemptively scanning emails, prohibit ESPs from contracting away their rights to scan emails, or delineate consequences for users should they refuse to submit to scanning. *Id.*, at 830. We concluded that "[a] reporting requirement, standing alone, does not transform an [ESP] into a government agent whenever it chooses to scan files sent on its network for child pornography." *Id.*; *see also United States v. Cameron*, 699 F.3d 621, 637-38 (1st Cir. 2012) (same); *United States v. Richardson*, 607 F.3d 357, 366-67 (4th Cir. 2010) (same).

Here, Google did not act as a government agent because it scanned its users' emails volitionally and out of its own private business interests. Google did not become a government agent merely because it had a mutual interest in eradicating child pornography from its platform. *See Cameron*, 699 F.3d at 637 ("We will not find that a private party has acted as an agent of the government 'simply because the government has a stake in the outcome of a search.'"). The government did not know of Google's initial searches of Ringland's gmail accounts, the government did not request the searches, and Google acted out of its own obvious interests in removing child sex abuse from its platform. *See United States v. Smith*, 383 F.3d 700, 705 (8th Cir. 2004). Again, Google was not required to perform any such affirmative searches. As we held in *Stevenson*, the reporting requirement for child pornography alone does not transform Google into a government agent. *See* 727 F.3d at 830. Moreover, the statutory scheme does not so strongly encourage affirmative searches such that it is coercive. In fact, the penalties for failing to report child pornography may even discourage searches in favor of willful ignorance. Thus, Google was

not a state actor here and its searches do not implicate the Fourth Amendment.

Ringland asserts this case is distinguishable from *Stevenson* because Google continued to scan his email and uncover his identifying information after its initial report to NCMEC, thus showing the government was aware of and acquiesced to Google's searches and Google acted to assist NSP. Ringland also asserts Google's size and far-reaching access to its users' personal data threatens the Fourth Amendment like in *Carpenter v. United States*, 138 S. Ct. 2206, 2212 (2018), wherein law enforcement officers obtained and executed court orders on Sprint and MetroPCS to disclose the cell-site location data of several robbery suspects. Ringland argues the same "seismic shifts in digital technology" allowing for long-term and specific location tracking apply here and warrant suppression of the evidence.

Ringland's attempts to distinguish Stevenson are unpersuasive. It is inconsequential that Google continued to scan his email accounts or uncover identifying information after sending its initial report. These continued searches were, again, unrequested by the government and comport with Google's private interests. Further, there is no evidence the government had any notice Google would conduct these searches prior to receiving the search results. That Google continued to monitor Ringland's emails and comply with reporting requirements does not anymore indicate its intent to help the government than its first report did. Nor is there any evidence that the government directed Google to continue its review of Ringland's accounts. The unity of interest between Google and the government does not imply some acquiescence or agreement between them to conduct searches in an informal, clandestine manner.

Simply put, Google's continued actions in its own interest and the government's continued receipt of the reports does not give rise to some form of agency. *See Stevenson*, 727 at 831 (holding an ESP's "voluntary efforts to achieve a goal that it shares with law enforcement" does not make it a government agent).

This case is also distinguishable from *Carpenter*. There, the Supreme Court reversed the Sixth Circuit Court of Appeals, which held the defendant lacked a reasonable expectation of privacy in cell-site location data from his phone because the defendant shared that information with his wireless carriers. 138 S. Ct. at 2213. Here, we find the search appropriate under the private search doctrine, not the third-party doctrine exception. *See United States v. Jacobsen*, 466 U.S. 109 (1984). *Cf. Carpenter*, 138 S. Ct. at 2217 (not extending third-party doctrine exception to cell phone location records).

Because Investigator Alberico searched only the same files that Google searched, the government did not expand the search beyond Google's private party search. *See Jacobsen*, 466 U.S. at 115-18 ("The additional invasions of respondents' privacy by the government agent must be tested by the degree to which they exceeded the scope of the private search."); *c.f. United States v. Ackerman*, 831 F.3d 1292, 1305-07 (10th Cir. 2016) (concluding that NCMEC qualified as a governmental entity that searched defendant's e-mail in a way that exceeded an earlier private search). Ringland insists that NCMEC's search, however, went beyond the scope of the search Google conducted. Even if true, Investigator Alberico's search warrant applications did not contain information from NCMEC's searches. Thus, we need not decide whether NCMEC is a government

agency or whether it expanded its search beyond Google's search.

IV.

Accordingly, we affirm the judgment of the district court.

APPENDIX C

IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA, Plaintiff, vs. MARK RINGLAND, Defendant.	**8:17CR289** **MEMORANDUM AND ORDER**

This matter is before the Court on the Findings and Recommendation (F&R), ECF No. 74, issued by Magistrate Judge Michael D. Nelson, recommending that the Motion to Suppress, ECF No. 47, and Motion to Suppress and Application for *Franks* Hearing, ECF No. 49, filed by the Defendant, Mark Ringland, be denied. Ringland filed an Objection to the Findings and Recommendation and a brief in support, ECF No. 75, as allowed by 28 U.S.C. § 636(b)(1)(C) and NECrimR 59.2(a). The Government did not respond to the Objection. For the reasons set forth below, the F&R will be adopted and the Motion to Suppress will be denied.

BACKGROUND

Defendant is charged with receipt of child pornography and possession of child pornography. Indictment, ECF No. 20. Ringland does not object to the Magistrate Judge's findings of fact included in the F&R, but objects to the Magistrate Judge's failure to

include each and every fact contained in Ringland's Supplemental Brief, ECF No. 70 at 2-24. The Court has reviewed the record and each of the facts listed in Ringland's briefs, and concludes that the Magistrate Judge did not err in failing to restate every fact listed in Ringland's briefs. Several of Ringland's asserted facts are descriptions of the law, legal argument, or legal conclusions. Each of the facts stated by the Magistrate Judge is supported by the record. To the extent certain facts were omitted, the F&R demonstrates that the Magistrate Judge considered all the evidence and did not omit any material facts.

The Court adopts the Magistrate Judge's factual findings in their entirety and provides the following by way of summary.

Investigator C.J. Alberico of the Nebraska State Patrol investigated Ringland's conduct, leading to the charges filed in this case. TR.[1] 55; D.E.[2] 163. According to Alberico, Google, Inc. (Google) first provided information to the National Center for Missing and Exploited Children (NCMEC) that a user of Google's services "had uploaded over seven hundred (700) files suspected of depicting sexually explicit conduct involving a minor." D.E. 109 at 7. Google identified the user by email address, mringland69@gmail.com, with associated telephone number 402-***-0642. Several IP addresses were associated with the uploaded files, which NCMEC traced to Sprint PCS in Omaha, Nebraska. Based on this information, on April 17, 2017, NCMEC created seven CyberTipline reports:

---

[1] References to "TR" are to the Transcript of the evidentiary hearing at ECF No. 68.

[2] References to G.E. and D.E. are to Government's Exhibit and Defendant's Exhibit, respectively.

#19083866, #19153972, #19938982, #19986242, #20035870, #20260729, and #20293287. D.E. 163 at 1.

Deputy Mark Dishaw, of the Douglas County, Nebraska, Sheriff's Office, testified that an electronic service provider ("ESP"), such as Google, has proprietary methods to filter and identify known child pornography images based on hash values. TR. 21-22, 24-25,51-53. The ESP then views the file images and reports potential violations to NCMEC which generates CyberTipline reports to send to law enforcement. TR. 14-16. Law enforcement then reviews the files identified by the ESP.

On June 23, 2017, Alberico received CyberTipline Report #20437297, which Google previously submitted to NCMEC. On June 27, 2017, Alberico prepared a Douglas County search warrant affidavit, search warrant, and non-disclosure order for the email account mringland69@gmail.com, associated with telephone number 402-***-0642. D.E. 163 at 1-2; D.E. 109-110. Alberico stated in her affidavit supporting the application that Google "reviewed five hundred and two (502) files from the CyberTips submitted" and that she "only viewed files that were reviewed by Google . . . to confirm they depicted child pornography." D.E. 109 at 7. Alberico obtained a warrant to search the account.

Alberico observed that email address mringland69@gmail.com had sent child erotica photographs and images of child pornography to the email address mringland65@gmail.com. D.E. 163 at 2. On July 19, 2017, Alberico received CyberTipline reports #21681475 and #22346425. These reports listed the email address markringland65@gmail.com, with associated telephone 402-***-0902, and a secondary email

address, mringland69@gmail.com. NCMEC traced several of the IP addresses associated with the uploaded files to Sprint PCS in the Omaha area, and Google provided the name "Mark Ringland" associated with the two email addresses. D.E. 163 at 2. Pursuant to a subpoena served by Alberico on July 20, 2017, Sprint PCS identified the subscriber of telephone number 402-***-0902 as Mark Ringland, residing at 1904 Pleasantview Ln, Bellevue, Nebraska 68005.

On August 7, 2017, Alberico received nine more CyberTipline reports: #22968026,#22968382, #22968534, #23001904, #23002061, #2302151, #23002255, #23043174, and #23043630, all of which were associated with the email address markringland65@gmail.com. On the same date, Alberico prepared a Douglas County search warrant affidavit, search warrant, and non-disclosure order for the email accounts mringland65@gmail.com and markringland65@gmail.com, associated with telephone number 402-***-0902. D.E. 122-123.

On August 14, 2017, Alberico received five additional CyberTipline reports, #23245909, #23274478, #23249764, #23249764 and #23068622, and on August 25, 2017, six more, #23411893, #23488795, #23512952, #23545730, #23588762, and #233890937. All the reports were associated with email addresses markringland65@gmail.com and mringland69@gmail.com, and the telephone number 402-***-0902. D.E. 163 at 4.

On August 18, 2017, Alberico received information from Google pursuant to the previous search warrant. Alberico reviewed files from Google and concluded

that several of the files contained images and/or videos of suspected child pornography and bestiality. D.E. 124 at 10. Based on that information, Alberico applied for a United States District Court search and seizure warrant affidavit, search warrant, and non-disclosure order for a cellular ping order for telephone number 402-***-0902, which was presented to and signed by a United States Magistrate Judge. D.E. 124-125; D.E. 163 at 4.

Alberico located Mark Ringland in the Nebraska Criminal Justice System (NCJIS), which indicated that a black Ford Windstar SE sport van with Nebraska license plate number UZP192 was registered to Ringland in June 2017, and that as of August 2017, the vehicle's registration address was 16406 Taylor Street, Omaha, NE 68116. Nebraska Department of Labor records indicated that Ringland was employed by Merrick Machine Company, located in Alda, Nebraska, and by the temporary agency Essential Personnel Inc., based out of Grand Island Nebraska, with hub offices in Kearney, Nebraska and Denver, Colorado. D.E.163 at 3.

On September 1, 2017, Alberico obtained a United States District Court search warrant for Ringland's person and cellular telephone, phone number 402-***-0902, D.E. 126-127, and a criminal complaint and arrest warrant. On the same date, law enforcement executed a search warrant at 16406 Taylor Street in Omaha, and arrested Ringland pursuant to the warrant. Ringland was read his *Miranda* rights, which he waived, and consented to an interview. D.E. 163 at 4. Alberico indicated in her report that on September 5, 2017, Ringland made spontaneous statements to the United States Marshals transporting him for his initial hearing. D.E. 163 at 4-5.

Ringland seeks to suppress all evidence seized in connection with the searches of his email accounts, and any incriminatory statements made after his arrest and during transportation to his initial appearance. Ringland argues that Google acted as a government agent when it searched his emails without a warrant and forwarded those contents to NCMEC; that NCMEC expanded upon Google's warrantless searches; and that the warrants obtained by Alberico were supported in substantial part by such warrantless searches. Ringland also seeks a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978), arguing that the applications supporting the warrants in this case omitted information material to the probable cause determination. The Magistrate Judge recommends that both motions be denied. Ringland objects to the Magistrate Judge's conclusions. Although Ringland asserts twelve different objections, many of them overlap and each is addressed below.

STANDARD OF REVIEW

Under 28 U.S.C. § 636(b)(1)(C) and NECrimR 59.2(a), the Court shall make a *de novo* review of the portions of the Magistrate's Findings and Recommendation to which objections have been made. The Court may accept, reject, or modify, in whole or in part, the Magistrate Judge's findings and recommendations. The Court may also receive further evidence or remand the matter to the Magistrate Judge with instructions.

DISCUSSION

I. Franks Hearing

Affidavits supporting a search warrant are presumed valid. *Franks v. Delaware,* 438 U.S. 154, 171

(1978). "Under *Franks,* a criminal defendant may request a hearing to challenge a search warrant on the ground that the supporting affidavit contains factual misrepresentations or omissions relevant to the probable cause determination." *United States v. Arnold,* 725 F.3d 896, 898 (8th Cir. 2013). To meet the burden of demonstrating that such a hearing is warranted, the defendant must make "a substantial preliminary showing." *Franks,* 438 U.S. at 155. The defendant must demonstrate that the affidavit supporting the warrant "contained false statements or omissions that were material to the finding of probable cause," *United States v. Oleson,* 310 F.3d 1085, 1090 (8th Cir. 2002). "The type of showing required is not easily met." *United States v. Gabrio,* 295 F.3d 880, 883 (8th Cir. 2002).

Ringland argues that he is entitled to a *Franks* hearing because Alberico did not include in her warrant applications that there were other geographic locations and internet protocol (IP) addresses associated with images outlined in the NCMEC CyberTipline reports. Ringland also argues that he is entitled to a *Franks* hearing because only a small portion of the files was categorized as "apparent child pornography." Finally, Ringland argues that Google and NCMEC were state actors for purposes of the Fourth Amendment and therefore their warrantless searches of his personal email and phone numbers were unconstitutional. Upon review of the record, none of these arguments entitles Ringland to a *Franks* hearing.

A. IP Addresses and Geographic Locations

It is undisputed that Alberico did not include information about other IP addresses contained in the

NCMEC CyberTipline reports in the affidavit. Yet information in the affidavit related to Ringland's identity was sufficient to support a probable cause finding. The record demonstrates that the CyberTipline reports identified email addresses and a phone number connected to Ringland. For example, the first application stated that the tips were related to the email address markringland69@gmail.com and phone number 402-xxx-0642. The second warrant application identified markringland65@gmail.com and mringland69@gmail.com, as well as the phone number 402-xxx-0902. Based on the information obtained from the first two warrants and independent investigation, investigators obtained a ping warrant that led them to Ringland's geographic location. The issuing judge reasonably relied on information about the phone number repeatedly appearing in reports to issue the ping warrant that identified Ringland's precise geographic location, regardless of the IP addresses or geographic locations associated with them. The omission of information regarding additional IP addresses did not diminish the evidence supporting probable cause. Accordingly, the Court adopts the Magistrate Judge's conclusion.

B. Categorization of Files as Apparent Child Pornography

Each report from NCMEC contains an executive summary that describes the total number of uploaded files sent by Google and contains NCMEC's categorization of the material contained in those files, *e.g.*, "Apparent Child Pornography" or "Uncategorized." D.E. 101-108; 112-121; & 128-143. Ringland notes throughout his briefing that the great majority of the files were deemed "uncategorized," and the Court infers that he suggests such files did not contain child

pornography and the omission of this fact from the application was misleading.[3]

Dishaw's testimony demonstrated that the "uncategorized" label was not an indication that a file contained no child pornography. Rather, the files that were categorized as potentially containing child pornography were ones that had been flagged by hash values. TR. 52. Files that were "uncategorized" were not tagged by hash values but were identified as containing child pornography through some other method. *Id*. In Alberico's application, she stated that she reviewed 502 image files identified and viewed by Google, and confirmed they depicted child pornography. Thus, even though the files were labeled as "uncategorized" in the NCMEC executive summary, there is evidence that they contained child pornography.

C. Google and NCMEC as State Actors

Ringland argues that Google and NCMEC were state actors and conducted an illegal search under the Fourth Amendment. This argument is the principal basis for Ringland's motion to suppress. For the reasons stated below, the Court cannot conclude that Google or NCMEC conducted an illegal search or that Alberico impermissibly examined the files prior to requesting a warrant. Accordingly, Ringland is not entitled to a *Franks* hearing on that basis.

II. Motion to Suppress

Ringland argues that his Fourth Amendment rights were violated when Google and NCMEC searched his email accounts without a warrant. Ring-

---

[3] Ringland never expressly describes his argument with respect to the uncategorized files.

land argues that Google was a government actor because its purpose was to help law enforcement and the government knew Google was searching Ringland's emails. Ringland also argues that NCMEC impermissibly expanded the scope of Google's search.

The Fourth Amendment demands that people shall "be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, . . . and no Warrants shall issue, but upon probable cause. . . ." U.S. Const., amend. IV. "The Fourth Amendment applies only to state action, so it does not constrain private parties unless they act as agents or instruments of the government." *United States v. Stevenson*, 727 F.3d 826, 829 (8th Cir. 2013) (citing *United States v. Jacobsen,* 466 U.S. 109, 113 (1984)). For purposes of the Fourth Amendment, private parties act as agents of the government when "a statute or regulation compels a private party to conduct a search" or "a statute or regulation so strongly encourages a private party to conduct a search that the search is not primarily the result of private initiative." *Id*. (internal quotation marks and citation omitted).

The statutes at issue in this case do not compel or "strongly encourage" disclosure of private information. The Stored Communications Act, 18 U.S.C. § 2701, generally prohibits computing service providers from disclosing contents of accounts except under specific, enumerated circumstances. Section 2702(b)(6) provides that service providers may "divulge the contents of a communication . . . to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A." Section 2258A requires service providers to report to the NCMEC any apparent violation of the child pornography laws discovered while providing electronic

communication services. *Stevenson*, 727 F.3d at 829 (citing 18 U.S.C. § 2258A(a)).

The Eighth Circuit has held that the reporting requirement of § 2258A, standing alone, "does not transform an [i]nternet service provider into a government agent whenever it chooses to scan files sent on its network for child pornography." *Id.* at 831. Instead, courts must consider several factors to determine whether a private party acts as an instrument of the government. *See id.* at 830 (citing *United States v. Smith,* 383 F.3d 700, 705 (8th Cir. 2004). These factors include "(1) whether the government had knowledge of and acquiesced in the intrusive conduct;" (2) "whether the citizen intended to assist law enforcement agents or instead acted to further his own purposes;" and (3) "whether the citizen acted at the government's request." *Smith*, 383 F.3d at 705. Applying these factors to Google and NCMEC, the Magistrate Judge correctly concluded that these entities were not government actors for purposes of the Fourth Amendment.

A. Google

There is no evidence that Google searched Ringland's email accounts at the Government's request. Ringland argues that the § 2258A's statutory scheme nevertheless "strongly encouraged" the search. However, the Eighth Circuit has held that § 2258A's reporting requirements are not sufficient on their own to make Google a government actor. *Stevenson*, 727 F.3d at 831.

There is also no evidence that Google acted with intent to assist government agents rather than to further its own purposes. Cathy McGoff, Senior Manager, Law Enforcement and Information Security at

Google, stated Google's terms of service prohibit using Google's services in violation of law. McGoff Decl., ECF No. 73-2 at 1. The terms of service also provide that Google "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." *Id*. at 1-2. McGoff explained that Google has a "strong business interest in enforcing our terms of service and ensuring that our services are free of illegal content, including in particular child sexual abuse material." *Id*. at 2. For this reason, Google "independently and voluntarily take[s] steps to monitor and safeguard our services against this content because users will stop using our services if they become associated with being a haven for abusive content." *Id*. Google discovered the images using its own hash values and reviewers, and the searches furthered Google's own business interests. *Id*. at 3. Forwarding the images to NCMEC consistent with § 2258A did not make Google a government actor, nor does it indicate that Google acted with intent to aid law enforcement.

Ringland argues that Google's intent to aid law enforcement is demonstrated by its accelerated investigatory efforts after the initial report to NCMEC and the fact that Google connected Ringland's two email addresses. Ringland argues that "protracted, independent investigatory acts suggest that Google remained an active participant in this investigation well beyond the initial CyberTips." Yet Ringland cites no authority to support his theory that once a private actor becomes aware of potentially illegal conduct it must cease further investigation. After Google became aware of potential issues with Ringland's accounts, it reasonably investigated to determine whether there

were other potential violations of the terms of service. These actions furthered Google's legitimate business interests and Google did not violate the Fourth Amendment by fulfilling its reporting requirements under § 2258A.

Finally, there is no evidence that the government knew of or acquiesced to Google's conduct, giving rise to any violation the Fourth Amendment. As the Magistrate Judge noted, "voluntary efforts to achieve a goal that it shares with law enforcement do not, by themselves, transform the company into a government agent." F&R, ECF No. 74 at 10 (quoting *Stevenson*, 727 F.3d at 831). Although Google actively investigated and reported information about Ringland's accounts, there is no evidence that it did so at the request of government officials.

B. NCMEC

Ringland argues that even if Google was not a government actor, NCMEC violated the Fourth Amendment when it expanded the searches initiated by Google. The Eighth Circuit has not addressed this subject, but other circuits have. The Tenth Circuit concluded that NCMEC is a government agent when it expands upon the scope of a service provider's investigation without a warrant. *See United States v. Ackerman*, 831 F.3d 1292, 1306–07 (10th Cir. 2016). Conversely, where the NCMEC only views files flagged as containing child pornography, it does not violate the Fourth Amendment. *United States v. Reddick*, 900 F.3d 636, 639–40 (5th Cir. 2018). The Magistrate Judge concluded there was no evidence that NCMEC viewed more files than those reviewed by Google. Ringland "strenuously objects" to the Magistrate Judge's conclusion, arguing that NCMEC

viewed several files that Google had not. *See* F&R, ECF No. 74 at 10.

In Alberico's affidavit supporting her initial warrant application, she stated that Google reviewed 502 of the 1,216 files submitted to NCMEC. *See* D.E. 109 at 7. The Magistrate Judge concluded that this case is like *Reddick* because Alberico stated she only reviewed those 502 files. Ringland objects to this conclusion because the executive summary of initial CyberTip reports refers to "over 700 uploaded files." D.E. 109 at 1. The Court infers that Ringland argues this case is more like *Ackerman* because NCMEC admitted it reviewed more files than Google reviewed.

The affidavit supporting the initial warrant relied on Google's and Alberico's review of the same files. Alberico acknowledged that the initial CyberTip reports included 1,216 files, but she affirmed that she viewed only the files already reviewed by Google. Thus, even if NCMEC viewed more than 502 files, the initial application relied only on the 502 files already reviewed by Google.

Ringland does not explain how NCMEC's review could have tainted the application. John Shehan,[4] Vice President of the Exploited Children Division of the NCMEC, testified that NCMEC is not required to

---

[4] Ringland objects to the Magistrate Judge's failure to find that Shehan's declaration was not credible. In support, Ringland offers Shehan's testimony in another case, *United States v. Miller*, No. CR 16-47-ART-CJS, 2017 WL 9325815 (E.D. Ky. May 19, 2017), *report and recommendation adopted*, No. CV 16-47-DLB-CJS, 2017 WL 2705963 (E.D. Ky. June 23, 2017), where Shehan failed to mention NCMEC's program that prevents NCMEC employees from reviewing files that had not been reviewed by the private service provider. Because NCMEC's program is not material to the Court's decision, the objection is overruled.

review any files, and that it does so in furtherance of its private mission to aid children. G.E. 1 at 4. Shehan testified that after compiling CyberTipline reports, NCMEC forwards them to law enforcement for review. *Id*. at 5. Although CyberTipline reports triggered an investigation in this case, the application and ensuing warrant relied on Alberico's statement that she reviewed only files reviewed by Google. Accordingly, the Magistrate Judge's conclusion was not erroneous.

III.Good Faith

Ringland objects to the Magistrate Judge's conclusion that the good faith exception to the exclusionary rule applies to this case. Even where probable cause is lacking, an exception to the exclusionary rule applies where officers rely on a warrant in good faith. *United States v. Hessman,* 369 F.3d 1016, 1019 (8th Cir. 2004). In *United States v. Leon,* 468 U.S. 897 (1984), the Supreme Court curtailed the use of the exclusionary rule as a remedy for unconstitutional searches and noted that the stated purpose of the exclusionary rule is "to deter *police* misconduct rather than to punish the errors of judges and magistrates." *Id*. at 916 (emphasis in original). "In the absence of an allegation that the magistrate abandoned his detached and neutral role, suppression is appropriate only if the officers were dishonest or reckless in preparing their affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause." *Id. at* 920.

There is no allegation that the issuing judge wholly abandoned a detached and neutral role. Nor is there evidence that law enforcement officers were dishonest or misleading in preparing the Affidavit. Instead,

Ringland argues that the good-faith exception does not apply in this case because the warrants were the product of illegal searches. For the reasons stated above, the Court concludes that the warrants were not illegal searches. Moreover, as addressed above, Albericio based her initial application on her own review of the files Google reviewed. Subsequent applications reasonably relied on information obtained under valid search warrants. Accordingly, the Magistrate Judge correctly concluded that the warrants were within the *Leon* good faith exception.

CONCLUSION

For the reasons discussed, the Findings and Recommendation will be adopted, and the Motions to Suppress and request for *Franks* hearing will be denied.

IT IS ORDERED:

1. The Findings and Recommendation, ECF No. 74, are adopted in their entirety;
2. The Motion to Suppress, ECF No. 47, and Motion to Suppress and Application for *Franks* Hearing, ECF No. 49, filed by the Defendant, Mark Ringland, are denied; and
3. The Objection to the Findings and Recommendation, ECF No. 75, is overruled.

Dated this 2nd day of January, 2019.

BY THE COURT:

s/Laurie Smith Camp
Senior United States District Judge

APPENDIX D

IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA, Plaintiff, vs. MARK RINGLAND, Defendant.	**8:17CR289** **FINDINGS AND RECOMMENDATION**

This matter is before the Court on the Motion to Suppress Evidence and Statements and Request for Evidentiary Hearing (Filing No. 47) and the Motion to Suppress, Application for *Franks* Hearing, and Request for Evidentiary Hearing and Oral Argument (Filing No. 49) filed by Defendant, Mark Ringland. Defendant filed briefs in support of both motions (Filing No. 48; Filing No. 50) and the government filed a brief in opposition (Filing No. 58).

The Court held an evidentiary hearing on Defendant's motions on July 19, 2018, and a transcript (TR.) of the hearing was prepared and filed on August 4, 2018. (Filing No. 68). Defendant was present with his attorney, Richard McWilliams. The government was represented by Assistant United States Attorney, Michael Norris. Mark Dishaw ("Deputy Dishaw"), a Deputy with the Douglas County Sheriff's Office and an assigned Investigator to the FBI Child Exploitation Task Force, testified on behalf of the government. The

Court received into evidence, without objection, Exhibit 1 (Declaration of John Shehan) and Exhibit 2 (DVD of seven (7) CyberTipline Reports) offered by the government, and Exhibits 101-163 offered by Defendant. (TR. 6, 56). Exhibits 101-108, 111-121, and 128-143 constitute thirty-five CyberTipline reports. Exhibits 109-110, 122-123, 124-125, and 126-127 constitute the four separate applications and warrants relevant to Defendant's motions.

The Court granted Defendant's oral request to file supplemental briefing following the evidentiary hearing; Defendant filed a supplemental brief on August 10, 2018, (Filing No. 70) and the government filed a supplemental brief on August 30, 2018, (Filing No. 73). The government's supplemental brief incorporates two attachments marked as "Exhibit 1" (Filing No. 73-1 - Google's Terms of Service) and "Exhibit 2" (Filing No. 73-2 - Declaration of Cathy A. McGoff).[1] This matter is now fully submitted to the Court. For the following reasons, the undersigned magistrate judge recommends that Defendant's motions be denied.

BACKGROUND

Defendant is charged in a two-count Indictment with receipt of child pornography and possession of child pornography under 18 U.S.C. §§ 2252(a)(2), (a)(4)(B) and (b)(2). (Filing No. 20). Investigator C.J.

---

[1] To avoid confusing these post-hearing exhibits with Exhibits 1 and 2 received at the evidentiary hearing, hereinafter, the post-hearing exhibits will be referred to by their filing numbers. The government requested that the evidentiary record remain open until all briefs were submitted, without objection, although the parties later agreed that a motion would be filed to reopen the record for the Court's consideration. (TR. 11, 57-58, 69).

Alberico ("Investigator Alberico") of the Nebraska State Patrol prepared a report (Exhibit 163) that "provides a pretty succinct timeline" of her investigation leading up to the charges being filed in this case. (TR. 55; Ex. 163). According to Investigator Alberico's report, Google, Inc. ("Google") first provided information to the National Center for Missing and Exploited Children ("NCMEC") that a user of Google's services "had uploaded over seven hundred (700) files suspected of depicting sexually explicit conduct involving a minor." Google identified the user by email address, mringland69@gmail.com, with associated telephone number 402-***-0642.[2] Several IP addresses were associated with the uploaded files, which NCMEC traced to Sprint PCS in Omaha, Nebraska. Based on this information, on April 17, 2017, NCMEC created seven CyberTipline Reports: #19083866, #19153972, #19938982, #19986242, #20035870, #20260729 and #20293287. (Ex. 163 at p. 1). Exhibit 2 includes these seven CyberTipline Reports containing the 502 images viewed by Investigator Alberico. (TR. 10). On May 12, 2017, Investigator Alberico submitted a preservation letter to Google for the email account mringland69@gmail.com. (Ex. 163 at p. 1).

Deputy Dishaw explained the general process of how CyberTipline reports are generated and provided to law enforcement. Deputy Dishaw testified that electronic service providers ("ESP") such as Google have proprietary methods to filter and identify known child

---

[2] On May 16, 2017, Investigator Alberico served a subpoena on Sprint to identify the subscriber information associated with telephone number 402-***-0642. Sprint identified the subscriber as "H. L.," residing at an address in Carter Lake, Iowa. Investigator Alberico's investigation ultimately did not link H.L. to this case. (Ex. 163 at p. 1).

pornography images based on hash values. (TR. 21-22, 24-25,51-53). The ESP will then view the file images and report potential violations to NCMEC, and then NCMEC will generate CyberTipline reports to send to law enforcement. (TR. 14-16). Deputy Dishaw testified that, particularly after the ruling in *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), investigators make sure that they are only reviewing files that the ESP reviewed first and reported to NCMEC. (TR. 16-17, 25-26, 52-53). Deputy Dishaw explained that if NCMEC is not clear whether the ESP reviewed a file, NCMEC will make a notation for the investigator, and then the investigator will contact the ESP to confirm whether or not the ESP viewed the file. Deputy Dishaw testified that if the ESP confirms it did not view the file, he will obtain a search warrant to view those files. (TR. 18).

Investigator Alberico continued to receive additional CyberTipline reports subsequent to the initial seven provided to her on April 17, 2017. On June 23, 2017, Investigator Alberico received CyberTipline Report #20437297, which Google had previously submitted to NCMEC.[3] On June 27, 2017, Investigator Alberico prepared a Douglas County search warrant affidavit, search warrant and non-disclosure order for the email account mringland69@gmail.com, associated with telephone number 402-***-0642. (Ex. 163 at pp. 1-2; Ex. 109-110). In obtaining the warrant, Investigator Alberico averred that Google "reviewed five hundred and two (502) files from the CyberTips sub-

[3] Investigator Alberico's affidavit dated August 7, 2017, submitted with an application for a search warrant in Douglas County states that the two images from the June 23, 2017, CyberTip (#20437297) were not viewed by Google. (Ex. 122 at p. 6).

mitted" and that she "only viewed files that were reviewed by Google . . . to confirm they depicted child pornography." (Ex. 109 at p. 7). On the same date, Investigator Alberico submitted the warrant electronically to Google through the Law Enforcement Request System ("LERS"). (Ex. 163 at p. 2).

On July 14, 2017, Investigator Alberico received the contents requested by the search warrant via FedEx from Google and saved the data to a digital case file. In reviewing the data, Investigator Alberico observed that email address mringland69@gmail.com had sent child erotica photographs and images of child pornography to the email address mringland65 @gmail.com. (Ex. 163 at p. 2). On the same date, the South Dakota Bureau of Criminal Investigation ("SDBCI") contacted Investigator Alberico by email stating that it had received information from NCMEC that a case the SDBCI was working on was linked to Alberico's case. On July 19, 2017, Investigator Alberico received CyberTipline reports #21681475 and #22346425, which were originally assigned to the SDBCI.[4] These CyberTipline reports listed the email address markringland65@gmail.com, with associated telephone 402-***-0902, and a secondary email address, mringland69@gmail.com. NCMEC traced several of the IP addresses associated with the uploaded files to Sprint PCS in the Omaha area, and Google provided the name "Mark Ringland" associated with the two email addresses. (Ex. 163 at p. 2). Pursuant to a subpoena served by Investigator Alberico on July 20, 2017, Sprint identified the subscriber of telephone number 402-***-0902 as Mark Ringland, residing at

[4] Investigator Alberico averred that neither she nor Google reviewed these files. (Ex. 122 at p. 7).

1904 Pleasantview Ln, Bellevue, Nebraska 68005. On August 4, 2017, Investigator Alberico submitted a preservation letter to Google for the email account markringland65@gmail.com, associated telephone number 402-***-0902. (Ex. 163 at pp. 2-3).

On August 7, 2017, Investigator Alberico received nine more CyberTipline reports: #22968026, #22968382, #22968534, #23001904, #23002061, #2302151, #23002255, #23043174 and #23043630, all of which were associated with the email address markringland65@gmail.com.[5] NCMEC traced some of the associated IP addresses to Sprint PCS, in the Omaha, Lincoln, and Grand Island, Nebraska areas. On the same date, Investigator Alberico prepared a Douglas County search warrant affidavit, search warrant, and non-disclosure order for the email accounts mringland65@gmail.com and markringland65@gmail.com, associated with telephone number 402-***-0902. (Ex. 122-123).

On August 14, 2017, Investigator Alberico received five additional CyberTipline reports, #23245909, #23274478, #23249764, #23249764 and #23068622, and on August 25, 2017, received six more, #23411893, #23488795, #23512952, #23545730, #23588762 and #233890937. All the reports were associated with email addresses markringland65 @gmail.com and mringland69@gmail.com, and the telephone number 402-***-0902. (Ex. 163 at p. 4).

On August 18, 2017, Investigator Alberico received the search warrant response via LERS from Google and saved the data to a digital case file maintained at

---

[5] Investigator Alberico averred that neither she nor Google reviewed these files. (Ex. 126 at p. 13).

her office. (Ex. 163 at pp. 3- 4). According to Investigator Alberico, several of the files contained images and/or videos of suspected child pornography and bestiality. (Ex. 124 at p. 10). Based on the information obtained during her investigation, on August 31, 2017, Investigator Alberico applied for a United States District Court search and seizure warrant affidavit, search warrant, and non-disclosure order for a cellular ping order for telephone number 402-***-0902, which was presented to and signed by a United States Magistrate Judge. (Ex. 124-125; Ex. 163 at p. 4).

On September 1, 2017, Investigator Alberico prepared a United States District Court search warrant affidavit for Ringland's person and cellular telephone, phone number 402-***-0902, (Ex. 126-127), and a criminal complaint (Filing No. 1) and arrest warrant (Filing No. 3), which were signed by the undersigned magistrate judge. On the same date, members of the CETF, FBI, Nebraska State Patrol, and Douglas County Sheriff's Office implemented a search warrant at 16406 Taylor Street in Omaha, and arrested Ringland pursuant to the warrant. According to Investigator Alberico's report, Ringland was read his *Miranda* rights, which he waived, and consented to an interview. (Ex. 163 at p. 4). Investigator Alberico further indicated in her report that on September 5, 2017, Ringland made spontaneous statements to the US Marshals transporting him for his initial hearing. (Ex. 163 at pp. 4-5).

On September 5, 2017, Investigator Alberico received five more CyberTipline reports: #2360300, #23625155, #23660907, #23697631, and #23729375, which were associated with the email addresses markringland65@gmail.com and mringland69@gmail

.com, and telephone number 402-***-0902. (Ex. 163 at p. 5). The Indictment was filed in this case on September 19, 2017. (Filing No. 20).

Defendant has filed the instant motions seeking suppression of all evidence seized during the investigation from the searches of his email accounts and any incriminatory statements he made after his arrest and during transportation to his initial appearance. (Filing Nos. 47, 49; TR. 55-56). Defendant argues that Google acted as a government agent when it searched his emails without a warrant and forwarded those contents to NCMEC, that NCMEC expanded upon Google's warrantless searches, and that the warrants obtained by Investigator Alberico were supported in substantial part by such warrantless searches. (Filing No. 47 at pp. 1-2). Defendant also seeks suppression of evidence and a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), arguing that the warrants were issued upon misleading applications that omitted material information. Defendant separately argues that the applications in support of the warrants included information obtained by unconstitutional searches by government agents, and that no probable cause exists if that information was excluded from the warrant application. (Filing No. 49 at p. 1).

ANALYSIS

A. Defendant's Request for *Franks* Hearing

Defendant argues he is entitled to a *Franks* hearing both because material facts were intentionally omitted from the four search warrant applications and because the four search warrant applications included information and evidence that had been obtained through unconstitutional warrantless searches

by Google and NCMEC. (Filing No. 49 at p. 3). A criminal defendant may request a hearing to challenge a search warrant on the ground that the supporting affidavit contains factual misrepresentations or omissions relevant to the probable cause determination. See *Franks*, 438 U.S. at 155-56. In order for a defendant to prevail on a request for a *Franks* hearing, the defendant must make a "substantial preliminary showing" that (1) the affiant "knowingly and intentionally" made reckless false statements or omissions and (2) if the false information is excised (or the omitted information is included), the affidavit no longer establishes probable cause. *United States v. Snyder*, 511 F.3d 813, 816 (8th Cir. 2008). "The requirement of a substantial preliminary showing is not lightly met[.]" *United States v. Arnold*, 725 F.3d 896, 898 (8th Cir. 2013)(quoting *United States v. Mathison*, 157 F.3d 541, 548 (8th Cir. 1998)).

Defendant first contends he is entitled to a *Franks* hearing because Investigator Alberico recklessly omitted from her warrant applications the fact that there were other geographic locations and IP addresses associated with the images in the CyberTipline reports. (Filing No. 50 at p. 2). Specifically, Defendant asserts that although the initial eight CyberTiplines supporting the June 27, 2017, warrant application contained two IP addresses that were traced to Sprint PCS in Omaha, several other IP addresses were associated with Des Moines, Chicago, Cleveland/Akron, the Quad Cities, and Minneapolis. (*Id.* at pp. 5-6). Defendant contends that the August 7, 2017, warrant application similarly omitted the material information that the two tips forwarded from the SDBCI were associated with IP addresses in Des Moines, Grand Island, and Chicago, and that the other nine tips reported IP

addresses in Dannebrog, Nebraska, Watertown, South Dakota, Grand Island, and Raymore, Missouri. Defendant also states the August 7, 2017, application recklessly omitted the fact that, out of "the 11 CyberTips and 1113 files recounted in the application, NCMEC identified only 22 as 'apparent child pornography' and labeled 1087 as 'uncategorized.'" (*Id.* at pp. 6-7). Likewise, Defendant asserts the August 31, 2017, ping warrant application omitted "dozens" of other IP addresses in ten other metropolitan areas and did not mention that "only 1.9% of those 1,109 files had been characterized as 'apparent child pornography' and 98.1% were deemed '"uncategorized."' (*Id.* at p. 7). Finally, Defendant argues the September 1, 2017, warrant application repeated all of the above omissions and also included "fruits of the receipts" from those warrants. (*Id.* at p. 8).

Upon review, the undersigned finds that Defendant has failed to demonstrate that the above omissions were material or necessary to a finding of probable cause. First, the omission of other IP addresses contained in the CyberTipline reports from Investigator Alberico's affidavits did not render the application materially misleading. Deputy Dishaw explained the difference between IP addresses assigned to a fixed tower as opposed to a mobile device. Deputy Dishaw testified that a fixed tower IP address can be geolocated to a certain area, whereas mobile service providers "have a limited number of IP addresses and cannot provide for every single customer of theirs an IP address," and therefore may need to assign an IP address from a different jurisdiction to a mobile user. (TR. 34-35; 53-54). Unlike a fixed tower IP address, therefore, a mobile IP address does not necessarily indicate the mobile user was accessing the internet in a

certain geographic area; for example, a mobile user in Omaha may be assigned an IP address from Atlanta if one of the predetermined number of Omaha IP addresses were unavailable. (TR. 54). Moreover, as recognized by the government, Defendant is overstating the significance of the IP addresses to the finding of probable cause. (Filing No. 58 at p. 7). In this case, the CyberTipline reports identified email addresses and a phone number conclusively owned by Defendant which were associated with the files that triggered Google's reporting, making it very likely that a judge would have found sufficient probable cause to issue the warrant even had information about the other IP addresses been included in the affidavits. Therefore, the undersigned finds that any omitted information regarding the additional IP addresses would not have impacted the finding of probable cause in this case. See, e.g., *United States v. Miller*, No. 8:15CR172, 2015 WL 5824024, at *3 (D. Neb. Oct. 6, 2015)(rejecting similar argument that omission of other IP addresses from CyberTipline Reports rendered warrant application misleading).

Defendant's argument that the warrant applications recklessly omitted the breakdown of how many files were identified by NCMEC as "uncategorized" versus "apparent child pornography" is also unavailing. Deputy Dishaw explained the differences in NCEMC designations of "apparent child pornography" versus "uncategorized." Deputy Dishaw testified that "apparent" child pornography files have been flagged by hash values, whereas "uncategorized" means the file was identified in manner other than by hash value; the fact that the file is labeled "uncategorized" does not exclude it from being child pornogra-

phy. (TR. 52-53). More importantly, Investigator Alberico averred in her warrant application that she reviewed 502 images identified and viewed by Google, and confirmed they depicted child pornography. Accordingly, the fact that NCMEC designated other files as "uncategorized" has no bearing on the finding of probable cause, and as such, its omission from the warrant applications was not misleading.

Defendant's second argument in support of his request for a *Franks* hearing is tied to his separate motion to suppress (Filing No. 47); he contends that Google and NCMEC were state actors for purposes of the Fourth Amendment and that therefore their warrantless searches of his personal email and phone numbers were unconstitutional, and that such unconstitutionally obtained evidence impermissibly formed the "the entirety" of the probable cause supporting the warrants. (Filing No. 50 at p. 2). The undersigned will address Defendant's arguments in detail below, but in short, finds that the searches of Defendant's email and phone numbers were constitutional under the Fourth Amendment. Accordingly, the inclusion of such evidence in the warrant applications was not reckless or otherwise improper. Therefore, the undersigned recommends Defendant's request for a *Franks* hearing be denied.

B. Motion to Suppress Evidence

Defendant argues that his Fourth Amendment rights were violated when Google searched his email accounts without a warrant, and that all evidence obtained directly or indirectly from that search and the several subsequent searches should be suppressed.

The Fourth Amendment only applies to state action and its protection against unreasonable searches

and seizures "is wholly inapplicable to a search or seizure . . . effected by a private individual not acting as an agent of the Government." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). Defendant contends that Google effectively acted as a government agent under the Fourth Amendment when it undertook repeated searches of his email accounts and reported suspected child pornography to NCMEC. (Filing No. 48 at p. 3).

As previously discussed by the Eighth Circuit Court of Appeals, an internet service providers' fulfillment of child pornography reporting requirements under 18 U.S.C. § 2258A, standing alone, "does not transform an Internet service provider into a government agent whenever it chooses to scan files sent on its network for child pornography." *United States v. Stevenson*, 727 F.3d 826, 830 (8th Cir. 2013)(concluding AOL did not act as a government agent when it scanned a user's e-mail and reported apparent child pornography to NCMEC). Recognizing this Eighth Circuit precedent, Defendant asserts that *Riley v. California*, 134 S. Ct. 2473 (2014) has implicitly affected the decision in *Stevenson* because the Supreme Court "held that law enforcement needs a warrant before they can search the content of an individual's cell phone." (Filing No. 58 at p. 4). While the Supreme Court in *Riley* makes it clear that *law enforcement* generally needs to obtain a search warrant before searching data on cell phones, the decision in *Riley* does not address or discuss the propriety of a search by a private party such as Google. In this case, it is undisputed that Google is a private, for profit entity. Google's Senior Manager of Law Enforcement and Information Security submitted a sworn declaration indicating that Google implemented its "proprietary

hashing technology" based on its "private, non-governmental interests" and based on its "strong business interest in enforcing our terms of service and ensuring that our services are free of illegal content, including[,] in particular[,] child sexual abuse material." (Filing No. 73-2 at p. 2). A private internet service provider's "voluntary efforts to achieve a goal that it shares with law enforcement do not, by themselves, transform the company into a government agent." *Stevenson*, 727 F.3d at 831. The undersigned therefore concludes Google simply complied with its statutory duty to report violations of child pornography laws and did not become a state actor by conducting its own searches of Defendant's email accounts to protect its own private, non-governmental interests.

Defendant next argues that, even if the Court concludes that Google's searches fall under the private search doctrine, his Fourth Amendment rights were nevertheless violated because NCMEC expanded upon Google's private search. (Filing No. 48 at pp. 5-6). Defendant relies on *United States v. Ackerman,* 831 F.3d 1292 (10th Cir. 2016), wherein the Tenth Circuit concluded that NCMEC is a government agent that violated the Fourth Amendment by expanding upon the scope of a private internet service provider's investigation without a warrant. In *Ackerman*, the undisputed facts established that NCMEC opened and viewed information other than the image flagged by AOL's hash values as known child pornography and had not been previously examined by AOL. Therefore, the Tenth Circuit found that NCMEC exceeded, and did not merely repeat, the internet service provider's private search in violation of the Fourth Amendment. See *Ackerman*, 831 F.3d at 1306-07; see *United States v. Boyer*, 914 F.2d 144, 146 (8th Cir.

1990)("[T]he government may not exceed the scope of the private search unless it has the right to make an independent search[.]"). Conversely, in *United States v. Reddick*, 900 F.3d 636, 637 (5th Cir. 2018), the Fifth Circuit found that law enforcement did not violate the Fourth Amendment because the investigator "reviewed only those files whose hash values corresponded to the hash values of known child pornography images" as ascertained by the internet service provider's system. *Id.* at 640.

In this case, the undersigned finds that the evidence does not support Defendant's assertion that NCMEC viewed more files than those identified and reviewed by Google. Therefore, this case is more like *Reddick* than *Ackerman*. Between March 20, 2017 and April 18, 2017, Google identified and reported 1,216 instances of suspected child pornography linked to email accounts owned by Defendant to NCMEC. Google reported having viewed 502 of these files. In her affidavit, Investigator Alberico attested that she viewed the same 502 images that has been reviewed by Google. (Ex. 109 at p. 7). The evidence did not establish that NCMEC reviewed more files than those reviewed by Google, and it is clear that Investigator Alberico's review did not exceed the scope of the private search done by Google. Accordingly, the Fourth Amendment is not implicated, and the undersigned therefore recommends that Defendant's motion to suppress be denied.

Finally, Defendant argues that the good faith exception does not apply in this case. (Filing No. 70 at p. 39). An exception to the exclusionary rule applies where officers rely on a warrant in good faith. *United States v. Hessman*, 369 F.3d 1016, 1019 (8th Cir.

2004). "In the absence of an allegation that the magistrate abandoned his detached and neutral role, suppression is appropriate only if the officers were dishonest or reckless in preparing their affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause." *United States v. Leon*, 468 U.S. 897, 920 (1984). Even assuming that the warrantless searches performed by Google or NCMEC were found to be violative of the Fourth Amendment, the undersigned finds no evidence of deliberate, reckless, or grossly negligent conduct by law enforcement in relying on the warrants prepared based upon that information. When Investigator Alberio applied for an acquired the search warrants, she had no reason to believe that NCMEC had provided her with information procured in violation of Defendant's Fourth Amendment rights. The evidence reflects that Investigator Alberico submitted her applications for warrants based on her personal review of the 502 images she knew to have already been reviewed by Google, which formed the basis of the probable cause upon which the applications relied. Accordingly, the undersigned concludes that law enforcement acted reasonably and in good faith in relying on the warrants issued in this case.

Upon consideration,

IT IS HEREBY RECOMMENDED to Chief United States District Court Judge Laurie Smith Camp that:

1. Defendant's Motion to Suppress Evidence and Statements and Request for Evidentiary Hearing (Filing No. 47) be denied, and

2. Defendant's Motion to Suppress, Application for *Franks* Hearing, and Request for Evidentiary Hearing and Oral Argument (Filing No. 49) be denied.

Dated this 19th day of October, 2018.

BY THE COURT:

s/ Michael D. Nelson
United States Magistrate Judge

ADMONITION

Pursuant to NECrimR 59.2, any objection to this Findings and Recommendation shall be filed with the Clerk of the Court within fourteen (14) days after being served with a copy of this Findings and Recommendation. Failure to timely object may constitute a waiver of any such objection. The brief in support of any objection shall be filed at the time of filing such objection. Failure to file a brief in support of any objection may be deemed an abandonment of the objection.