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]

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

---

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

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-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

[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.

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.

---

[3]From August 4, 2017, to August 31, 2017, Google uploaded 566 more files from markringland65 to NCMEC, but none of this information went into any warrant application.

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 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 government, 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.