United States Court of Appeals for the Fifth Circuit

United States Court of Appeals
Fifth Circuit
FILED
December 30, 2021
Lyle W. Cayce
Clerk

No. 20-40752

UNITED STATES OF AMERICA,

Plaintiff—Appellee,

versus

STEPHEN SCOTT MEALS, JR.,

Defendant—Appellant.

Appeal from the United States District Court
for the Southern District of Texas
USDC No. 2:19-CR-36-1

Before OWEN, *Chief Judge,* and JONES and WILSON, *Circuit Judges*.

EDITH H. JONES, *Circuit Judge*:

Stephen Meals, then thirty-seven years old, used a Facebook messaging application to discuss with A.A., a fifteen-year-old, their previous sexual encounters and their plans for future encounters. Facebook discovered these conversations and forwarded a cyber tip to the National Center for Missing and Exploited Children (NCMEC). NCMEC reported to local law enforcement, which then obtained a warrant for Meals's

electronic devices and found child pornography. Meals, charged with several counts relating to his child exploitation, moved to suppress the evidence on the ground that Facebook and NCMEC are government agents. The district court denied his motion, and Meals pled guilty to production and possession of child pornography. On appeal, Meals persists in his contention that the court should suppress the messages and images. The conviction is AFFIRMED, because Facebook did not act as a government agent and NCMEC's search, assuming that it is a government agent, did not exceed the scope of Facebook's cyber tip.

I. BACKGROUND

Meals's run-in with the law began when Facebook decided on its own to surveil, collect, and review his private messages with fifteen-year-old A.A., which indicated that Meals and A.A. were in an active sexual relationship. Facebook decided that the messages violated its terms of service, its community standards, and probably federal law. In November 2018, after a Facebook employee reviewed the messages, Facebook sent copies to the NCMEC via a "cyber tip".

NCMEC reviewed the cyber tip before forwarding the messages to local law enforcement in Corpus Christi, Texas, where both Meals and A.A. lived. Detective Alicia Escobar of the Corpus Christi Police Department used the messages to obtain a search warrant for the Facebook accounts of Meals and A.A. The search revealed more conversations confirming Meals's sexual relationship with A.A. Detective Escobar then obtained a second warrant with the additional evidence to search Meals's electronic devices,

home, and a trailer. That search uncovered child pornography on Meals's devices, consisting primarily of images of A.A. that Meals apparently produced.

A grand jury indicted Meals in December 2019 on four counts of production of child pornography, in violation of 18 U.S.C. §§ 2251(a) and 2251(e) (Counts 1–4); and one count of possession of child pornography, in violation of 18 U.S.C. §§ 2252(a)(4)(B) and 2252(b)(2) (Count 5). Meals moved to suppress all the evidence. He argued that he had an expectation of privacy in his Facebook chats; that Facebook and NCMEC violated his Fourth Amendment rights as government agents when they searched his messages without a warrant; and that the exclusionary rule's good-faith exception was inapplicable. Following an evidentiary hearing, the district court denied Meals's motion under the private search doctrine. Specifically, the district court held that the search did not violate appellant's Fourth Amendment rights because Facebook was not the government or one of its agents, and even if NCMEC were a government agent, neither its conduct nor local law enforcement's review of Meals's messages exceeded the scope of Facebook's initial search.

Ultimately, Meals pled guilty on the condition he could appeal the denial of his suppression motion. The district court sentenced Meals to 600 months of imprisonment, followed by lifetime supervised release. Meals timely appealed. See FED. R. APP. P. 4(b)(1)(A).

II. Standard of Review

"When reviewing a denial of a motion to suppress evidence, [this court] review[s] the district court's factual findings for clear error and its legal conclusions, including the ultimate constitutionality of the actions of law enforcement, de novo." *United States v. Williams*, 880 F.3d 713, 717 (5th Cir. 2018). The facts underlying the suppression determination are reviewed in the light most favorable to the prevailing party, which in this case is the Government. *United States v. Powell*, 732 F.3d 361, 369 (5th Cir. 2013). Generally, the court "may affirm the district court's ruling on a motion to suppress 'based on any rationale supported by the record.'" *United States v. Wise*, 877 F.3d 209, 215 (5th Cir. 2017) (quoting *United States v. Waldorp*, 404 F.3d 365, 368 (5th Cir. 2005)).

III. Discussion

Under the private search doctrine, when a private actor finds evidence of criminal conduct after searching someone else's person, house, papers, and effects without a warrant, the government can use the evidence, privacy expectations notwithstanding. *United States v. Jacobsen*, 466 U.S. 109, 117, 104 S. Ct. 1652, 1658 (1984). In other words, if a non-government entity violates a person's privacy, finds evidence of a crime, and turns over the evidence to the government, the evidence can be used to obtain warrants or to prosecute. The rationale for this doctrine is obvious. The Fourth Amendment restrains the government, not private citizens. *Burdeau v. McDowell*, 256 U.S. 465, 475, 41 S. Ct. 574, 576 (1921).

There are two exceptions to the private search doctrine. First, the doctrine does not apply if the "private actor" who conducted the search was actually an agent or instrument of the government when the search was conducted. *See Coolidge v. New Hampshire*, 403 U.S. 443, 487, 91 S. Ct. 2022, 2048, 2049 (1971). If the private actor was such an agent or instrument, a warrant is required to authorize the search. *Id.* Second, if the government, without a warrant, exceeds the scope of the private actor's original search and thus discovers new evidence that it was not substantially certain to discover, the private search doctrine does not apply to the new evidence, and the new evidence may be suppressed. *See Walter v. United States*, 447 U.S. 649, 657, 100 S. Ct. 2395, 2402 (1980); *United States v. Runyan*, 275 F.3d 449, 463 (5th Cir. 2001).

To suppress evidence produced by a private actor's search under one of these exceptions, the defendant has the burden of proof by a preponderance. *Runyan*, 275 F.3d at 456. If the defendant's proof fails on either point, the private search doctrine permits use of the evidence privately gathered. *See Jacobsen*, 466 U.S. at 117, 104 S. Ct. at 1658.

Meals contends that the district court erred by refusing to find that (1) Facebook was a government agent when it reviewed his private messages and reported them to NCMEC; (2) NCMEC exceeded the bounds of permissible government action by reviewing the messages; and (3) the government violated Meals's Fourth Amendment rights under the chattel trespass doctrine. We address each argument in turn.

A.

Meals first contends that Facebook was a government agent, not a private actor, when it searched his messages, rendering the private search doctrine inapplicable. He cites no factual evidence in support of this argument, and it is contradicted by an affidavit of a Facebook officer. Instead, Meals relies on a statute that requires electronic communication service providers ("internet companies")[1] and remote computing services to send a cyber tip to NCMEC for all instances of child exploitation that they discover on their platforms. *See* 18 U.S.C. § 2258A(a).

Assuming that merely citing a statute in this context could satisfy his evidentiary burden, Meals's citation to § 2258A fails. Section § 2258A(a) mandates reporting child exploitation on internet platforms to NCMEC, but it neither compels nor coercively encourages internet companies to search actively for such evidence. In fact, subparagraph (f) of § 2258A states that "nothing in [§ 2258A] shall be construed to require a provider to—(1) monitor any user, subscriber, or customer of that provider; (2) monitor the content of any communication of any person described in paragraph (1); or (3) affirmatively search, screen, or scan for facts or circumstances described in sections (a) and (b)." Given this forceful statutory disclaimer that any search mandate is placed on internet companies, Meals's effort to

[1] "[E]lectronic communication service means any service which provides to users thereof the ability to send or receive wire or electronic communications[.]" 18 U.S.C. § 2510(15) (internal quotation marks omitted).

characterize Facebook as a mandatory government agent or instrument falls flat.[2]

Meals also asserts that this court has no test for determining whether a private actor acted as a government agent or instrument, that the district court chose the wrong test, and that if the district court had used the correct test it would have found that Facebook was a government agent. Specifically, Meals argues that the district court incorrectly relied on the First Circuit's test rather than that of the Sixth Circuit. *Compare United States v. Cameron*, 699 F.3d 621, 637 (1st Cir. 2012) (using a three-factor test to determine whether a private actor acted as a government agent), *with United States v. Hardin*, 539 F.3d 404, 419 (6th Cir. 2008) (using a two-factor test to determine whether a private actor acted as a government agent).[3] But we need not address what factors are applicable to the government agent exception because Meals offered no evidence suggesting that Facebook may be a government agent. There is no reason to hypothesize standards that could pertain to evaluating non-existent evidence. Because Meals's reliance on § 2258A(a) is misplaced, this contention fails.

---

[2] Section 2258A(e) reinforces this interpretation of § 2258A. Under § 2258A(e), internet companies face significant fines for failing to report "actual knowledge" of child exploitation. There are no such fines for internet companies who refrain from searching through their users' data to learn such knowledge.

[3] The Fifth Circuit has not adopted a government agent test, but the court has used such tests in similar cases when a guideline was necessary to help sort through the evidence. *See United States v. Pierce*, 893 F.2d 669, 673 (5th Cir. 1990) (utilizing a two-factor test to analyze a case-specific question of whether an airline's employees were acting as a private actor or government agent when they searched the defendant's bags).

B.

Meals next argues that NCMEC is a government agent that exceeded the scope of Facebook's search by reviewing the messages Facebook provided. Further, NCMEC's search was excessive because NCMEC was not substantially certain before reviewing the messages that they were not products of a reported cyber-attack, nor was it substantially certain that Meals and A.A. were, respectively, thirty-seven and fifteen years old. According to Meals's logic, NCMEC needed a warrant before reviewing Facebook's cyber tip.

Contrary to Meals's supposition, NCMEC is a private, nonprofit corporation, not a government entity. The government takes no position on this question, and like the district court, we need not do so either. But assuming arguendo that NCMEC is a government agent, NCMEC did not exceed the scope of Facebook's search by merely reviewing the identical evidence that Facebook reviewed and placed in a cyber tip. Cyber tips have "significant indicia of reliability," and the information contained in such tips is per se substantially certain. *United States v. Landreneau*, 967 F.3d 443, 453 (5th Cir. 2020). But regardless of the reliability of cyber tips, substantial certainty is required only when a government agent opens containers obtained in the private search but left unopened by the private party. *See Runyan*, 275 F.3d at 463. In such instances, the additional evidence must be suppressed unless the government was "substantially certain" that certain incriminating evidence would be in the unopened containers. Here, the cyber tip was the only thing NCMEC "opened," and it contained only the content

reviewed and forwarded by a Facebook employee. In a critical distinction from the *Ackerman* case on which Meals relies, NCMEC did not and could not open any non-existent unopened containers, emails, or attachments, and therefore could not have exceeded the scope of Facebook's search. *See United States v. Ackerman*, 831 F.3d 1292, 1306-07 (10th Cir. 2016). As a result, even if NCMEC were a government agent, its review of information obtained by a "search conducted by private citizens [did] not constitute a 'search' within the meaning of the Fourth Amendment" because the review was confined to the scope and product of the initial search. *Runyan*, 275 F.3d at 458 (quoting *United States v. Bomengo*, 580 F.2d 173, 175 (5th Cir. 1978)); *see also United States v. Reddick*, 900 F.3d 636, 639 (5th Cir. 2018).

Because Meals has not carried his burden concerning NCMEC's participation in the search, NCMEC's review of Facebook's cyber tip did not violate his Fourth Amendment rights.

C.

Finally, Meals contends that the district court erred by not applying the chattel trespass test, as set forth in *United States v. Jones*, 565 U.S. 400, 132 S. Ct. 945 (2012), rather than the reasonable expectation of privacy test, when it evaluated whether NCMEC violated Meals's Fourth Amendment rights. Meals urges that the district court should have relied on *Ackerman*, 831 F.3d at 1307-08, in which the Tenth Circuit evaluated the applicability of the chattel trespass test to the opening of a previously unopened e-mail attachment.

The chattel trespass test, like the reasonable expectation of privacy test, may be relevant when evaluating whether *government* actions run afoul of a person's possessory interests protected by the Fourth Amendment. Meals has not shown that Facebook acted on behalf of the government. Thus, the original search was privately conducted. But even if NCMEC is a government actor, that organization did not access an original file or even a copy thereof that Meals possessed, consequently, there could be no governmental "trespassing of a chattel" like the court found in *Ackerman*. In *Ackerman,* as was just explained, NCMEC opened images attached to an email that had been intercepted *before* it got to the intended recipient, and NCMEC's analyst expanded the scope of the private search by opening those previously unopened attachments and an unopened email. *Id.* Accordingly, the chattel trespass test was not violated in this case.

IV. Conclusion

Because Meals has not carried his burden to show that Facebook is a government agent or instrument, the private search doctrine applies. Later investigative techniques employed by NCMEC and government officials did not impermissibly expand the scope of the original search. The district court correctly denied Meals's motion to suppress, and the conviction is Affirmed.