APPENDIX A

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.

APPENDIX B

United States Court of Appeals for the Fifth Circuit

United States Court of Appeals
Fifth Circuit
FILED
March 3, 2022
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

ON PETITION FOR REHEARING

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

PER CURIAM:

IT IS ORDERED that the petition for rehearing is DENIED.

APPENDIX C

Case No. 20-40752

UNITED STATES OF AMERICA,

Plaintiff – Appellee

v.

STEPHEN SCOTT MEALS, JR.,

Defendant – Appellant

IN THE
UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

Appeal from the United States District Court
for the Southern District of Texas

BRIEF FOR APPELLANT

DERLY J. URIBE
Attorney for Appellant
Law Offices of
Francisco J. Saldaña, Jr.
217 W. Village Blvd., Suite 3
Laredo, Texas 78041
Telephone: (956) 726-1631
Fax: (956) 726-4158

CERTIFICATE OF INTERESTED PERSONS

United States v. Stephen Scott Meals, Jr.
No. 20-40752

The undersigned counsel of record certifies that the persons having an interest in the outcome of this case are those listed below:

1. **Stephen Scott Meals, Jr.**, Defendant-Appellant;

2. **Carmen Castillo Mitchell**, U.S. Attorney;

3. **Brittany Lee Jensen and Andrew Gould**, Assistant U.S. Attorney, who represented Plaintiff-Appellee in the district court;

4. **Scott F.C. Lemanski**, Counsel who represented Defendant-Appellant in the district court; and

6. **Derly J. Uribe**, Court-Appointed Counsel who represents Defendant-Appellant in this Court.

This certificate is made so that the judges of this Court may evaluate possible disqualification or recusal.

s/Derly Joel Uribe
DERLY JOEL URIBE
Attorney for Defendant-Appellant

REQUEST FOR ORAL ARGUMENT

Defendant-Appellant, Stephen Scott Meals, Jr., requests oral argument pursuant to Federal Rule of Appellate Procedure 34(a) and Fifth Circuit Rule 34.2.

TABLE OF CONTENTS

TABLE OF CITATIONS

Page

CASES

TABLE OF CITATIONS-(Cont'd)

STATUTES AND RULES

STATEMENT OF JURISDICTION

1. **Subject Matter Jurisdiction in the District Court.** This case arose from the prosecution of alleged offenses against the laws of the United States. The district court exercised jurisdiction under 18 U.S.C. § 3231.

2. **Jurisdiction in the Court of Appeals.** This is a direct appeal from a final decision of the United States District Court for the Southern District of Texas, entering a judgment of criminal conviction. This Court has jurisdiction of the appeal under 28 U.S.C. § 1291 and 18 U.S.C. § 3742(a).

Under Fed. R. App P. 4(b), a criminal defendant who wishes to appeal a district court judgment must file notice of appeal in the district court within 10 days after the entry either of the judgment or order appealed from, or a notice of appeal by the Government. Rule 4(b)(2) further states that "[a] notice of appeal filed after the court announces a decision, sentence, or order—but before the entry of the judgment or order—is treated as filed on the date of and after the entry." In this case, the written judgment was signed on October 29, 2020, and Mr. Meals filed his notice of appeal on November 6, 2020. This appeal is therefore timely.

ISSUE PRESENTED FOR REVIEW

Whether the district court committed reversible error by denying Mr. Meals' motion to suppress the evidence.

STATEMENT OF THE CASE[1]

A. Course of proceedings and disposition in the court below.

On December 11, 2019, a federal grand jury in the Southern District of Texas returned a five count superseding indictment charging Mr. Meals with four counts of production of child pornography (Counts 1-4) in violation of 18 U.S.C. § 2251(a), 2251(e), and one count of possession of child pornography (Count 5) in violation of 18 U.S.C. § 2251(a), 2252(a)(4)(B) and 2252(b)(2). ROA.353-357. Mr. Meals filed a motion to suppress all the evidence on the basis that all the evidence in support of the charges against him was obtained by an unconstitutional search and seizure. ROA.54-59. Mr. Meals further argued that all the evidence seized by the Government should also be suppressed pursuant to the "fruit of the poisonous tree" doctrine. ROA.475.

The district court held an evidentiary hearing on the motion to suppress on February 4, 2020, and denied it that same day. ROA.590, 635. The district court subsequently entered a written order denying the motion to suppress. ROA.539-545. On February 20, 2020, pursuant to a

[1] The record on appeal for the trial is cited as "ROA. [page]."

written plea agreement, Mr. Meals entered a conditional guilty plea to Counts One (production of child pornography) and Five (possession of child pornography), reserving "the right to take an appeal from the judgment on the issue of the denial of Defendant's Motion to Suppress Evidence in this case." ROA.869 (plea agreement); *see also* ROA.644, 662. In exchange for his promise to plead guilty to Counts One and Five, the government agreed that, at sentencing, it would: recommend a prison sentence within the applicable guideline range and that he receive full credit for acceptance of responsibility if he qualifies, and move to dismiss the remaining counts. ROA.869-870.

On October 28, 2020, the district court sentenced Mr. Meals to a 600 month term of imprisonment and a life term of supervised release. ROA. 560-562, 669, 803. It did not impose a fine, but it did impose $10,200 in special assessments. ROA.564, 803-805. And on the government's motion, the district court dismissed the remaining counts (Counts, Two, Three and Four). ROA.560. Mr. Meals filed a timely notice of appeal. ROA.566.

B. Relevant factual history.

The facts relevant to the motion to suppress and to this appeal, discussed below, were established at the evidentiary hearing held on

February 4, 2020 and are for the most part undisputed. ROA.590-640. The charges made against Mr. Meals are based on private chats that took place in October 2018 on Facebook Messenger, (hereinafter "the Private Chats"). ROA.810-815, 854. Facebook reviewed the Private Chats, and on November 6, 2018 reported them to the National Center for Missing and Exploited Children ("NCMEC"), in what is referred to as a CyberTip. ROA. 540. The CyberTip further provided the Facebook accounts, usernames, dates of birth, genders, emails, addresses, telephone numbers, and IP addresses of those associated with the Private Chats. ROA.540.

The CyberTip further reported to the NCMEC that the Private Chats contained sexually explicit conversations that appeared to be between an adult male in his thirties and a minor female who had expressed in the Private Chats to have engaged in sexual activity and were planning to do so again. ROA.540, 854. NCMEC then sent the CyberTip to the Texas Attorney General, who then forwarded it to the Corpus Christi Police Department ("CCPD") on November 7, 2018. ROA. 540. Based on the CyberTip, the CCPD applied for and obtained search warrants which yielded evidence against Mr. Meals including photographs found on his cellphone. ROA.541.

C. Basis of Appeal

Mr. Meals challenges the district court's order denying his motion to suppress.

SUMMARY OF THE ARGUMENT

The district court committed numerous errors when it considered Mr. Meals' motion to suppress. The first error the district court committed was its determination that Facebook did not act as an agent of the Government when it searched and reviewed the Private Chats. The district court erred in this regard because it did not apply the correct test. The district court further erred when it determined that the private search doctrine applied to NCMEC's search of the Private Chats. The district court erred in this regard because the district court relied upon case law that is materially distinguishable to the case at bar. The case law relied upon by the district court is materially distinguishable because those cases involved the online distribution of child pornography and not private chats sent on Facebook Messenger as in the case at bar. Finally, even if this Court determines that Mr. Meals' motion to suppress should have been determined pursuant to the chattel trespass test required by *U.S. v. Jones*, 565 U.S. 400, 409-410 (2012), the district court still committed reversible error in denying Mr. Meals' motion to suppress.

ARGUMENTS AND AUTHORITIES

I. The district court erred in denying Mr. Meals' motion to suppress.

A. Standard of Review.

With respect to a district court's denial of a motion to suppress, this Court reviews factual findings for clear error and conclusions of law *de novo*. *United States v. Rodriguez*, 702 F.3d 206, 208 (5th Cir. 2012); *United States v. Payne*, 341 F.3d 393, 399 (5th Cir. 2003).

B. Discussion

To show a Fourth Amendment violation, a defendant must first establish that the search invaded a legitimate expectation of privacy that society recognizes as reasonable. *See Minnesota v. Olson*, 495 U.S. 91, 95-96 (1990). The Supreme Court has admonished that "the most basic constitutional rule in this area is that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specially established and well-delineated exceptions.'" *Coolidge v. New Hampshire*, 403 U.S. 443, 454-55 (1971) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967). And the exceptions are to be "jealously and

carefully drawn." *Jones v. United States*, 357 U.S. 493, 499 (1958).

Federal courts have acknowledged the following facts regarding Facebook and Facebook Messenger:

> Facebook operates one of the largest social media platforms in the world, with over one billion active users. About seven in ten adults in the United States use Facebook. Facebook has a messaging function on its platform that allows users to send electronic messages to one or more users. Facebook explains on its website that these messages are 'private' because their contents and history are viewable only to the sender and his or her chosen recipients—in contrast to, for example, posts shared with a broader audience, such as all of the user's Facebook friends.

Campbell v. Facebook, Inc., 951 F.3d 1106, 1111-1112 (9th Cir. 2020). (Citations omitted). Since messages sent on Facebook Messenger are private communications as Facebook publicly represents to its users, Facebook Messenger is essentially the same as e-mail communications, which have Fourth Amendment protection from warrantless searches and seizures. *See United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010). (Emails have Fourth Amendment protection because email "is the technological scion of tangible mail, and it plays an indispensable part in the Information Age."); *see also City of Ontario v. Quon*, 130 S.Ct. 2619, 2631 (2010) (implying that "a search of [an individual's personal e-mail

account" would be just as intrusive as "a wiretap on his home phone line."). Given the stark similarities between email communications and Facebook Messenger communications, it would be non-sensical not to afford Facebook Messenger Fourth Amendment protections on par with emails. Indeed, even the Government stipulated that Mr. Meals had a reasonable expectation of privacy in the Private Chats. ROA.626 ("[The Court] can assume, as the 5th Circuit did in *Reddick*, that [Mr. Meals] did enjoy a legitimate expectation of privacy in these messages."). In light of the Government's stipulation, the district court agreed that Mr. Meals had a reasonable expectation of privacy in the Private Chats. ROA.542.

1. The district court erred in determining Facebook was an agent of the Government when it reviewed the Private Chats.

After determining that Mr. Meals had a reasonable expectation of privacy in the Private Chats, the district court then considered whether Facebook acted as an agent of the Government when it reviewed the Private Chats. ROA.542. The district court erred with respect to the test it applied in making this determination. *See* ROA.543. The proper test the district court should have applied is not the test applied by the First

Circuit (ROA.543), but the two part test adopted by the Sixth Circuit: "In the context of a search, the defendant must demonstrate two facts: (1) Law enforcement 'instigated, encouraged or participated in the search' and (2) the individual 'engaged in the search with the intent of assisting the police in their investigative efforts." *United States v. Hardin*, 539 F.3d 404, 419 (6th Cir. 2008)(quoting *United States v. Lambert*, 771 F.2d 83, 89 (6th Cir. 1985)).

Private parties like Facebook become government agents by virtue of their statutory obligations. ROA.544; *see also Skinner v. Railway Labor Executives' Ass'n*, U.S. 602, 615-16 (1989); *United States v. Ackerman*, 831 F.3d 1292, 1296 (10th Cir. 2016). Facebook has statutory reporting obligations pursuant to 18 U.S.C. § 2258A(a). *See also United States v. Landreneau*, 967 F.3d 443, 452-453 (5th Cir. 2020). Since Facebook had mandatory reporting legal obligations, and actually did report, one can easily see that: (1) the government encouraged the search; and (2) Facebook clearly intended to assist the police in their investigative efforts. For these reasons, the district court erred in concluding that Facebook was not required to obtain a warrant in accordance with the Fourth

Amendment to conduct the search it did of the Private Chats.

2. The district court erred in determining that the private search doctrine applied to NCMEC's search of the Private Chats.

If the Court determines Facebook did not act as an agent of the Government, the district court still erred in deciding that NCMEC, a government agent,[2] did not violate the Fourth Amendment pursuant to the private search doctrine. ROA.544 (citing *United States v. Runyan*, 275 F.3d 449, 458 (5th Cir. 2001) (citing *United States v. Bomengo*, 580 F.2d 173, 175 (5th Cir. 1978). The district court erred because *Runyan* and Supreme Court precedent actually supports Mr. Meals' position that the private search doctrine does not apply and does not absolve NCMEC from obtaining a warrant.

In its analysis of the private search doctrine, the district court failed to consider or scrutinize in any way the level of certainty NCMEC could have had that the Private Chats were actually what they purported to be. The district court erred because in order for NCMEC to conduct a

[2] The Government took no position on whether NCMEC is or is not a government actor. ROA.633-634. The district court assumed NCMEC is a government agent. ROA. 544.

warrantless search pursuant to the private search doctrine it needed to have been "virtually" or "substantially certain" that the Private Chats were in fact a communication between an adult male and a minor planning a sexual encounter. *See United States v. Jacobsen*, 466 U.S. 109, 119-20 (1984); *Runyan*, 275 F.3d at 463 (5th Cir. 2001) ("[O]pening a container that was not opened by private searchers would not necessarily be problematic *if the police knew with substantial certainty* ... what would be inside.") (emphasis added); *see also United States v. Lichtenberger*, 786 F.3d 478, 485-86 (6th Cir. 2015)("Under the private search doctrine, the critical measures of whether a governmental search exceeds the scope of the private search that preceded it are how much information the government stands to gain when it re-examines the evidence and, relatedly, *how certain it is regarding what it will find.*"). (Emphasis added).

NCMEC could not have known with any reasonable degree of certainty that the Private Chats were only limited to such improper communications and were in fact what they purported to be because the evidentiary record indicates it only *appeared* to Facebook that the Private

Chats were communications between an adult male and a minor female. The only evidence submitted with respect to what Facebook did and did not do regarding the Private Chats is contained in the affidavit of Raquel Morgan, an employee of Facebook, Inc. ROA.853-855. Said affidavit states *inter alia*: "On November 6, 2018, after a person had reviewed the interactions, Facebook submitted CyberTipline Report 42808969 to NCMEC, which reported that an adult male *appeared to be* enticing a minor female to engage in sexual activity." ROA.854. (Emphasis added).

Unlike cases involving pornographic images such as *Reddick* that involved government review of only illegal images, there is no evidence that Facebook took any measures to limit its review of only improper communications and that it did not delve into private communications beyond that. There is also no evidence Facebook did anything to verify that the relevant Facebook accounts were in fact what they purported to be including but not limited to doing anything to rule out that said accounts were not hacked or fake or that the participants in the Private Chats were actually not consenting adults engaging in role-playing. It further bears noting that the district court was informed of the

uncertainty aspects of the Private Chats before it denied Mr. Meals' motion to suppress. ROA.609-611, 631. The Government even went as far as to emphasize to the district court the significance of the "substantially certain" requirement of the private search doctrine:

> [T]he question there in *Reddick* was, well, by opening the image, did the Corpus Christi Police Detective, did he exceed the scope of the private search and the 5th Circuit answered no based on Supreme Court president [*sic*], namely *United States versus Jacobson*, [*sic*] because the officer could be *substantially certain* of what he would find inside of that image.

ROA.623. (Emphasis added).

It is further worth mentioning that in September 2018, the month before the Private Chats occurred, Facebook reported that cyber attackers breached its computer network which allowed the attackers to gain access to user accounts and take control of them. The attack was the largest in Facebook's history which exposed the personal information and accounts of nearly fifty million users.[3] The fact that Facebook had just experienced its largest attack in its history the month before the Private Chats occurred—which made its user accounts vulnerable to being

[3] *See* Isaac, M. and Frenkel, S., (2018, Sept. 28). Facebook Security Breach Exposes Accounts of 50 Million Users, *New York Times*. Retreived from http://www.nytimes.com

hacked—further bolsters the point that NCMEC could not have been virtually certain that the Private Chats were actually what they purported to be.

The applicable case law relied upon by the district court in denying Mr. Meals' motion to suppress, including *Jacobsen* and *Reddick* are materially distinguishable because the case at bar involves private chats and not the online distribution of child pornography. When child pornography is distributed online, private companies like Facebook rely on hash value matching technology to identify such content without relying on human searchers or intruding into the privacy of its users regarding other matters. *See United States v. Reddick*, 900 F.3d 636, 636-37, 639 (5th Cir. 2018). ("[O]pening the file [by the government] merely confirmed that the flagged file was indeed child pornography, as suspected. As in *Jacobsen*, 'the suspicious nature of the material made it *virtually certain* that the substance tested was in fact contraband.'"). (Emphasis added).

In other words, *Reddick* is distinguishable because the case at bar does not involve the distribution of child pornographic content. And

because it does not do so, it is erroneous to conclude, as the district court did, that NCMEC's review of the Private Chats was virtually certain to reveal the online solicitation of a minor and that its review was limited to only that. NCMEC's review of the Private Chats was not virtually certain to so reveal because, as established *supra*, there is no evidence that Facebook did anything to verify that the relevant Facebook accounts were in fact what they purported to be including but not limited to doing anything to rule out that said accounts were not hacked or fake or that the participants in the Private Chat were actually not consenting adults engaging in role-playing.

There is also no evidence that Facebook made any effort to determine if the relevant Facebook accounts had in fact been hacked as part of the largest cyber attack Facebook reported to have occurred in September 2018. Because it is irrefutable that the Private Chats could not have been virtually certain to have been what they purported to be at the time NCMEC received the CyberTip from Facebook, or that Facebook limited its search to only such communications, NCMEC, a government actor, cannot rely on the private search doctrine for the search it conducted of the Private Chats without a warrant. Accordingly, NCMEC's

warrantless search constituted a search and seizure in violation of the Fourth Amendment.

3. The district court erred even if this Court rules that Mr. Meals' motion to suppress should have been determined pursuant to the chattel trespass test and not the reasonable expectation of privacy test.

Mr. Meals further argues in the alternative that the district court erred in failing to apply the trespass test required by *United States v. Jones*, 565 U.S. 400 (2012) in determining whether NCMEC needed to obtain a warrant to view the Private Chats, as opposed to the "reasonable expectation of privacy test" it applied as required by *Jacobsen*:

> *Jones* explained that government conduct can constitute a Fourth Amendment search *either* when it infringes on a reasonable expectation of privacy *or* when it involves a physical intrusion (a trespass) on a constitutionally protected space or thing ("persons, houses, papers, and effect") for the purpose of obtaining information.

United States v. Ackerman, 831 F.3d 1292, 1307 (10th Cir. 2016). *Ackerman* clearly considered *Jones'* applicability in this regard, and since both Mr. Meals and the Government brought *Ackerman* to the district court's attention and both argued it was applicable to the case at bar, (ROA.632, 633), and the district court even cited it, (ROA.544), it cannot be argued

that it is being brought up for the first time on appeal.

Ackerman determined that NCMEC violated the Fourth Amendment when it reviewed private emails under the private search doctrine under *Jacobsen's* reasonable expectation of privacy test because there was no virtual certainty that the email itself and the other three attachments contained child pornography: "Indeed, when NCMEC opened Mr. Ackerman's email it could have learned any number of private and protected facts...." *Id.* at 1306. It bears noting however, that *Ackerman* further questioned whether *Jacobsen's* reasonable expectation of privacy analysis still applied in light of *Jones*:

> Given the uncertain status of *Jacobsen* after *Jones*, we cannot see how we might ignore *Jones's* potential impact on our case. And its impact here seems even cleaner than in *Jacobsen*. After all, we are not dealing with a governmental drug test that destroyed but a trace amount of potential contraband. We are dealing instead with the warrantless opening and examination of (presumptively) private correspondence that could have contained much besides potential contraband for all anyone knew. And that seems pretty clearly to qualify as exactly the type of trespass to chattels that the framers sought to prevent when they adopted the Fourth Amendment.

Id. at 1307.

Ackerman further determined that the application of the *Jones*

chattel trespass test further yielded the same conclusion–that NCMEC violated the Fourth Amendment when it opened and viewed Mr. Ackerman's email without a search warrant. *Id.* at 1308. *Ackerman* noted that email and regular mail are analogous in terms of having Fourth Amendment protection and further noted and cited "many courts that have already applied the common law's ancient trespass to chattels doctrine to electronic, not just written, communications. *Id.* Since Facebook Messenger is akin to email in that they both constitute electronic papers and effects worthy of Fourth Amendment protection, there is no reason not to apply *Ackerman's* and *Jones'* reasoning and holding to the case at bar. *See id.* And since Ackerman had Fourth Amendment protection when NCMEC had his email because Ackerman possessed a physical property right within the data of the email itself, so to did Mr. Meals in the Private Chats. Therefore, NCMEC's act of opening and reviewing the Private Chats, Mr. Meals' electronic papers and effects, constitutes a physical intrusion into a constitutionally protected space or thing. Accordingly, NCMEC violated the Fourth Amendment under the *Jones'* trespass to chattel theory as well. *See id.*

CONCLUSION

The district court erred in denying Mr. Meals' motion to suppress and not suppressing the Private Chats as well as all the other evidence obtained from the subsequent search warrants pursuant to the fruit of the poisonous tree doctrine. ROA.475; *Brown v. Illinois*, 422 U.S. 590, 602-604 (1975); *Wong Sun v. United States*, 371 U.S. 471, 484-488 (1963). Accordingly, the Court should reverse Mr. Meals' conviction.

Respectfully submitted,

s/Derly Joel Uribe
DERLY JOEL URIBE
Law Offices of Francisco J. Saldaña, Jr.
Attorney for Appellant
217 W. Village Blvd., Suite 3
Laredo, Texas 78041
Telephone: (956) 726-1631
Fax: (956) 726-4158

CERTIFICATE OF SERVICE

I hereby certify that a copy of the above and foregoing document was served on the U.S. Attorney's Office via ECM electronic mail on April 5, 2021, to those attorneys receiving service via ECM automatically. I further hereby certify that a copy of the above and foregoing document was served to the below named defendant at the below stated address via certified mail, 7018 0680 0001 0192 7099, return receipt requested:

Stephen Scott Meals
Register No. 74966-479
FCI JESUP
Federal Correctional Institution
2680 301 South
Jesup, GA 31599

s/ Derly Joel Uribe
Derly Joel Uribe

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of FED. R. APP. P. 32(a)(7)(B) because this brief contains 3,754 number of words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of FED. R. APP. P. 32(a)(5) and the type style requirements of FED. R. APP. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Corel WordPerfect Office X5 in Century Schoolbook 14 point font in text and Century Schoolbook 12 point font in footnotes.

s/ Derly Joel Uribe
DERLY JOEL URIBE
Attorney for Appellant
Dated: April 5, 2021