

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA**

UNITED STATES OF AMERICA,

Plaintiff,

v.

MATTHEW WILLIAM SCHWIER,

Defendant.

Case No. 3:17-cr-00095-SLG

**ORDER RE S-1 MOTION TO SUPPRESS EVIDENCE: COUNTS 3&4 OF
THE FOURTH SUPERSEDING INDICTMENT**

Before the Court at Docket 317 is Defendant Matthew William Schwier's S-1 Motion to Suppress Evidence: Counts 3 & 4 of the Fourth Superseding Indictment. The government's Response in Opposition is at Docket 325. The defense's Reply is at Docket 329. The defense did not request an evidentiary hearing on the motion.

BACKGROUND

On April 28, 2017, a magistrate judge issued a search warrant for the defendant's home.¹ The search warrant application was supported by an affidavit of FBI Special Agent Daryl Allison.² In the affidavit, Agent Allison states that twice on October 20, 2016, "an FBI agent working in an undercover capacity connected to a P2P [peer to peer] file sharing program" operating from an IP address later

¹ Docket 325-1 at 1.

² Docket 325-1 at 2-74.

associated with the defendant's computer.³ On each occasion, the undercover agent attempted to download data "uniquely identified by . . . info hash[es] . . . known to consist of photos and/or video containing child pornography."⁴ The undercover agent was not successful in downloading the data.⁵ The affidavit provides a narrative description of the content of several of the files that the agent was unable to download from the IP address, noting for each that "[n]o part of this video was received" by the FBI.⁶ The narrative descriptions are derived from archived law enforcement copies of the files.⁷

Agent Allison states in the affidavit that an undercover agent connected to a second IP address, also later associated with the defendant's computer, several times in November 2016.⁸ From November 20 to November 21, an undercover

³ Docket 325-1 at 27–34, ¶¶ 21–23. The affidavit describes peer-to-peer file-sharing in detail. Docket 325-1 at 27–28, ¶¶ 18–20. The affidavit also describes the process by which the IP address was identified as relating to the defendant. Docket 325-1 at 41–43, ¶¶ 31–36.

⁴ Docket 325-1 at 29–34, ¶¶ 22–23. The affidavit defines a "hash value" as "a mathematical algorithm generated against data to produce a numeric value that is representative of that data," and Agent Allison states that he is "unaware of any instance in which two files have been naturally assigned the same SHA-1 hash value." Docket 325-1 at 11, ¶ 10.b.v.

⁵ Docket 325-1 at 29–34, ¶¶ 22–23.

⁶ Docket 325-1 at 30–34, ¶¶ 22–23.

⁷ Docket 325-1 at 39–41, ¶¶ 27–29. According to the affidavit, "[t]hese [archived] files are verified to be identical to the files described by the torrent by hashing algorithms." Docket 325-1 at 40, ¶ 20.

⁸ Docket 325-1 at 34–39, ¶¶ 24–26.

agent made two unsuccessful attempts to download data identified by info hashes “known to consist of photos and/or videos containing child pornography.”⁹ The affidavit provides a narrative description of several of these files, noting again that “[n]o part of this video was received” by the FBI.¹⁰ The affidavit states that from November 22 to November 24, an undercover agent made a third, successful attempt to download data from the second IP address.¹¹ The undercover agent downloaded two complete files, reviewed them, “and determined that one of the files contained child pornography.”¹² Agent Allison’s affidavit provides a narrative description of this file, and notes that “[t]his image is being made available to the magistrate judge to review at the time the warrant is sworn.”¹³

Although Agent Allison’s affidavit does not name the forensic software used by the FBI agent to connect to the IP addresses associated with the defendant—later identified as Torrential Downpour—it describes the program as follows: “This P2P program identifies other computers on the network that are sharing image and video files of child pornography. The program identifies these files by

⁹ Docket 325-1 at 34–37, ¶¶ 25–26.

¹⁰ Docket 325-1 at 34–38, ¶¶ 25–26.

¹¹ Docket 325-1 at 38–39, ¶ 26.

¹² Docket 325-1 at 38, ¶ 26.

¹³ Docket 325-1 at 38–39, ¶ 26.

comparing hash values of previously identified images and videos of child pornography with the hash values being shared on the network.”¹⁴ Agent Allison also identifies in the affidavit several limitations of the Torrential Downpour software and provides several explanations for why the program may have been unable to download the majority of the data it sought from the two subject IP addresses.¹⁵

The magistrate judge issued the search warrant,¹⁶ which the FBI executed on May 1, 2017.¹⁷ The government subsequently charged the defendant with multiple counts of possession, distribution, and receipt of child pornography. The Fourth Superseding Indictment, filed on December 19, 2019, contains four counts.¹⁸ Counts 1 and 2 respectively charge possession and distribution of child pornography and stem from the government’s use of Torrential Downpour to identify files on the defendant’s computer.¹⁹ Counts 3 and 4 respectively charge possession and receipt of child pornography and stem from physical evidence

¹⁴ Docket 325-1 at 29, ¶ 21.

¹⁵ Docket 325-1 at 39–41, ¶¶ 27–30.

¹⁶ Docket 325-1 at 1.

¹⁷ Docket 317 at 6; Docket 325 at 4.

¹⁸ Docket 279.

¹⁹ Docket 279 at 2.

seized from defendant's premises on May 1, 2017, pursuant to the search warrant.²⁰

On November 8, 2019, the Court granted the defense's motion to compel production of Torrential Downpour, finding that defense testing of the software was material to the defense of Counts 1 and 2 of the indictment then in place.²¹ The government ultimately decided to dismiss Counts 1 and 2 rather than produce Torrential Downpour to the defense for testing; the Court granted the government's motion to dismiss those counts on February 3, 2020.²² The defense filed the instant motion to suppress on February 12, 2020.²³

DISCUSSION

The defense contends that "the search warrant was issued without probable cause" and that "the search violated the defendant's rights under the fourth and fifth amendments."²⁴ As such, the defense requests that "[t]he evidence seized

²⁰ Docket 279 at 3. The government's briefing explains that evidence indicating that child pornography that had been downloaded to defendant's computer but deleted prior to the May 1, 2017 search "led to Count 4 of the Fourth Superseding Indictment." Docket 325 at 5.

²¹ Docket 243 at 3–7. Counts 1 and 2 of the Third Superseding Indictment, filed April 25, 2019, are not materially different from Counts 1 and 2 of the Fourth Superseding Indictment. *Compare* Docket 138 (Third Superseding Indictment) *with* Docket 279.

²² Docket 314. The subsequent Judgment of Partial Discharge is at Docket 315.

²³ Docket 317.

²⁴ Docket 317 at 11.

under the warrant . . . be suppressed as fruit of the poisonous tree.”²⁵ The defense analogizes Torrential Downpour to a confidential informant and notes that “[w]hen the information contained in the [probable cause] affidavit comes from an informant, the magistrate is to consider the ‘informant’s veracity, *reliability* and basis of knowledge”²⁶ The defense maintains that “there is nothing in the record before the magistrate judge who granted the search warrant application that establishes the reliability of the software used,” and thus asserts “there is no basis on which the court can conclude that there was probable cause to support the issuance of the search warrant.”²⁷

The government contends that the defense’s motion fails to cite to the appropriate law in support of its suppression argument.²⁸ The government also claims that even if the defense had done so, “the argument would be meritless because the evidence would not be suppressed because the FBI relied in good faith when executing [the search warrant].”²⁹ In *United States v. Leon*, the

²⁵ Docket 317 at 12 (citing *Wong Sun v. United States*, 371 U.S. 471 (1963)).

²⁶ Docket 317 at 9 (emphasis in defense briefing) (quoting *United States v. Alvarez*, 358 F.3d 1194, 1203 (9th Cir. 2004)); see also *id.* at 10–11 (“As with a human informant or a canine alert, only software that is established before the magistrate to be reasonably reliable can support a finding of probable cause.”).

²⁷ Docket 317 at 11.

²⁸ Docket 325 at 8–11.

²⁹ Docket 325 at 11 (citing *United States v. Leon*, 468 U.S. 897 (1984)). The government also

Supreme Court held that suppression of “evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant” was not an appropriate remedy under the Fourth Amendment.³⁰ The Supreme Court explained that “[i]n the ordinary case, an officer cannot be expected to question the magistrate’s probable-cause determination or his judgment that the form of the warrant is technically correct,” and concluded that “[p]enalizing the officer for the magistrate’s error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations.”³¹

The Supreme Court carved out several exceptions to the rule announced in *Leon*. In its reply, the defense argues that two of those exceptions apply to this case.³² The first exception, which is governed by *Franks v. Delaware*,³³ applies when “the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth.”³⁴ Determinations under *Franks* are proper

maintains that “the affidavit established ample probable cause.” Docket 325 at 12 n.15.

³⁰ 468 U.S. 897, 922 (1984).

³¹ *Id.* at 921.

³² Docket 329 at 2, 4.

³³ 438 U.S. 154 (1978).

³⁴ *Leon*, 468 U.S. at 923 (citing *Franks v. Delaware*, 438 U.S. 154 (1978)).

only where the defendant “makes . . . ‘a substantial preliminary showing that the affidavit contain[ed] intentionally or recklessly false statements, and . . . [that] the affidavit purged of its falsities would not be sufficient to support a finding of probable cause.’”³⁵

The defense contends that Agent Allison misled the magistrate in this case by

fail[ing] to inform the magistrate of the name of the software used, let alone that the software was not commercially tested but a privately developed program made exclusively for law enforcement that never underwent *alpha* or *beta* testing like commercially available software, and that the software had never been independently tested by a non-interested third party to establish that the software worked as intended.³⁶

The defense further maintains that Agent Allison “had a duty to inform the magistrate of various claims that had already been made in other cases about the unreliability of the Torrential Downpour software.”³⁷ The defense cited four cases to support this assertion; in each, the district court rejected an argument almost identical to the defense’s in this case.³⁸

³⁵ *United States v. Bennett*, 219 F.3d 1117, 1124 (9th Cir. 2000) (alterations in original) (quoting *United States v. Meling*, 47 F.3d 1546, 1553 (9th Cir. 1995)).

³⁶ Docket 329 at 2. Deliberate or reckless omission can constitute false statements for the purposes of a *Franks* inquiry. See *United States v. Perkins*, 850 F.3d 1109, 1119 (9th Cir. 2017); *United States v. Hall*, 113 F.3d 157, 159 (9th Cir. 1997).

³⁷ Docket 329 at 3.

³⁸ Docket 329 at 3 n.2 (citing *United States v. Maurek*, 131 F. Supp. 3d 1258 (W.D. Okla. 2015));

For example, in *United States v. Maurek*, the district court rejected the defense’s argument that a search warrant affidavit was deficient because it omitted the fact that Torrential Downpour “is only accessible to law enforcement and [that] there was nothing that attested to the program’s technical or scientific reliability.”³⁹

The district court reasoned:

The material fact law enforcement was obligated to disclose was its use of investigative technology to track, identify, and download the files from Defendant’s computer. This fact was fully disclosed. More exacting details and disclosures simply were not required to establish probable cause.⁴⁰

The district court relied on *United States v. Chiaradio*, 684 F.3d 265 (1st Cir. 2012), where the First Circuit held that “the issuing magistrate[s] . . . sensible determination, based on a detailed affidavit [describing use of a program similar to Torrential Downpour], that a search of the defendant’s residence was likely to turn up illicit images” was “sufficient to find probable cause.”⁴¹

For similar reasons, the Court finds that the *Franks* exception does not apply in this case. Like the affiants in *Chiaradio* and *Maurek*, Agent Allison provided a

United States v. Waguespack 3:16-cr-00058-JWD-RLB (M.D. La. March 20, 2017), ECF No. 60; *United States v. Case*, No. 2:13-cr-120-LA (E.D. Wis. March 17, 2014), ECF No. 43; and *United States v. Hoeffener*, No. 4:16-cr-00374 (E.D. Mo. June 13, 2018), ECF No. 110.)

³⁹ 131 F. Supp. 3d at 1263.

⁴⁰ *Id.* at 1266 (citing *United States v. Biglow*, 562 F.3d 1272, 1280 (10th Cir. 2009)).

⁴¹ *Id.* at 1265 (citing *Chiaradio*, 684 F.3d at 279).

detailed affidavit that disclosed the use of an investigative software program to download a file containing child pornography from the defendant's computer. He was not required to disclose any as yet unsuccessful challenges to the reliability of Torrential Downpour,⁴² nor does the Court find that this omission constituted reckless disregard for the truth.⁴³ In short, the defense has not made the requisite substantial preliminary showing that Agent Allison's affidavit recklessly omitted key information that, if provided, would have prevented the magistrate judge from finding probable cause.⁴⁴

The second exception to *Leon* applies when "a warrant [is] based on an affidavit 'so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.'"⁴⁵ The defense argues that "[b]ecause the

⁴² The defense has not cited, nor has the Court identified, a case in which Torrential Downpour was found to be unreliable. *Cf. Hall*, 113 F.3d at 158–61 (suppressing evidence produced by search warrant where state trooper "withheld information bearing on [informant's] credibility" including "*conviction* for the offense of falsely reporting a crime" (emphasis added)).

⁴³ Indeed, Agent Allison states in his affidavit that he "ha[s] not included each and every fact known to me or the government" and "ha[s] only included those facts necessary to establish probable cause" to search defendant's premises. Docket 325-1 at 4, ¶ 6. *Cf. Perkins*, 850 F.3d at 1119 (concluding that affiant had "omitted facts required to prevent technically true statements in the affidavit from being misleading" (quoting *United States v. Ruiz*, 758 F.3d 1144, 1149 (9th Cir. 2014))).

⁴⁴ *See Chiaradio*, 684 F.3d 265, 279–80 (holding that omission of statements "about the reliability of EP2P [investigative software similar to Torrential Downpour], including, but not limited to, the absence of peer review . . . would not have diluted the affidavit's showing of probable cause").

⁴⁵ *United States v. Leon*, 468 U.S. 897, 923 (1984) (quoting *Brown v. Illinois*, 422 U.S. 590,

affidavit contained absolutely no information establishing the reliability of Torrential Downpour, no officer could have had an objectively reasonable belief that the warrant was based on probable cause.”⁴⁶ The defense relies on *United States v. Luong*, where the Ninth Circuit held that a sparse affidavit that “relie[d] on an unverified tip” had “no appreciable indicia of probable cause.”⁴⁷ The defense compares Torrential Downpour to an anonymous tip or a dog sniff and contends that “no officer could have an objectively reasonable belief that an affidavit lacking any . . . showing [of reliability and/or veracity] establishes probable cause.”⁴⁸

In *Luong*, the Ninth Circuit explained that for this exception to apply, the affidavit must lack even “a colorable argument for probable cause.”⁴⁹ The relevant “inquiry [is] whether the affidavit is ‘sufficient to create disagreement among thoughtful and competent judges as to the existence of probable cause.’”⁵⁰ Agent Allison’s affidavit clearly demonstrates indicia of probable cause sufficient to support the issuance of a search warrant of the defendant’s home. The Court

610–11 (1975) (Powell, J., concurring in part)).

⁴⁶ Docket 329 at 4.

⁴⁷ 470 F.3d 898, 903 (9th Cir. 2006).

⁴⁸ Docket 329.

⁴⁹ 470 F.3d at 903 (citing *Leon*, 468 U.S. at 923).

⁵⁰ *Id.* (quoting *Leon*, 468 U.S. at 926).

is not convinced that investigative software like Torrential Downpour is analogous to an unverified tip; however, even if it were, the affidavit's description of the use of the software to investigate the defendant's IP addresses does not suffer from the same deficiencies as the unverified tip in *Luong*. A "tip must include a 'range of details,' and it must predict future actions by the suspect that are subsequently corroborated by the police."⁵¹ Agent Allison's affidavit supplied a range of details produced by the Torrential Downpour investigative software. Most importantly, the affidavit included the hash values of the files the software had identified as present on the defendant's computer. And, according to the affidavit, these details were corroborated by the FBI agent's review of the files downloaded from the defendant's computer, one of which the agent determined to be child pornography. The affidavit is, at the very least, sufficient to create disagreement among reasonable jurists about the existence of probable cause. Accordingly, the second *Leon* exception raised by the defense does not apply.

The Court finds that the FBI reasonably relied upon the April 28, 2017 search warrant and that suppression would therefore be an improper remedy even if that warrant is assumed to be invalid.⁵² Accordingly, the Court does not reach the

⁵¹ *Id.* (quoting *United States v. Morales*, 252 F.3d 1070, 1075 (9th Cir. 2001)).

⁵² See *Leon*, 468 U.S. at 922 ("[S]earches pursuant to a warrant will rarely require any deep inquiry into reasonableness,' for 'a warrant issued by a magistrate normally suffices to establish'

remainder of the defense's arguments in favor of suppression.⁵³

CONCLUSION

In light of the foregoing, the defense's Motion to Suppress at Docket 317 is DENIED.

DATED this 16th day of March, 2020, at Anchorage, Alaska.

/s/ Sharon L. Gleason
UNITED STATES DISTRICT JUDGE

that a law enforcement officer has 'acted in good faith in conducting the search.'" (alteration in original) (first quoting *Illinois v. Gates*, 462 U.S. 213, 267 (1983) (White, J., concurring in judgment), then quoting *United States v. Ross*, 456 U.S. 798, 823 n.32 (1982))).

⁵³ To the extent that the defense intimates that the government is required under *Brady v. United States*, 397 U.S. 742 (1970), to produce Torrential Downpour as evidence material to the defense's Fourth Amendment claim, see Docket 317 at 8–11, that argument is moot in light of the findings set out above.

Case No. 3:17-cr-00095-SLG, *United States v. Schwier*
Order re S-1 Motion to Suppress
Page 13 of 13