IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF IOWA
WESTERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, vs. MATTHEW JOSEPH COLLINS, Defendant.	**No. 1:09-cr-00010-JEG** **O R D E R**

This matter is before the Court on a Motion to Suppress brought by Defendant Matthew Collins (Collins), which the Government resisted. A joint evidentiary hearing was held on the matter in conjunction with factually and legally similar motions to suppress in case numbers 4:09-cr-00031-JEG and 4:09-cr-00032-RP on Monday, November 16, 2009. Defendant was represented by Federal Public Defender John Burns[1]. The Government was represented by Assistant United States Attorney John Courter. The matter is fully submitted and ready for review.

I. BACKGROUND

Iowa Division of Criminal Investigation (DCI) Special Agent Robert Larsen (Special Agent Larsen) participated in Operation Wirebreaker, a coordinated law enforcement effort within the jurisdiction of the Southern District of Iowa to locate individuals downloading and making available for download visual depictions of minors engaging in sexually explicit conduct on peer-to-peer (P2P) networks. As part of his investigation, Special Agent Larsen utilized Peer Spectre, an automated software program designed for and used by law enforcement to help locate Internet Protocol (IP) addresses likely to be download candidates for these contraband files. Peer Spectre essentially automates the search process that officers could otherwise complete through a less efficient manual process. Special Agent Larsen entered search terms into the Peer Spectre program consistent with what he knew to be contraband files. In turn, Peer

[1] Mr. Burns also represented the defendant in case no. 4:09-cr-00031-JEG. Brent Rosenberg represented the defendant in case no. 4:09-cr-00032-RP.

Spectre used ultrapeers[2] to locate public advertisements from computers making child sexual abuse files available for download on a P2P network. Peer Spectre captures the date, time, file name, and Secure Hash Algorithm Version 1 (SHA-1)[3] values of files that match the requested search term. Special Agent Larsen testified that, in his experience, an ultrapeer had never sent him false information. As part of his investigation, Special Agent Larsen documented that IP address 70.187.16.156 was identified as a likely download candidate thirteen times from September 5, 2008, through September 18, 2008.

Special Agent Larsen directly connected[4] to IP address 70.187.16.156 by utilizing the P2P software and, after receiving a list of files available for download from that address, noted that the file names were consistent with the names of files likely to contain visual depictions of minors engaging in sexually explicit conduct. Because file names are not always completely accurate, Special Agent Larsen next compared the SHA-1 values of files from IP address 70.187.16.156 to the SHA-1 values of files in DCI's collection of contraband images, which had been obtained through prior investigations, in order to further verify the content of the files

---

[2] An "ultrapeer" is usually another user on a P2P network with a fast internet connection who helps users locate sought after files. Ultrapeers operate by taking requests from users and then scanning the file lists of other users on the P2P network to locate the needed files.

[3] A mathematical algorithm assigns a unique SHA-1 value to computers files, including images and video content files. Special Agent Larsen testified that a SHA-1 value is akin to a digital fingerprint and that it is more than 99.9999% reliable. As explained by the warrant application in question:

> [T]he method used by the P2P Operation described herein involves a compressed digital representation method called Secure Hash Algorithm Version 1 or SHA1. The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), for use with the Digital Signature Standard (DSS) as specified within the Secure Hash Standard (SHS). The United States of America has adopted the SHA1 hash algorithm described herein as a Federal Information Processing Standard.

Gov't Ex. 1.

[4] A direct connection allows peer A on a P2P network to link up with peer B, thereby giving peer A access to the list of files that peer B made available for distribution to all peers on the network.

available for download. Special Agent Larsen found that three of the files made available for distribution by IP address 70.187.16.156 matched files from the DCI's collection that Special Agent Larsen knew to be contraband.

On September 29, 2008, Immigration and Customs Enforcement (ICE) Special Agent Shane Nestor (Special Agent Nestor) sent a subpoena to Cox Communications (Cox), the Internet Service Provider for IP address 70.187.16.156, seeking identifying information connected to the IP address. Cox identified Defendant as the account holder and provided law enforcement with Defendant's name and address. On October 17, 2008, Special Agent Larsen completed a records check through Iowa State Patrol Communications and found that Defendant had a suspended Iowa driver's license. Special Agent Larsen conducted an additional records check and found that one vehicle had been registered to Defendant but that the registration had expired. Agent Nestor also completed a records check with the United States Postal Inspection Service, which confirmed that Defendant was receiving mail at the same residential address provided by Cox. On October 27, 2008, Special Agent Larsen conducted surveillance and took photos of Defendant's residence.

Special Agent Larsen was involved in preparing an affidavit and application for a search warrant authorizing the search of Defendant's residence. Relevant to this motion, the affidavit explained how P2P networks operate, how ultrapeers assist users in the search process, how Peer Spectre works, and why SHA-1 values are a useful and reliable means of confirming the presence of contraband content. The affidavit then specifically detailed the steps that Special Agents Larsen and Nestor took in gathering evidence in this case. The affidavit summarized the investigation by explaining how Special Agent Larsen used Peer Spectre to help identify IP address 70.187.16.156 as a download candidate; retrieved the file list associated with that IP address and noted that some of the file names were indicative of images depicting minors engaged in sexual conduct; compared and matched three images associated with IP address

70.187.16.156 to known contraband images in the DCI's own library; sent a subpoena to Cox to gain the account holder information for IP address 70.187.16.156; conducted a records check to learn who lived at the residence associated with the IP address; and conducted surveillance of the residence.

Special Agent Larsen also indicated that before signing the warrant, U.S. Magistrate Judge Ross Walters asked many questions regarding the investigation and the P2P operations in this case. He further noted that Judge Walters is always diligent in asking questions, and if there is something that is initially complex, Judge Walters ensures that law enforcement can explain the issue at hand before signing the warrant. On November 12, 2008, Judge Walters signed a warrant authorizing the search of Defendant's residence.

On February 24, 2009, following a search of Defendant's residence that uncovered contraband, the grand jury returned a four-count indictment charging Defendant with one count of distribution of visual depictions of minors engaging in sexually explicit conduct, in violation of 18 U.S.C. § 2252(a)(2) (Count One); one count of receipt of visual depictions of minors engaging in sexually explicit conduct, in violation of 18 U.S.C. § 2252(a)(2) (Count Two); one count of possession of visual depictions of minors engaging in sexually explicit conduct, in violation of 18 U.S.C. § 2252(a)(4)(B) (Count Three); and one count of forfeiture (Count Four).

On October 29, 2009, Defendant filed this Motion to Suppress, arguing that the warrant was facially deficient of probable cause. At hearing, counsel for the Defendant clarified that he was seeking a Franks[5] hearing and that all evidence against him should be suppressed because the officers preparing the warrant application failed to include necessary information. Specifically, Defendant contends (1) that the warrant affidavit lacked information regarding malicious ultrapeers in P2P networks, which Defendant asserts prevent law enforcement from gaining accurate information to support a warrant application, and (2) the warrant lacked information

[5] Franks v. Delaware, 438 U.S. 154 (1978).

confirming Peer Spectre's reliability.[6] The Government resists, arguing that Defendant failed to make the substantial preliminary showing necessary to warrant a Franks hearing. The Government also argues that the issue of ultrapeers is irrelevant with regard to the probable cause determination, that the SHA-1 values from Defendant's IP address and the DCI's collection of images matched, and that Peer Spectre was only the starting point for the investigation. Further, the Government argued that even if the information submitted to support the issuance of a search warrant did not amount to probable cause, the exception to the exclusionary rule identified in United States v. Leon, 468 U.S. 897 (1984), should apply.

II. DISCUSSION

A. Franks

"A search warrant is valid under the Fourth Amendment if it is supported by probable cause." United States v. Stevens, 530 F.3d 714, 717-18 (8th Cir. 2008). "A judge's finding of probable cause to support the issuance of a search warrant is afforded great deference on review." United States v. Montgomery, 527 F.3d 682, 686 (8th Cir. 2008). As such, this Court "will not upset a judicial finding of probable cause unless there was no substantial basis for that finding." Id.

"Under Franks, if an officer omits critical information from a search warrant application and obtains a warrant, the resultant search may be unreasonable under the Fourth Amendment." United States v. Stropes, 387 F.3d 766, 771 (8th Cir. 2004). "In order to be entitled to a hearing under Franks the defendant must make a substantial preliminary showing of a false or reckless

[6] Defendant argued in his brief that using SHA-1 values to compare files was an inaccurate method of confirming the presence of contraband content because of the theoretical possibility that two SHA-1 values could collide. In the wake of evidence that, in actual real world experience, two SHA-1 values have never collided, the Defendant withdrew this argument. In fact, Defendant's forensic computer expert agreed with Special Agent Larsen that SHA-1 values are in excess of 99.9999 percent accurate and that if a collision of values ever did occur, it would make P2P networks entirely obsolete.

statement or omission and must also show that the alleged false statement or omission was necessary to the probable cause determination." United States v. Crissler, 539 F.3d 831, 833 (8th Cir. 2008) (quoting United States v. Milton, 153 F.3d 891, 896 (8th Cir. 1998)). Defendant's burden is "not easily [met]." United States v. Engler, 521 F.3d 965, 969 (8th Cir. 2008); see also Stropes, 387 F.3d at 771 ("In other words, the defendant must show 'that the alleged omission[s] would have made it impossible to find probable cause.'" (quoting United States v. Mathison, 157 F.3d 541, 548 (8th Cir. 1998))). "[I]f, when material that is the subject of the alleged falsity or reckless disregard is set to one side, there remains sufficient content in the warrant affidavit to support a finding of probable cause, no hearing is required." Franks, 438 U.S. at 171-72. "[I]f the remaining content is insufficient, the defendant is entitled, under the Fourth and Fourteenth Amendments, to his hearing." Id. at 172.

The Defendant relied upon the testimony of Greg Chatten (Chatten),[7] whom the Defendant held out to be a computer forensics expert. Chatten testified that the search results that ultrapeers send back to users are not one-hundred percent accurate. He stated that there are "malicious" ultrapeers that purposely mislead users. As a result of these malicious ultrapeers, Chatten testified that it was possible that the internet searches conducted by law enforcement could return incorrect dates, IP addresses, file names, and SHA-1 values. However, Chatten was unable to quantify how often this might occur. Chatten opined that law enforcement should have more fully explained the possibility that a malicious ultrapeer would affect search results and that Special Agent Larsen should have kept a computer log to prove that he remained directly connected to Defendant's computer. Chatten also noted that he questioned Peer Spectre because

[7] Chatten stated that his qualifications were based upon his hands-on experience in computer programming and forensic evaluation. Chatten did not receive a college degree in computer science, information management technology, or anything similar. Further, he is not a certified forensic computer examiner. However, for purposes of the current motion, the Court finds Mr. Chatten meets minimal qualifications as an expert, by knowledge, experience, and training, to offer the opinions herein. See Fed. R. Evid. 702.

law enforcement does not release the computer software program for review by non-law enforcement personnel. On the basis of his inability to independently test and evaluate Peer Spectre, together with his experience in observing what he regarded as inconsistent information between Peer Spectre results and eventual examination of target computers, Chatten simply offers that he harbors some generalized suspicion about Peer Spectre.

The opinions offered by Chatten stand in sharp contrast to the remaining record that Peer Spectre is routinely and widely used by law enforcement officers to conduct similar investigations, with wide-ranging acceptance for reliability. The record does not contain any indication of wider acceptance of the opinions expressed by Mr. Chatten, nor any evidence that law enforcement was, or should have been, aware of such challenges to Peer Spectre reliability that should have been communicated to the Magistrate Judge.

The standard that Defendant must meet in order to warrant a Franks hearing is high because "[a]llegations of negligence or innocent mistake will not suffice to demonstrate reckless or deliberate falsehood." United States v. Snyder, 511 F.3d 813, 816 (8th Cir. 2008). This standard is illustrated in United States v. Crissler, 539 F.3d at 832, where a confidential informant provided information to law enforcement that indicated defendant Crissler was a drug dealer. Law enforcement used the confidential informant's statement, along with information already collected in the course of an investigation, to apply for a search warrant of Crissler's residence. Id. at 832-33. Following the issuance of a warrant, law enforcement conducted a search of Crissler's residence and found drugs, drug paraphernalia, and a firearm. Id. at 833. Crissler appealed the district court's denial of his request for a Franks hearing, arguing that law enforcement should have informed the issuing judge that the confidential informant had previously been deactivated from confidential informant status and that the informant was only providing information in an attempt to get relief from his own criminal charges. Id. at 834. The Eighth Circuit denied Crissler's appeal inter alia because "Crissler made no offer of proof that

the alleged omissions were intentionally or recklessly omitted." Id. The court further noted that the fact the informant was no longer an active confidential informant did not mean that he gave unreliable information and that, in fact, law enforcement *had* informed the issuing judge that the informant had been arrested the morning he provided law enforcement with information regarding Crissler. Id. The court also noted that "Crissler failed to meet his preliminary burden under Franks" because police had "adequately corroborated the information provided by [the confidential informant]." Id. at 834-35.

In this case, Defendant has not met his substantial burden under Franks. First, the Court notes that Agent Larsen testified that he thought Judge Walters had asked about the reliability of ultrapeers and the steps law enforcement takes to ensure the search process, which utilized Peer Spectre, is not unreliable. However, even if law enforcement had never discussed the reliability of ultrapeers with the issuing judge, Defendant, like Crissler, presented no evidence that law enforcement either recklessly or intentionally omitted information regarding possible malicious ultrapeers or logs detailing law enforcement's direct connection with Defendant's computer. Id. at 834; Engler, 521 F.3d at 970 (upholding denial of Franks hearing, in part, because "[the defendant] provided no evidence to establish that law enforcement officers deliberately or recklessly omitted information in an attempt to mislead the issuing judicial officer"); Snyder, 511 F.3d at 816 ("Allegations of negligence or innocent mistake will not suffice to demonstrate reckless or deliberate falsehood."); United States v. Davis, 471 F.3d 938, 946 (8th Cir. 2006) ("Neither mere negligence nor an innocent mistake will, by themselves, void a warrant."); United States v. Carpenter, 422 F.3d 738, 745 (8th Cir. 2005) (holding that a denial of a Franks hearing was appropriate because "[w]hile the agent did omit [some] information, [the defendant] has not demonstrated that this was intentional rather than negligent"). Further, as in Crissler, law enforcement verified all of the information it received following the internet search by (1) establishing a direct connection with Defendant's computer; (2) gaining a list of available files on

Defendant's computer; (3) comparing the SHA-1 values of the images on Defendant's computer to the SHA-1 values of images in DCI's library, which Special Agent Larsen knew to be visual depictions of minors engaging in sexual conduct; (4) using Defendant's IP address to locate his physical residence; (5) completing a records search to learn who lived at Defendant's address; and (6) conducting surveillance at Defendant's residence. By completing these steps, law enforcement adequately corroborated the information it originally received by utilizing Peer Spectre and ultrapeers on the P2P network. See Crissler, 539 F.3d at 834-35. Thus, Defendant has not made the substantial preliminary showing that law enforcement intentionally or recklessly omitted information from the warrant affidavit so as to entitle him to a Franks hearing.

Additionally, even if the omitted information had been included in the warrant affidavit, probable cause for the search warrant would still exist. See Stropes, 387 F.3d at 771. "Probable cause exists when a 'practical, common-sense' inquiry that considers the totality of the circumstances set forth in the information before the issuing judge yields a 'fair probability that contraband or evidence of a crime will be found in a particular place.'" Stevens, 530 F.3d at 718 (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)). Here, the affidavit submitted by law enforcement was sufficient because it provided as much, if not more, support for and verification of the information gained through Peer Spectre than a mere recitation of the omitted margin of error in the Peer Spectre or possibility of malicious ultrapeers would have provided. At best, had the omitted information been included, Judge Walters would have been aware of some small amount of unquantifiable doubt[8] as to whether the ultrapeers had correctly relayed the requested

[8] The record contains scant information regarding the level of testing, technical standards, and other bases for the opinions offered by Chatten. While the determination herein can be made accepting or rejecting the opinions, it must be observed that the completely unquantifiable concerns that the witness offered in the form of opinions lack essential foundation that "(1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case." Fed. R. Evid. 702. See Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579, 592-95 (1993).

information to law enforcement. This is not sufficient to alter the outcome under the standard that this Court is bound to apply. As the court noted in United States v. Cartier, 543 F.3d 442, 446 (8th Cir. 2008), "search warrants are issued based on the totality of the circumstances indicating that it is fairly probable, *not certain*, that the contraband will be found at the place to be searched." (emphasis added). A practical, common sense inquiry under the totality of the circumstances shows that there was a "fair probability that contraband or evidence of a crime" would be found in Defendant's residence. Gates, 462 U.S. at 238; see also United States v. Stults, 575 F.3d 834, 844 (8th Cir. 2009) (finding probable cause supported issuance of search warrant where "information contained in the affidavit show[ed] that, through the P2P file-sharing program, [law enforcement] was able to access and download files directly from [defendant's] computer that contained child pornography images"); Cartier, 543 F.3d at 446 (affirming the denial of defendant's motion to suppress inter alia because law enforcement declared in warrant affidavit that defendant downloaded images from P2P network with identical hash values to images known to law enforcement to be visual depictions of minors engaged in sexual conduct). For the reasons stated, Defendant has not made a sufficient showing to require a Franks hearing. The Court finds no improper omission by the officers seeking the search warrant, and the Court finds the inclusion of the information at issue would have left the Magistrate Judge with a sound basis upon which to conclude it was fairly probably evidence of a crime would be found at the Defendant's residence.

B. Leon

In the alternative, the Government argues if this Court finds that the search warrant was not supported by probable cause, the Leon good faith exception to the exclusionary rule should apply. Defendant provides no new arguments with regard to Leon. The good faith exception provides that "evidence seized pursuant to a search warrant issued by a magistrate that is later determined to be invalid will not be suppressed if the executing officer's reliance upon the

warrant was objectively reasonable." United States v. Ross, 487 F.3d 1120, 1122 (8th Cir. 2007) (quoting United States v. Proell, 485 F.3d 427, 430 (8th Cir. 2007)). "The rationale for such an exception is that no justification exists to exclude evidence 'when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope.'" United States v. Puckett, 466 F.3d 626, 630 (8th Cir. 2006) (quoting Leon, 468 U.S. at 920).

> The Supreme Court has identified four circumstances in which an officer's reliance on a search warrant would be objectively unreasonable: (1) when the affidavit or testimony in support of the warrant included a false statement made knowingly and intentionally or with reckless disregard for its truth, thus misleading the issuing judge; (2) when the judge "wholly abandoned his judicial role" in issuing the warrant; (3) when the affidavit in support of the warrant was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; and (4) when the warrant is "so facially deficient" that the executing officer could not reasonably presume the warrant to be valid.

United States v. Grant, 490 F.3d 627, 632-33 (8th Cir. 2007) (quoting Leon, 468 U.S. at 923).

As previously discussed, there was no evidence presented that the affidavit or the testimony in support thereof included false statements made intentionally or with reckless disregard for the truth. Nor is there evidence that the issuing judge abandoned his judicial role in determining whether probable cause supported the warrant. See United States v. Koons, 300 F.3d 985, 992 (8th Cir. 2002) (noting that a judge abandons his judicial role where "a magistrate fails to read a warrant application or affidavit, relies on an officer's oral testimony rather than the written affidavit, approves a warrant without specifics as to the objects of the search, fails to comply with legal formalities such as required signatures, or otherwise acts contrary to law"). Furthermore, there is no evidence that it was unreasonable for law enforcement to believe that the affidavit provided probable cause to issue a warrant. See Puckett, 466 F.3d at 630 (noting that it is not unreasonable for law enforcement to believe that an affidavit provided probable cause where "the issuing state-court judge, the Magistrate Judge, and the District Judge all believed that the affidavit provided probable cause for the search warrant to issue"). Finally, the

warrant was not facially deficient because it set out with particularity both the place to be searched and the items to be seized. United States v. Hessman, 369 F.3d 1016, 1023 (8th Cir. 2004) ("[T]he fourth exception [to Leon] does not apply because the warrant was not so facially deficient in failing to particularize the place to be searched or the things to be seized so that no officer could reasonably rely upon it."). The Court finds that none of the four exceptions outlined in Leon apply; and, therefore, assuming *arguendo* the Court had found the warrant lacked probable cause, the Leon exception would apply and evidence seized from Defendant's residence would be admissible against him at trial. Grant, 490 F.3d at 632 (noting that, even without probable cause to issue a warrant, disputed evidence will still be admitted so long as "it was objectively reasonable for the officer executing [the] search warrant to have relied in good faith on the judge's determination that there was probable cause to issue the warrant").

III. CONCLUSION

For the reasons stated, Defendant's Motion to Suppress (Clerk's No. 27) must be **denied.**

IT IS SO ORDERED.

Dated this 24th day of November, 2009.

JAMES E. GRITZNER, JUDGE
UNITED STATES DISTRICT COURT