UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**Case No. 4:16-CR-374 JAR/PLC**
	)	
ROLAND HOEFFENER,	)	
	)	
Defendant.	)	

Order and Report and Recommendation

This matter is before the Court[1] on Defendant's Motion to Suppress Evidence and Request for a Hearing Pursuant to Franks v. Delaware [ECF No. 29].[2] The Court held an evidentiary hearing on Defendant's Motion to Suppress and preliminarily denied the request for a Franks hearing.[3] Based upon the arguments of the parties and the evidence adduced at the hearing, the Court recommends denial of Defendant's motion and request for a Franks hearing.

Background

The Government charged Defendant with violating 18 U.S.C. § 2252A(a) by: (1) receiving over the internet videos and images of child pornography; and (2) possessing two storage devices containing images and videos of child pornography [ECF Nos. 56 and 57]. Each of the three counts includes a list identifying four visual depictions of a minor allegedly engaging

[1] This matter is before the undersigned United States Magistrate Judge pursuant to 28 U.S.C. Section 636(b).

[2] Defendant seeks leave to file a supplemental affidavit of Defendant's forensic examiner, Michele Bush, executed after she examined computers and related seized items from Defendant's home [ECF No. 66]. Because Ms. Bush's testimony at the evidentiary hearing encompassed the subject matter of the supplemental affidavit, the Court grants Defendant's request. In his post-evidentiary hearing memorandum, Defendant also requests a second reconsideration of the order denying Defendant's motion to compel. Defendant has not provided any new grounds supporting reconsideration and the Court denies this request.

[3] The Court did, however, permit Defendant to adduce evidence in support of a Franks hearing.

in sexually explicit conduct. Defendant filed a motion to suppress evidence and a request for a Franks hearing. As grounds for a Franks hearing, Defendant contends: (1) in his opening motion that the search warrant affiant's claims that the images referenced in the search warrant constitute child pornography are an overstatement and therefore misleading;[4] and (2) in his post-evidentiary hearing memorandum that the search warrant affiant intentionally withheld from the reviewing judge information that the referenced images were not "files of interest."[5]

As grounds for the motion to suppress evidence, Defendant states in his opening motion that: (1) he had a reasonable expectation of privacy in the content of his online communications through the BitTorrent peer-to-peer network; (2) the information obtained from his computer by law enforcement using Torrential Downpour was not in "plain view;" (3) use of Torrential Downpour is a violation of the Electronic Communications Privacy Act ("ECPA") 18 U.S.C. §§ 2510-2522; (4) the search warrant was not based on probable cause because it was issued as a result of "omissions pertaining to BitTorrent and the investigators (sic) use of Torrential Downpour;" and (5) the state circuit court judge who issued the search warrant ("issuing judge") lacked the technological expertise to determine probable cause and "abdicated his role as a neutral and detached magistrate." In the post-evidentiary hearing memorandum, Defendant adds a ground absent from his initial motion: the search warrant lacks probable cause because "the evidence does not conclusively support that a single source download was performed on Defendant's computer."

---

[4] In his post-evidentiary hearing memorandum, Defendant refines his argument, asserting that the search warrant affiant falsely described as child pornography the referenced search warrant images when they were actually "child erotica."

[5] According to Defendant, "files of interest" are images that have been reviewed by law enforcement at some point in the past and flagged as child pornography. Detective Baine explained "files of interest" are ascertained by law enforcement reviewing torrents or files with names considered indicative of child pornography and/or flagging ones with images the reviewer considers to be child pornography.

The Government opposes a Franks hearing on the grounds the two images contained in the search warrant affidavit meet the definition of child pornography under United States v. Dost, 636 F.Supp 828 (S.D. Cal. 1986),[6] aff'd sub nom., United States v. Wiegand, 815 F.2d 1239 (9th Cir. 1987), and the descriptions of the images do not constitute false statements. The Government also contends that Defendant has not demonstrated that the search warrant contains omissions related to BitTorrent or Torrential Downpour.

With respect to the Motion to Suppress Evidence, the Government argues that Defendant does not have a legitimate expectation of privacy "when sharing files with unknown peers" on the BitTorrent network. More specifically, the Government asserts that the law enforcement computer was an "intended recipient" of shared data, i.e. Defendant voluntarily sent information about the incriminating files to the law enforcement computer. In addition, the Government does not rely on the "plain view" exception to the warrant requirement to support its use of Torrential Downpour. With respect to ECPA, the Government contends that law enforcement did not violate ECPA "because they did not intercept any contents of Defendant's electronic communications." Furthermore, the Government rejects the assertion that the search warrant affidavit contains omissions sufficient to prevent a finding of probable cause. The Government also argues that the issuing judge was a "neutral party" and capable of determining probable

[6] In determining whether an image is "lascivious" within the meaning of the Child Protection Act of 1989, the Eighth Circuit applies the factors set forth in Dost. United States v. Lohse, 797 F.3d 515 (8th Cir.), cert. denied, 136 S.Ct 600 (2015). The Dost factors include:

> (1) whether the focal point of the image is on the minor's genital or pubic area; (2) whether the setting of the image is sexually suggestive; (3) whether the minor is depicted in unnatural poses or inappropriate attire considering the minor's age; (4) whether the minor is fully or partially clothed or is nude; (5) whether the image suggests sexual coyness or a willingness to engage in sexual activity; and (6) whether the image is intended to elicit a sexual response in the viewer.

Lohse, 797 F.3d at 930 (quoting Dost, 636 F.Supp. at 832).

cause. Finally, the Government asserts that the law enforcement computer's "log files" conclusively demonstrate a single-source download occurred during use of Torrential Downpour.

Facts

A. The Investigation

1. Detective Bobby Baine

On December 15, 2012, Detective Bobby Baine of the St. Louis Metropolitan Police Department was running a software program called Torrential Downpour on the department computer system. Torrential Downpour is a law enforcement "software program configured to search the BitTorrent network for [Internet Protocol ("IP") addresses] … offering to share or possessing files known to law enforcement that contain images/videos of child pornography."[7] Torrential Downpour connected to an IP address in the St. Louis area after discovering the IP address had videos or images of child pornography known to law enforcement. Shortly thereafter, Detective Baine checked his computer's logs to determine if any files were downloaded from the suspect IP address. Detective Baine located 196 images in one file and, following a review, identified two of the downloaded images that he believed were child pornography.

After concluding that the download contained child pornography, Detective Baine prepared a subpoena intended to determine the physical address for the suspect subscriber's IP address. To that end, the subpoena was directed to AT&T Internet Services on January 22, and the results were received on February 5, 2013.

Detective Baine testified that Torrential Downpour cannot access non-public areas of a suspect computer. Detective Baine also testified that if his computer was "blocked," he would

[7] Memorandum and Order denying Defendant's motion to compel at 2 [ECF No. 63].

not be able to connect to the suspect IP address. In addition, Detective Baine explained that in contrast to the way users normally participate in the BitTorrent network, the law enforcement software does not allow the law enforcement computer to share files from it.

2. Detective Dustin Partney/the search warrant

In 2013, Dustin Partney, a detective with the St. Louis County Police Department, worked in the Special Investigations Unit. The Special Investigations Unit primarily investigated internet crimes against children. Detective Partney was the affiant on the search warrant directed to Defendant's home address. Detective Partney received approximately a month of training prior to drafting the search warrant. Prior to the search warrant used in Defendant's case, Detective Partney had drafted one search warrant affidavit and assisted on approximately eight search warrants.

Detective Partney learned of the investigation with respect to Defendant through a contact from Sergeant Adam Kavanaugh, Detective Partney's supervisor in the Special Investigations Unit. The investigation was initiated by Detective Bobby Baine of the St. Louis Metropolitan Police Department through an undercover operation on the BitTorrent network. Detective Baine identified an IP address "that was displaying the willingness to share … and that they possessed child pornography." Detective Baine downloaded 196 image files from the IP address that was the subject of the investigation - - later identified as Defendant's IP address. Two of the images downloaded from Defendant's IP address formed the basis for the search warrant.

In the search warrant affidavit, Detective Partney describes the images as follows:

1. File name: spread.em.chan12\125943702341
   Description: An image file depicting a prepubescent female lying on her right side. The female is pulling her panties to the side, exposing the side of her vagina and anus.

2. File name: spread.em.chan12\1125946249912
Description: An image file depicting a prepubescent female lying on her back with her legs spread, exposing the pubic area and making the focal point of the image her vagina.

The issuing judge did not view the images described in the affidavit prior to issuing the warrant.[8]

Detective Partney did not include information in the description that the subjects of the images were clothed. More specifically, Detective Partney did not state in his description that each subject's "actual vagina" was covered.

3. Post-seizure forensic examinations

a. Torrential Downpour/Detective Robert Erdely [9]

Detective Robert Erdely currently works for the Indiana County, Pennsylvania District Attorney's Office as a county detective. Detective Erdely has investigated peer-to-peer file sharing since approximately 1998 when he joined the Pennsylvania State Police's Computer Crime Unit. He has been involved in developing investigative software that is "used by law enforcement across the country and around the world." Detective Erdely has testified approximately 50 times as an expert in computer forensics and on-line investigations.

Detective Erdely explained that, through use of Torrential Downpour, a law enforcement investigator is able to observe the IP address of computers seeking to obtain or share the torrent the investigator is investigating. The investigator then chooses a computer's IP address, and port for Torrential Downpour to connect to. Torrential Downpour next ascertains whether the suspect computer has the suspect torrent, and, if so, directly connects to the suspect computer. Torrential

[8] The images were identified and admitted at the evidentiary hearing held on the Motion to Suppress Evidence.

[9] The material in this section is drawn from the findings in the order denying Defendant's motion to compel [ECF No. 63]. Detective Erdely testified at the hearing on the Motion to Compel. See also Government's Ex. 2 to Govt's resp. to Def.'s mot. suppress evidence [ECF No. 38-2].

Downpour logs the date, time and infohash of the activity occurring during the investigation, the path and file name investigated, and the investigated computer's IP address, port identifier and BitTorrent software.

Detective Erdely reviewed the log for Detective Baine's December 15, 2012 investigation. The log confirmed that the investigated computer contained all pieces of the torrent investigated, "did not need anything from the investigating computer," and provided the data during one connection.

Detective Erdely testified that Torrential Downpour does not access encrypted material on a computer, but while uTorrent is "downloading to an encrypted volume" the data "is in a decrypted state" and shared. When the user "unmounts [the downloaded data] so it is no longer accessible," the sharing stops because data is now encrypted and BitTorrent software "cannot see" the encrypted data. Encrypted data "cannot be accessed unless it is decrypted and connected to [or] in a computer." Additionally, if a user accesses data through a Virtual Private Network, Torrential Downpour "still sees" the computer's IP address, but at a different location, and law enforcement is able to locate the computer after further investigation of the log information. According to Detective Erdely, Torrential Downpour cannot access unshared portions of an investigated computer or override settings on that computer.

b. Officer Steven Grimm

Steven Grimm is a Webster Groves, Missouri police officer who has been detached full-time to the Regional Computer Crimes Education and Enforcement Group ("RCCEEG") for approximately ten years. He has an undergraduate certificate in management information systems from St. Louis University as well as a bachelor's degree in English and a master's degree in organizational security administration. He also has digital forensics training through

the National Computer Forensics Institute. He has forensically examined thousands of devices in child pornography investigations.

Over the course of approximately two months, Officer Grimm examined Defendant's computers and computer devices, consisting of 48 items, including computers, external hard drives, thumb drives, CDs, DVDs, and other items. Officer Grimm determined that the uTorrent file sharing application was installed on "Item 45." Officer Grimm advised that the uTorrent application saved .torrent files to the L drive. A storage device was attached to the L drive. Officer Grimm testified that he found items of child pornography on the L drive and that files could be shared from other locations on Defendant's computer. Officer Grimm also advised that he found references to the spread.em files mapped to the Y drive, "whether or not that data was resident on Item 45 or on another device."

Officer Grimm discussed the presence of "encrypted containers" on Defendant's computer system, noting that there were multiple encrypted containers. Officer Grimm was unable to access any of Defendant's encrypted containers.

c. <u>Michele Bush</u>

Michele Bush is the daughter of Tami Loehrs, owner of Loehrs & Associates in Tuscon, Arizona, a computer forensics firm. Ms. Bush is an employee of Loehrs & Associates. Ms. Bush graduated from the University of Arizona in 2015 with a degree in psychology. She is 24 years old and stated she began testing peer-to-peer networks at fourteen years old, or, as she put it, "as a kid." She testified in one previous federal court proceeding. She has no formal training in the forensics of peer-to-peer applications but has participated in several "labs." Specifically, with respect to BitTorrent network and uTorrent software, Ms. Bush's experience consisted of "[t]esting and researching on [her] own and as well as [what she had been taught] in lectures and

labs."

Defendant retained Ms. Bush to consult "regarding the Government's forensic examination." She reviewed Detective Partney's affidavit and the police report as well as the RCCEEG forensics report, supplemental forensic reports, and a "details log" generated by the Torrential Downpour software.[10] Ms. Bush's experience with Torrential Downpour included demonstrations facilitated by Detective Erdely, observation of Detective Erdely's live testimony and Detective Erdely's affidavits.

Ms. Bush testified that she performed a forensic examination of Defendant's seized computer equipment, particularly Item 45, the computer found to have the file sharing application uTorrent. Her examination consumed approximately fifteen hours. She determined that Defendant set the uTorrent application to save downloads to a specific directory – the L directory. On cross-examination, Ms. Bush acknowledged that at the time Defendant downloaded the suspect images to the law enforcement computer running Torrential Downpour, Defendant's setting could have mapped to the Y drive. Ms. Bush also conceded that the uTorrent software running on Defendant's computer could share files from either a Y drive or an L drive "[a]s long as it's mapped and attached currently."

Ms. Bush also testified to Defendant's use of an anti-malware software program, Malwarebytes. At the time Torrential Downpour identified Defendant's IP address, Defendant was blocking numerous IP addresses through Malwarebytes. Prior to attending the evidentiary hearing, Ms. Bush did not know the IP address used by Detective Baine's computer when it connected with Defendant's computer through Torrential Downpour. Upon learning the address

[10] Ms. Bush described the details log as "automatically generated by the [Torrential Downpour] software…that includes information about the network activity, the files that were identified and other information."

at the hearing, however, Ms. Bush testified that the log of all addresses blocked by Malwarebytes did not include Detective Baine's IP address.

Ms. Bush also testified to some general features of the uTorrent software Defendant had installed on his computer. She stated that uTorrent warns the user that it is an "open publicly available file sharing network," that the user will be sharing files "with other users on the network," and that the user may "have no idea who those other users are."

Finally, with respect to hacking, Ms. Bush did not analyze Defendant's computer for evidence of hacking. In particular, when asked if she found any evidence that Torrential Downpour had hacked into non-public areas of Defendant's computer, Ms. Bush stated: "I didn't do a hacking analysis, so I can't say one way or another."

Discussion

A. Request for a Franks hearing

Defendant requested that the Court grant him a hearing pursuant to Franks v. Delaware, 438 U.S. 154 (1978) on the grounds that he made a "substantial showing that the search warrant affidavit contained statements that are either false, misleading, or show a reckless disregard for the truth; and furthermore deletion of these statements would leave the affidavit insufficient to establish probable cause." [ECF No. 86]. First, Defendant argues that the "suspect images" constituted child erotica, not child pornography, and Detective Partney therefore, exaggerated his descriptions in the search warrant affidavit. Second, Defendant asserts that Detective Partney failed to advise the issuing judge that the search warrant's referenced images were not "files of interest," i.e. files previously flagged by law enforcement as constituting child pornography.

1. Legal standard

"Where the defendant makes a substantial preliminary showing that a false statement

knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request." Franks v. Delaware, 438 U.S. 154, 155-56 (1978). The Eighth Circuit has held that: "[a] defendant may obtain a Franks hearing if (1) he makes a 'substantial preliminary showing' that the affiant intentionally or recklessly included a false statement in the warrant affidavit, and (2) the false statement was 'necessary to the finding of probable cause.'" United States v. Shockley, 816 F.3d 1058, 1061 (8th Cir. 2016) (citation omitted). The Eighth Circuit has also repeatedly recognized that "[t]he requirement of a substantial preliminary showing is not lightly met." United States v. Arnold, 725 F.3d 896, 898 (8th Cir. 2013) (quoting United States v. Mathison, 157 F.3d 541, 548 (8th Cir. 1998)). More to the point, "[a] Franks hearing must be denied unless the defendant makes a strong initial showing of deliberate falsehood or reckless disregard of the truth." United States v. Freeman, 625 F.3d 1049, 1052 (8th Cir. 2010) (internal quotation marks omitted).

To determine whether a defendant has established the requisite showing for a Franks hearing, "[a]llegations of negligence or innocent mistake will not suffice to demonstrate reckless or deliberate falsehood Franks, 438 U.S. at 171." United States v. McIntyre, 646 F.3d 1107, 1114 (8th Cir. 2011) (emphasis omitted) (internal quotation marks omitted) (quoting United States v. Mashek, 606 F.3d 922, 928 (8th Cir. 2010)). Rather, the test is "whether, after viewing all the evidence, the affiant must have entertained serious doubts as to the truth of his statements or had obvious reasons to doubt the accuracy of the information he reported." Id. (internal quotation marks omitted) (quoting United States v. Butler, 594 F.3d 955, 961 (8th Cir. 2010)).

The Eighth Circuit has extended Franks "to allow challenges to affidavits based on

deliberate or reckless omissions." United States v. Gater, 868 F.3d 657, 659 (8th Cir. 2017), cert. denied 138 S.Ct. 751 (2018) (citing United States v. Reivich, 793 F.2d 957, 960-61 (8th Cir. 1986)). In the context of a challenge to a search warrant affidavit based on an omission, a hearing is required:

> … where the defendant makes a substantial preliminary showing that: (1) the affiant omitted facts with the intent to mislead the issuing judge, or omitted the facts in reckless disregard of the fact that the omissions would mislead; and (2) the affidavit, if supplemented by the omitted information, could not support a finding of probable cause."

Id. at 659-60 (citing United States v. Conant, 799 F.3d 1195, 1200 (8th Cir. 2015)).

2. Detective Partney's affidavit did not contain overstatements and/or exaggerated descriptions of the referenced images.

Defendant contends that the following two descriptions contained in the search warrant are exaggerated when compared to the actual images:

> (1) An image file depicting a prepubescent female lying on her right side. The female is pulling her panties to the side, exposing the side of her vagina and anus.
> (2) An image file depicting a minor female lying on her back with legs spread, exposing the pubic area and making the focal point of the images her vagina.

With respect to the first image, Defendant concedes that the image is of a girl and that her "underpants" are "laying at an angle which arguably shows the edge of her vagina…." [ECF No. 86]. However, Defendant also claims that the subject's "vagina and pubic area are not exposed;" her "anus is not visible" and her "hands are not actively 'pulling' her panties in any manner." With respect to the second image, Defendant acknowledges that the image is a girl, "wearing a bra and underpants laying on her back with her legs spread." The underpants "are laying at an angle which arguably may show the edge of her labia."

In support of his argument, Defendant relies primarily on United States v. Perkins, 850 F.3d 1109, 1115-19 (9th Cir. 2017). Perkins is of little assistance here. The affiant for the

Perkins warrant omitted information that Canadian authorities dismissed child pornography charges because the images were not pornographic as well as particular descriptive language used by Canadian authorities. Id. at 1113-14. Importantly, the Ninth Circuit concluded, based on the affiant's testimony, that the omissions "reveal a clear, intentional pattern in [the affiant's] actions: he selectively included information bolstering probable cause, while omitting information that did not." Id. at 1117.

At the hearing, Detective Partney testified at length about his view that the images that form the basis of the search warrant were child pornography. More specifically, Detective Partney concluded that the referenced images constituted "lewd and lascivious display of the genitals or pubic area" and explained his reasoning. In particular, Detective Partney confirmed that the girls in both images were exposing the sides of their vaginas and anuses.

Unlike in Perkins, the record here does not support a "clear, intentional pattern" of overstatement or selective inclusion of information designed to bolster probable cause. The focal point of these posed images is clearly the pubic area and the poses are unnatural and suggestive. In both images, the child's labia and edge of the anus are unquestionably visible. The clothing is, in fact, pulled to the side at the pubic area, by the unnatural spread of the child's legs. Defendant's suggestion that a failure to more clearly state that "pulling" of the clothing was accomplished by spreading of the legs rather than by a hand somehow renders the affidavit defective is unpersuasive. Likewise, the fact that the children depicted in the images are not engaged in sex acts does not establish that the images were or were not intended to be lascivious. See United States v. Johnson, 639 F.3d 433, 440 (8th Cir. 2011) ("The fact that the young women in the videos were not acting in an obvious sexual manner, suggesting coyness or a willingness to engage in sexual activity, does not necessarily indicate that the videos themselves

were or were not intended to be lascivious.").

Defendant further argues in his post-evidentiary hearing memorandum that hundreds of cheerleading pictures fall within Detective Partney's description. [Doc. 86]. Defendant also claims that certain photographers have "made careers taking nude and sexually suggestive photos of underage girls and selling these photos as art." [Doc. 86]. In addition, Defendant declares that "[d]efense counsel, members of his firm, and Defense Expert Ms. Bush have viewed thousands of images of child pornography in hundreds of cases [and] [t]he images selected by Detective Partney as the basis of his search warrant are not representative of child pornography and are child erotica." As a district court recently held, in words equally applicable here, "[s]omething more is needed than mere disagreement with the agent's descriptions of the images or the desire for a greater context to make the substantial preliminary showing required for a Franks hearing." United States v. Pearson, No. 17-CR-72 (JNE/TNL) 2017 U.S. Dist. Lexis 202476 at 38 (D.Minn. Oct. 18, 2017).

The actual record in this case supports a determination that Detective Partney did not either improperly exaggerate or overstate the description of the images that form the basis for the search warrant. Importantly, the record is devoid of any evidence that Detective Partney intentionally or recklessly included a false statement or harbored serious doubts as to the truth of the description. "When no proof is offered that an affiant deliberately lied or recklessly disregarded the truth, a Franks hearing is not required." United States v. Mathison, 157 F.3d 541, 548 (8th Cir. 1998) (internal quotation marks omitted) (quoting United States v. Moore, 129 F.3d 989-992 (8th Cir. 1997)). Viewing the images, which were admitted at the hearing, it is clear that Detective Partney's description of the referenced images is consistent with and satisfies the Dost requirements.

3. Detective Partney did not intentionally omit information related to "files of interest."

Defendant contends that Detective Partney "recklessly withheld from the issuing judge that the images referenced in the Search Warrant Affidavit are not 'files of interest,' a fact which likely would have caused the issuing judge to find a lack of probable cause." Defendant also claims that "it is likely that Detective Erdely viewed these images and found them to be child erotica." The Government responds that Defendant improperly concludes that because the referenced images were not flagged as "files of interest," they must not be child pornography.

Detective Baine testified that he does not "pay attention to files of interest." Rather, he looks at the files himself and judges "what is child pornography and what is not." Detective Partney advised that he was aware that the referenced images had not been previously flagged as "files of interest" before he submitted the search warrant affidavit. When asked whether something that is not a "file of interest, … may not be a suspected file of child pornography," Detective Partney responded: "It is possible. That is why they are reviewed."

Moreover, to the extent that Defendant is suggesting that if the referenced images are child erotica rather than child pornography the affidavit is necessarily not sufficient to support probable cause, his argument is unavailing. The Eighth Circuit has rejected the position that possession of images constituting child erotica, which is legal, "cannot establish probable cause that the individual also possesses child pornography." United States v. Hansel, 524 F.3d 841, 846 (8th Cir. 2008). Here, as in Hansel, even if, arguendo, the referenced images are characterized as child erotica, the totality of circumstances "established a fair probability that there was child pornography on [Defendant's] computer." Id. at 847. In particular, in paragraph 4 of the search warrant affidavit, Detective Partney advised that during an undercover operation, "Detective Baine identified a computer that possessed and distributed child pornography." In

paragraph 5, Detective Partney averred that Defendant's IP address had been identified through "investigative techniques as offering to share or possessing files known to law enforcement that contain images/videos of child pornography." The search warrant affidavit also contained an extensive explanation of the methods law enforcement agencies use to locate computers "distributing in part, images and/or videos believed to be child pornography." Based on the information in the affidavit, Detective Partney established that the seized computers would contain child pornography, even if the referenced images themselves arguably could be characterized as child erotica.[11]

Finally, Defendant fails to demonstrate in what way the affidavit, if supplemented with information that the referenced images were not "files of interest," would cause an issuing judge to refuse to find probable cause. In selecting and using the referenced images, both detectives relied primarily on their own visual inspection, not a prior designation of the files. The record is completely devoid of evidence that in so doing the detectives and in particular, Detective Partney, acted with the purpose of misleading the reviewing issuing judge. To the contrary, the evidence was undisputed that both detectives involved in the investigation independently reviewed the referenced images and concluded they constituted child pornography. Accordingly, Defendant failed to make the substantial showing required by the applicable precedent to justify

---

[11] It should be noted that at least two courts have held that an affiant's actual review of the content retrieved under similar circumstances is not necessary:

> [g]iven the accuracy and reliability of SHA 1 signatures and the development of a database listing of SHA 1 signatures for files containing child pornography, a judge may find, in all likelihood, that a suspect's computer contains images of child pornography even if the affiant officer has not opened and viewed the files on (and using) the defendant's computer, and has not viewed files downloaded directly from that computer.

United States v. Oliverius, 2011 U.S. Dist. LEXIS 110783 at 10-12 (D.Neb. Aug. 5, 2011), adopted by United States v. Oliverius, 2011 U.S. Dist. LEXIS 110782 (D.Neb. Sept. 27, 2011) (citations omitted). Also see United States v. Feldman, 2014 WL 7653617 at 7-10 (E.D. Wis. July 7, 2014).

a Franks hearing.

B. The Motion to Suppress Evidence

1. Defendant did not have a legitimate expectation of privacy when file sharing on a peer-to-peer network.

Defendant argues that law enforcement violated the Fourth Amendment by unlawfully intercepting and logging the content of his electronic communications while he was using the BitTorrent network on his computer. More generally, Defendant contends that he had a reasonable expectation of privacy in the use of his computer. The Government responds that Defendant had no legitimate expectation of privacy when sharing his files on BitTorrent, a peer-to-peer file sharing network.

The Fourth Amendment protects individuals against "unreasonable searches and seizures by the government and protects privacy interests where an individual has a reasonable expectation of privacy." Smith v. Maryland, 442 U.S. 735, 743-44 (1979). As the Supreme Court stated in Katz v. United States, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." 389 U.S. 347, 351 (1967). However, "[w]hat a person seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." Id.

In Hoffa v. United States, the Supreme Court held that the Fourth Amendment does not protect an individual who unknowingly converses with a government agent, reasoning that the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom be voluntarily confides his wrongdoing will not reveal it." 385 U.S. 293, 302 (1966). In On Lee v. United States 343 U.S. 747 (1952) and Lopez v. United States, 373 U.S. 427 (1963) the Supreme Court approved the transmission and recording of conversations with government agents. More recently, the Supreme Court affirmed that Hoffa and Lopez governed the transmission and

recording of conversations with undercover government agents, stating, "[i]f the law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent, neither should it protect him when that same agent has recorded or transmitted the conversations which are later offered in evidence to prove the State's case." United States v. White, 401 U.S. 745, 752 (1971).

"When moving to suppress evidence on the basis of an alleged unreasonable search, the defendant has the burden of showing a legitimate expectation of privacy in the area searched." United States v. Stults, 575 F.3d 834, 842 (8th Cir. 2009) (internal quotation marks and citation omitted). "If there is no legitimate expectation of privacy, then there can be no Fourth Amendment violation." United States v. Bach, 310 F.3d 1063, 1066 (8th Cir. 2002). With respect to computer files obtained through use of peer-to-peer software, the Eighth Circuit has held that a defendant has no legitimate expectation of privacy in the shared files:

> We hold that Stults had no reasonable expectation of privacy in files that the FBI retrieved from his personal computer where Stults admittedly installed and used LimeWire to make his files accessible to others for file sharing. One who gives his house keys to all of his friends who request them should not be surprised should some of them open the door without knocking. As a result, "[a]lthough as a general matter an individual has an objectively reasonable expectation of privacy in his personal computer, we fail to see how this expectation can survive [Stults's] decision to install and use file sharing software, thereby opening his computer to anyone else with the same freely available program." [United States v.] Ganoe, 538 F.3d [1117,] 1127 [(9th Cir. 2008)] (internal citation omitted). Even if we assumed that Stults "did not know that others would be able to access files stored on his own computer," Stults did know that "he had file sharing software on his computer; indeed, he admitted that he used it - - he says to get music [and to download pornography]." Id. As a result, Stults "opened up his download folder to the world, including Agent [Cecchini]." Id. "Having failed to demonstrate an expectation of privacy that society is prepared to accept as reasonable, [Stults] cannot invoke the protections of the Fourth Amendment."

Stults, 575 F.3d at 843 (third through fifth alterations added).

Defendant's attempt to distinguish Stults because the peer-to-peer file sharing network in

Stults was Limewire rather than BitTorrent is unavailing. In United States v. Maurek, 131 F.Supp.3d 1258 (W.D.Okla 2015), the court considered whether a defendant using the BitTorrent network and, whose computer was investigated by Torrential Downpour, had a reasonable expectation of privacy within the meaning of the Fourth Amendment. The court held as follows:

> Defendant does not dispute that the files downloaded from his computer were found and shared over the BitTorrent P2P network. Defendant, therefore, has not established a reasonable, subjective [**10] expectation of privacy and his Motion to Suppress is overruled on this ground. Defendant's attempt to distinguish the law enforcement version of the software as somehow different, or more invasive, than standard P2P programs does not alter the fact that he allowed public access to the files on his computer which contained images of child pornography, and thus compels no different conclusion.

Id. at 1263. Similarly, in United States v. Hall, No. 2:15-CR-7-FTM – 29CM, 2015 WL 5897532, at *6 (M.D. Fla. July 10, 2015), adopted in part by United States v. Hall, No. 2:15-CR-7-FTM-29cm, 2015 WL 5897519 (M.D.Fla. Oct. 7, 2015), the court carefully analyzed a Fourth Amendment challenge very similar to Defendant's here. In particular, the defendant argued in Hall that "law enforcement's search of [defendant's] computer using the BitTorrent Roundup program … constitutes an unlawful trespass." Rejecting the defendant's position, the court held that "defendant can have no objectively reasonable expectation of privacy, even if he were to have a subjective one, in files and content that he intentionally made available for everyone using peer-to-peer networks – including law enforcement – to access and download." Id.

In support of his contention that he has a "reasonable expectation of privacy" when sharing files through peer-to-peer software, Defendant relies on Kyllo v. United States, 533 U.S. 27 (2001), United States v. Jones, 565 U.S. 400 (2012), and Carpenter v. United States, No. 16-402 (US) (pending). These cases significantly differ from this case. In Kyllo, the Supreme Court held that law enforcement's use of thermal imaging technology constituted a warrantless search, reasoning that "[w]here, as here, the Government uses a device that is not in general

public use, to explore the details of the home that would previously be unknowable without physical intrusion, the surveillance is a 'search' and is preemptively unreasonable without a warrant." 533 U.S. at 40. In Jones, the Court held that the installation and use of a GPS device on a vehicle constituted a warrantless search because law enforcement physically occupied the defendant's "effects" to obtain information. 565 U.S. at 404-06. In Carpenter, the defendant moved to suppress cell-site data on Fourth Amendment grounds that a search warrant was necessary to obtain cellphone records from the Defendant's wireless carriers. United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016), pet. for cert. granted, 137 S.Ct. 2211 (2017). The Sixth Circuit held that "the government's collection of business records containing cell-site data was not a search under the Fourth Amendment." Id. at 890. The Supreme Court granted certiorari to consider the following question: "Whether the warrantless seizure and search of historical cellphone records revealing the location and movements of a user over 127 days is permitted by the Fourth Amendment."

None of the cases Defendant relies on involve a defendant's use of file sharing software and its impact on his expectation of privacy. Moreover, in addition to the Eighth Circuit in Stults, courts around the country continue to reject the position that a defendant has an expectation of privacy when using file sharing software. See, for example U.S. v. Borowy, 595 F.3d 1045 (9th Cir. 2010) (no reasonable expectation of privacy where files publicly accessible due to installation of peer-to-peer file sharing program); Ganoe, 538 F.3d 1117 (government's use of file sharing software program to access defendant's computer did not violate defendant's Fourth Amendment rights where he had installed and used file sharing software); United States v. Abston, 401 Fed.Appx. 357, at *6 (10th Cir. 2010) (peer-to-peer file sharing); United States v. Norman, 448 Fed.Appx. 895 at *1 (11th Cir. 2011) (unpublished per curiam) (defendant's belief

that his shared files were private not reasonable where he used peer-to-peer file sharing programs); United States v. Feldman, 2014 U.S. Dist. LEXIS 181040 (E.D.Wis., July 7, 2014); adopted by United States v. Feldman, 2016 U.S. Dist. LEXIS 5782 (E.D. Wis., Jan. 19, 2015) (use of government peer-to-peer software not generally available to public does not present a constitutional problem when used to monitor a defendant's activities on a public peer-to-peer network); People v. Evensen, 2016 WL 6302102, 4 Cal.App. 5th 1020 (Cal.App. 1st Dist. 2016), petition for review denied, 2017 Cal. LEXIS 887 (Cal.S.C. Feb. 1, 2017) (law enforcement use of a program that searched peer-to-peer networks did not violate Fourth Amendment even where defendant tried to prevent others from accessing files).

Defendant also contends that because the United States Supreme Court continues to broaden Fourth Amendment protection "in the digital age," he is entitled to suppress evidence under the circumstances here. In a recent case, the Fifth Circuit considered an argument that the Supreme Court's important decision in Riley v. California, 134 S.Ct. 2473 (2014) invalidated law enforcement's use of peer-to-peer software, without a warrant, to identify a defendant's IP address and download data that a defendant shares on a peer-to-peer network. United States v. Weast, 811 F.3d 743, 747-48 (5th Cir.), cert.denied, 137 S.Ct. 126 (2016). Rejecting the notion that Riley overrules prior Fourth Amendment precedent in the context of peer-to-peer networks, the Fifth Circuit held:

> [The defendant] broadcast his IP address far and wide in the course of normal internet use, and he made the child pornography files and related data publicly available by downloading them into a shared folder accessible through a peer-to-peer network. Such behavior eliminates any reasonable expectations of privacy in the information, rendering Riley inapposite.

Id. at 747-481 (footnotes omitted). Likewise, here, as even Defendant's forensic examiner, Ms. Bush, conceded the uTorrent software Defendant installed on his computer warned the user that

his files would be shared "with other users on the network" and that a user may "have no idea who the other users are."

There is no dispute that Defendant installed a peer-to-peer file sharing program on his computer. Law enforcement's "request" to obtain the files Defendant offered to share did not violate Defendant's Fourth Amendment expectation of privacy. Although Defendant may have had a subjective expectation of privacy, in light of his installation and use of a peer-to-peer computer program, his expectation was not reasonable.[12] Accordingly, law enforcement's access to Defendant's computer through use of Torrential Downpour did not violate Defendant's Fourth Amendment rights.

2. The plain view exception is not relevant.

Defendant argues that law enforcement's use of its proprietary file sharing program, Torrential Downpour, constitutes an unlawful warrantless search and the files acquired by it are not in "plain view" and therefore were improperly seized. As an initial matter, and as more fully discussed above, the Court rejects the Defendant's assertion that law enforcement's use of Torrential Downpour to interact with Defendant's computer's peer-to-peer file sharing program (uTorrent) violates the Fourth Amendment. In addition, the Government has not raised the "plain view exception" as a basis for the acquisition of the files on Defendant's computer.

[12] Defendant's use of malware blocking software does not enhance his argument under the facts of this case. First, there is no evidence that Defendant blocked the law enforcement request for the files in question. Nor is there any record evidence that law enforcement entered non-public areas of Defendant's computer. In fact, the evidence was to the contrary. Defendant's "subjective intention not to share his files did not create an objectively reasonable expectation of privacy in the face of such widespread public access." United States v. Borowy, 595 F.3d 1045, 1048 (9th Cir. 2010) (per curiam) (Defendant using peer-to-peer file sharing program intended to render files private, but his 'technical savvy' failed him); See also Evensen, 4 Cal.App. 5th at 1027-1029 (various measures undertaken to keep files private insufficient support for reasonable expectation of privacy where a law enforcement program accessed child pornography from an accessible folder).

Finally, Defendant provided no relevant case law in support of this argument in his opening memorandum and did not further discuss it in his post-evidentiary hearing memorandum. Accordingly, the Court concludes that the plain view exception is not relevant to the issues presented in this case.

3. The Electronic Communications Privacy Act (ECPA) does not afford Defendant protection.

Defendant contends that law enforcement's use of Torrential Downpour "without prior judicial authorization" constituted an unlawful search under the Electronic Communications Privacy Act, 18 U.S.C. 2510-22, ("ECPA") in violation of "reasonable expectations of privacy under that Act."[13] In response, the Government focuses on the applicability of the ECPA, denying that law enforcement intercepted content (within the meaning of the Act) when interacting with Defendant's computer as a peer through its peer-to-peer program, Torrential Downpour.

The ECPA as amended, protects wire, oral and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically. 18 U.S.C. §§ 2510-22. The procedure for interception of communications governed by ECPA is as follows: "Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication … shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application." 18 U.S.C. § 2518. Importantly, "[t]he legislative history of ECPA suggests that Congress wanted to protect electronic communications that are configured to be private…." Konop v. Hawaiian Airlines,

[13] In his post-hearing evidentiary memorandum, Defendant articulated the issue as follows: "…Detective Baine did not have a warrant to engage in the digital surveillance of Defendant's computer and therefore, the evidence obtained, and the fruits thereof, must be suppressed."

Inc., 302 F.3d 868, 875 (9th Cir. 2002).

Defendant has provided no support for the notion that when law enforcement used Torrential Downpour to log Defendant's IP address and torrent infohash it violated ECPA. As an initial matter, it is unlikely that the type of information acquired Detective Baine's when Torrential Downpour connected to Defendant's computer would be considered "content" under the Act. "Content" under the Act is defined as including "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). Defendant has not established, or even addressed how, the data collected here concerns "substance, purport or meaning." Moreover, the developing case law in the Fourth Amendment context suggests otherwise - - consistently rejecting the notion that an IP address or similar information is protected "content." See United States v. Perrine, 518 F.3d 1196, 1204-05 (10th Cir. 2008). But even if this is deemed "content," the Eighth Circuit has strongly rejected any notion of privacy where a defendant installs file sharing software on his computer. Stults, 575 F.3d 841-43. Defendant has not articulated any rationale for the proposition that ECPA enlarges Defendant's reasonable expectation of privacy beyond that required by the Fourth Amendment.

A similar argument was recently rejected in United States v. Morel, No. 14-CR-148-JL 2017 WL 2773538 (D.N.H. June 26, 2017). In Morel, although a defendant recognized the "abundant case law holding that there is no expectation of privacy in an IP address," he nevertheless asked the court to conclude that in light of ECPA, he had a reasonable expectation of privacy in his subscriber information. Id. at *2. The court declined to broaden defendant's privacy expectations beyond that required by the Fourth Amendment, reasoning that the "statute does not compel an alternative conclusion."[14] Id. at 3. On this record, the Court similarly

[14] Having determined that there is no basis to conclude that ECPA provides Defendant with a

discerns no basis for enlarging Defendant's privacy rights by virtue of Congress' enactment of ECPA.[15]

4. The search warrant did not lack probable cause because of omissions in the affidavit regarding BitTorrent and Torrential Downpour.[16]

Defendant contends that Detective Partney's affidavit "omitted relevant discussion regarding the behavior of Torrential Downpour." Defendant claims that such omissions are "inherently misleading" and the purpose of these omissions "was to overstate and misrepresent the likelihood that Defendant's IP address had originally requested files containing child pornography." The Government rejects the assertion that the affidavit contains omissions sufficient to prevent a determination of probable cause. More specifically, the Government asserts that Defendant fails to "point to which facts were intentionally left out."

The Eighth Circuit has set forth the following guidelines "to succeed in a Franks-type challenge":

> [A] defendant must establish by a preponderance of the evidence that the affiant, either knowingly and intentionally, or with reckless disregard for the truth, included a false statement within the warrant affidavit. The same analysis applies to omissions of fact. The defendant must show that the facts were omitted with intent to make, or in reckless disregard of whether they thereby make, the affidavit misleading. The reviewing court must then determine, whether absent the false material or supplemented with the omitted material, the affidavit's

---

reasonable expectation of privacy greater than the Fourth Amendment, under the circumstances present here, the Court declines to address whether law enforcement is a "party" exempted from ECPA when engaged in peer-to-peer file sharing. Suffice it to say however, that here Defendant admittedly installed file sharing software on his computer, and as the Eighth Circuit aptly stated, "[o]ne who gives his house keys to all of his friends who request them should not be surprised should some of them open the door without knocking." Stults, 575 F.3d at 843.

[15] Even if the Court were to find a violation of ECPA, the remedy does not include suppression of evidence. By its terms, 18 U.S.C. § 2515 applies only to "wire and oral communication," not "electronic communications." See United States v. Meriwether, 917 F.2d 955, 960 (6th Cir. 1990); United States v. Reyes, 922 F.Supp. 818, 837 (S.D.N.Y. 1996).

[16] Because the basis for arguing lack of probable cause is slightly different than articulated in the request for a Franks hearing, the Court addresses Defendant's argument regarding omissions in the affidavit as it applies to the motion to suppress.

> remaining contents are sufficient to establish probable cause. If the remaining contents are insufficient to establish probable cause, the warrant must be voided and the evidence or statements gathered pursuant to it excluded. Mere negligence or innocent mistake is insufficient to void a warrant.

United States v. Clapp, 46 F.3d 795, 799 (8th Cir. 1995) (internal citations omitted) (emphasis added).

Applying these guidelines to this case, it is clear that Defendant fails to demonstrate that the search warrant lacked probable cause. As an initial matter Defendant has not identified, beyond vague generalities, the omitted information. It is undisputed that the warrant contained considerable information about Defendant's use of the BitTorrent network and his computer's interaction with the law enforcement computer. The affiant specified that Defendant's IP address offered to share files of known child pornography on the network. Exh. 1, paragraph 4, 5. The affiant further described that the BitTorrent network communicated that it had 1128 of 1128 known pieces of child pornography. The affiant also explained how law enforcement acquired the two images referenced in the affidavit. Paragraphs 11-19 of the search warrant explained in general terms the mechanics of peer-to-peer networks. Finally, in Paragraph 5, the affiant clearly stated that Detetctive Baine utilized "software configured to search the BitTorrent network for IP addresses that have been previously identified through investigative techniques as officially child pornography."

At least one court has explicitly addressed the issue Defendant raises here with respect to Torrential Downpour. In United States v. Maurek, the defendant argued that the search warrant failed to establish probable cause due to "deliberate or reckless omissions regarding the use of Torrential Downpour, namely, the fact that it is only accessible to law enforcement and there was nothing that attested to the program's technical or scientific reliability." 131 F.Supp.3d 1258, 1263 (W.D. Okla. 2015). Noting that other courts had rejected similar arguments, and in

particular relying on United States v. Chiarlio, 684 F.3d 265 (1st Cir. 2012), the Maurek court stated as follows: "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." Id. at 1266. As the Maurek court concluded, and as this Court likewise determines, "had more information about the intricacies of Torrential Downpour been included, these additional disclosures would not have affected the determination of probable cause…." Id.[17]

5. The issuing judge did not lack technical expertise or abdicate a neutral role.

Defendant contends that the issuing judge lacked "technological expertise" needed to properly review a warrant involving "BitTorrent and complex computer networking." Defendant characterizes the issuing judge as a "rubber stamp for police." In his post-hearing brief, Defendant also criticizes the issuing judge for failing to "look at the pictures and relying totally on the affiant's descriptions." The Government rejoins that the search warrant affidavit did not "necessitate a scientific background" and Defendant "has made no attempt to show that the Judge was not a neutral, unbiased party."

A valid search warrant must be based upon a finding by a neutral and detached judicial officer that there is probable cause to believe that evidence, instrumentalities, or fruits of a crime, contraband, or a person for whose arrest there is probable cause, may be found in the place to be searched. Johnson v. United States, 333 U.S. 10 (1948); Warden v. Hayden, 387 U.S. 294 (1967); Rule 41, Federal Rules of Criminal Procedure. "In dealing with probable cause … as the

[17] The Court declines to further address Defendant's failure to demonstrate, by a preponderance of the evidence, that Detective Partney intentionally omitted facts to render the affidavit misleading. The record is devoid of evidence of an intentional effort to mislead and the discussion in Section A (3) is equally applicable here.

very name implies, we deal with probabilities. These are not technical; they are factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." Brinegar v. United States, 338 U.S. 160, 175 (1949). Information contained in applications and affidavits for search warrants must be examined through review of the totality of the circumstances presented. Illinois v. Gates, 462 U.S. 213, 230 (1983). "Reasonable minds frequently may differ on the question whether a particular affidavit establishes probable cause, and we have thus concluded that the preference for warrants is most appropriately effectuated by according 'great deference' to a magistrate's determination." United States v. Leon, 468 U.S. 897, 915 (1984) (citing Spinelli v. United States, 393 U.S. 410, 419 (1969); Illinois v. Gates, 462 U.S. at 236).

The record contains no evidence that the issuing judge was incapable of understanding the technical matters in the search warrant affidavit or that he abandoned his role as a neutral, detached magistrate. Defendant must do more than make vague and conclusory allegations. United States v. Farlee, 757 F.3d 810, 819-20 (8th Cir.), cert. denied, 135 S.Ct. 504 (2014). Here the record contains no more than unsupported allegations about the issuing judge's conduct and capabilities.

In addition, Defendant's assertion that the issuing judge's failure to review the referenced images amounts to serving as a "rubber stamp" is contrary to relevant authority. See United States v. Chrobak, 289 F.3d 1043, 1045 (8th Cir. 2002) (court rejects a defendant's assertion that a magistrate judge who does not view images failed to make an independent judicial determination, holding that "[t]o make this determination, the judge must either view the images or rely on a detailed factual description of them."); United States v. Mutschelknaus, 592 F.3d 826, 828 (8th Cir. 2010) ("As a general matter, an issuing court does not need to look at the

images described in the affidavit in order to determine whether there is probable cause to believe that they constitute child pornography. A detailed verbal description is sufficient.") (citation omitted). Accordingly, Defendant fails to demonstrate a basis to suppress the evidence on this ground.

6. The search warrant did not lack probable cause based on the possibility that Torrential Downpour failed to execute a single-source download.

Defendant argues the following: "if Torrential Downpour failed to perform a single source download, then there was never probable cause to issue a search warrant." The Government responds that Defendant's argument is based on speculation.

The record supports the determination that law enforcement program performed a single-source download. Moreover, Defendant fails to explain in what respect his argument impacts a finding of probable cause and whether there is any legal support for any such proposition. "The determination of whether or not probable cause exists to issue a search warrant is to be based upon a common-sense reading of the entire affidavit." United States v. Seidel, 677 F.3d 334, 388 (8th Cir. 2012) (citation omitted). Here the affidavit presented to the circuit judge provided sufficient facts to establish a fair probability that evidence of child pornography would be found on the computer associated with Defendant's IP address.

In United States v. Blouin, 2017 U.S. Dist. LEXIS 129886 (West.Dist.Wash. August 15, 2017), a district court considered the identical argument presented here. Rejecting an attack on probable cause, the court stated as follows:

> The Court concludes as a matter of law that, if files with hash values known to be associated with child pornography are reported to be on the "shared" folder of a suspect's computer, probable cause exists for searching such suspect's computer. Because hash values are analogous to fingerprints and provide high confidence that the contents of files associated with such hash values are known, the images or videos need not themselves be downloaded from the suspect's computer in advance of the issuance or execution of a search warrant. Thus, any question

> concerning whether, in this case, RoundUp eMule actually effected a single-source download from defendant's computer does not affect the validity of the search warrant.

United States v. Blouin, No. CR16-307TSZ 2017 WL 3485736 (W.D. Wash. Aug. 15, 2017) (emphasis added); see also United States v. Martinez, No. CR-12-122-RMP, 2013 WL 12124429, at *2 (E.D. Wash. June 20, 2013). The circumstances here are even stronger than in Blouin as the only record evidence establishes a single source download. Accordingly, the Court concludes that Defendant's attack on probable cause fails.

After careful and consideration,

IT IS HEREBY ORDERED that Defendant's request to file a supplemental affidavit in support of a Franks hearing [ECF No. 66] is **GRANTED**.

IT IS FURTHER ORDERED that Defendant's request for a hearing pursuant to Franks v. Delaware [ECF No. 29] is **DENIED**.

IT IS FURTHER ORDERED that Defendant's request for a second reconsideration of the order denying his motion to compel is **DENIED**.

IT IS FINALLY RECOMMENDED that Defendant's motion to suppress evidence [ECF No. 29] be **DENIED**.

The parties are advised that they have fourteen (14) days after service of this Order and Report and Recommendation in which to file written objections to it, unless an extension of time for good cause is obtained. Failure to file timely objections may result in a waiver of the right to review. See Thompson v. Nix, 897 F.2d 356, 357 (8th Cir. 1990); 28 U.S.C. § 636(b)(1); Fed. R. Crim. P. 59.

The trial of this matter has been set for **July 2, 2018** at **9:00 a.m.** before the **Honorable John A. Ross**.

Patricia L. Cohen

PATRICIA L. COHEN
UNITED STATES MAGISTRATE JUDGE

Dated this 9th day of May, 2018