UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

UNITED STATES OF AMERICA, CRIM. NO. 14-374 (PJS/JSM)

Plaintiff,

v. REPORT AND RECOMMENDATION

LEVI WAYNE BURNS,

Defendant.

This matter is before the Court upon Defendant's Motion to Suppress Evidence Obtained as a Result of Search and Seizure [Docket No. 32].[1] Katharine T. Buzicky, Assistant United States Attorney, appeared on behalf of the Government. Robert W. Owens, Esq., appeared on behalf of defendant, who was personally present.

The matter has been referred to this Court for a Report and Recommendation pursuant to 28 U.S.C. § 636(b)(1)(B) and Local Rule 72.1(c).

I. FACTUAL BACKGROUND

Defendant Levi Wayne Burns has been charged with one count of Distribution of Child Pornography in violation of 18 U.S.C. §§ 2252(a)(2) and 2252(b)(1), and one count of Possession of Child Pornography in violation of 18 U.S.C. §§ 2252(a)(4)(B) and 2252(b)(2). Defendant has challenged the search and seizure of physical evidence obtained following the execution of search warrant signed by Sgt. Ken Hanson of the Sherburne County Sheriff's Department from the residence located at XXXX 3rd St. W, Zimmerman, Minnesota.

[1] At the hearing on February 20, 2015, defendant withdrew Defendant's Motion to Suppress Wire Interceptions, Electronic Surveillance and Wiretapping. [Docket No. 30].

At the initial hearing on the motion on February 17, 2015, the Government indicated that it originally intended to call Sgt. Ken Hanson ("Sgt. Hanson"), the affiant to the search warrant at issue. See Government's Notice of Intent to Call Witnesses at Pretrial Motions Hearing [Docket No. 35]. However, due to an unexpected emergency, Sgt. Hanson could not attend the hearing. Consequently, at the hearing, the Government stated that it would offer the search warrant application and affidavit that defendant sought to suppress for a "four corners" analysis. Defendant, on the other hand, had assumed he would be able to obtain testimony from Sgt. Hanson, and objected to proceeding forward with the motion without his testimony, and possibly the testimony of the agent who had provided information to Sgt. Hanson—Task Force Officer Dale Hanson of the Minneapolis Police Department ("Officer Hanson"). In support of his objection, defendant stated he needed the testimony, if for no other reason, than to understand the meaning of several paragraphs in Sgt. Hanson's affidavit regarding the files that were downloaded by Officer Hanson from defendant's computer. While the Court was not convinced that testimony was relevant to the determination of probable cause, the Court, in an abundance of caution, continued the hearing, directed the Government to produce Sgt. Hanson for the hearing, and informed defendant that if he wanted Officer Hanson to testify, he would have to subpoena him. The hearing was continued until February 20, 2015, at which time the Government called both Sgt. Hanson and Officer Hanson.

A. Search Warrant Application and Affidavit

On March 17, 2014, Sgt. Hanson[2] applied for a warrant to search XXXX 3rd St. W, Zimmerman, Minnesota, for evidence of child exploitation and child pornography. Gov't Ex. 1. The relevant portions of Sgt. Hanson's affidavit in support of the search warrant are as follows:

In March, 2014, Sgt. Hanson received investigation reports from Officer Hanson. Gov't Ex. 1, Bates p. 29. The reports indicated that in January, 2014, Officer Hanson had participated in an undercover investigation to search "publicly available P2P file sharing software for child pornography, videos and images that were being offered for distribution."[3] Id.

---

[2] Sgt. Hanson "is a peace officer, licensed by the State of Minnesota for approximately 23 years and employed as a permanent Investigator by the Sherburne County Sheriff's Department. [Sgt. Hanson] has been a member of the Minnesota Internet Crimes Against Children Task Force ("ICAC") since 2009. [Sgt. Hanson] has been extensively trained in the investigation of computer use in the exploitation of children." Gov't Ex. 1 (Application for Search Warrant and Supporting Affidavit), Bates p. 28.

[3] "P2P" refers to peer-to-peer file sharing. As explained in Sgt. Hanson's affidavit,

> P2P file sharing is a method of communication available to Internet users through the use of special software. The software is designed to allow users to trade digital files through a worldwide network that is formed by linking computers together. . . . There are several different software applications that can be used to access these networks but these applications operate in essentially the same manner.
>
> To access the P2P networks, a user first obtains the P2P software, which can be downloaded from the Internet, most often for free. When the P2P software is installed on a computer, the user is directed to specify a "shared" folder. All files placed in that user's "shared" folder are available to anyone on the world-wide network for download; however, a user is not required to share filed to utilize the P2P network.

When a user initially logs onto the P2P network, a list of the files that the user is sharing is transmitted to the network. The P2P software then matches files in these lists to keyword search requests from other users. A user looking to download files simply conducts a keyword search, similar to searching on Google or other internet search engines. The results of the keyword search are displayed, and the user then selects file(s) which he/she wants to download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) hosting the file. Once a file has been downloaded, it is stored in the area previously designated by the user and will remain there until moved or deleted. Most of the P2P software applications keep logs of each download event. Often times a forensic examiner, using these logs, can determine the IP address from which a particular file was obtained.

A person interested in obtaining child pornography can open the P2P application on his/her computer and conduct a keyword search for files using a term such as “preteen sex.” The keyword search would return results of files being shared on the P2P network that match the term “preteen sex.” The user can then select files from the search results and those files can be downloaded directly from the computer(s) sharing those files.

The computers that are linked together to form the P2P network are located throughout the world; therefore, the P2P network operates in interstate and foreign commerce. A person that includes child pornography files in his/her “shared” folder is hosting child pornography and therefore is promoting, presenting, and potentially distributing child pornography.

Even though the P2P network links together computers all over the world and users can download files, it is not possible for one user to send or upload a file to another user of the P2P network. The software is designed only to allow files to be downloaded that have been selected. One does not have the ability to send files from his/her computer to another user’s computer without their permission or knowledge. Therefore, it is not possible for one user to send or upload child pornography files to another user’s computer without his/her active participation.

Using a software program available only to law enforcement agents, Officer Hanson received information from a computer at IP address[4] 96.2.123.120 that one or more alleged child pornography files were available for download to Officer Hanson's computer. Id. Officer Hanson established a direct connection to IP address 96.2.123.120 and partially downloaded four files. Id. To the extent that he could do so, Officer Hanson reviewed the downloaded files and then prepared a description of the downloaded payloads. Id. According to Sgt. Hanson, the payload descriptions, marked as "complete" or "partial," are from a reference file that was completely or partially downloaded from multiple sources, and was done for the purpose of identifying the content of each payload. Id. Sgt. Hanson indicated that the host computer (i.e. defendant's computer) reported having the files described below as fully or partially downloaded. Id.

Officer Hanson copied the downloaded files to a CD and gave them to Sgt. Hanson, along with a description of the downloaded files. Id. Sgt. Hanson reviewed the downloaded files and stated that, based on his training and experience, he knows them to contain child pornography as defined in Minn. Stat. § 617.247. Id.

The affidavit provided the following information as a sample of the downloaded files:

1. **Payload Hash**: 519814bc620eb52d8babb54b7f7b086f7d5196ab
a. **Content Folder Name**: Young Russian Lesbian Arina & Nelia

---

Gov't Ex. 1, Bates p. 28.

[4] "Internet Protocol (IP) addresses are used to definitively identify a particular computer on the internet. When a computer user visits a website on the internet, their IP address is visible to that website. Law enforcement entities, in conjunction with Internet Service Providers, have the ability to identify a user's IP address to a specific household or residence." Gov't Ex. 1, Bates p. 29.

b. **Download Status**: 149 Pieces Downloaded, Host Possessed 741 of 741 Pieces
c. **Date(s) Downloaded**: 1/3/2014, 1/4/2014, and 1/17/2014
d. **Number of Files Completely Downloaded**: 0
e. **Complete Payload Description**: This payload contains a folder named, Young Russian Lesbian Arina & Nelia. Within that folder are four video files. These videos, which run between 6 minutes and 15 minutes each, show 10-14 year old nude girls in front of the camera. They perform oral sex on each other or are shown masturbating in front of the camera.

2. **Payload Hash**: 29807e0752c9ec7f9fe7027efc6b0732642ff7e0
a. **Content File Name**: arina_nelia_video_1_totona.com_.avi
b. **Download Status**: 31 Pieces Downloaded, Host Possessed 455 of 538 Pieces
c. **Date(s) Downloaded**: 1/4/2014
d. **Number of Files Completely Downloaded**: 0
e. **Payload Description**: *No Description Available*

3. **Payload Hash**: 2dcbe0bf3a4e8f3c03bd83ee52249de6027bd73d
a. **Content Folder Name**: Download
b. **Download Status**: 0 Pieces Downloaded, Host Possessed 535 of 535 Pieces
c. **Date(s) Connected**: 1/17/2014
d. **Number of Files Completely Downloaded**: 0
e. **Partial Payload Description**: This payload contains a folder named Sundolls Nelia. Within the folder is a single video file. The four minute video shows a 12-14 year old female undressing while sitting on a couch. She removes all of her clothes and poses in a number of positions in front of the camera. She spreads her legs apart while the camera focuses closer on her genitalia. Later in the video, the girl inserts an object into her vagina.

4. **Payload Hash**: 4156afd36ce5998bcfc761867d899442503891b7
a. **Content Folder Name**: Arina & Nelia
b. **Download Status**: 3 Pieces Downloaded, Host Possessed 590 of 590 Pieces
c. **Date(s) Downloaded**: 1/17/2014
d. **Number of Files Completely Downloaded**: 0
e. **Complete Payload Description**: This payload contains a folder named Arina & Nelia. The folder contains eight video files. The videos show nude 12-14 year females engaged in various sex acts such as kissing, oral sex, and masturbation.

5. **Payload Hash**: 4c2ef2205056634046d58d1df111462e0ae76df0
a. **Content Folder Name**: Nelia (11Yo) & Arina (12Yo)
b. **Download Status**: 2 Pieces Downloaded, Host Possessed 1,642 of 1,642 Pieces

> c. **Date(s) Downloaded**: 1/17/2014
> d. **Number of Files Completely Downloaded**: 0
> e. **Partial Payload Description**: This payload contains a folder named Nelia (11Yo) & Arina (12Yo.) Within that folder are several video files. These videos show nude 12-14 females posing in front of the camera. The girls spread their legs open for the camera, while the camera focuses on their genitalia.

Id., Bates pp. 29-30.

Sgt. Hanson explained in his affidavit that "computer software has different methods to insure that two files are exactly the same;" the Gnutella network[5] uses a file encryption method known as Secure Hash Algorithm Version 1 ("SHA1"); and "SHA1 is the fingerprint, or DNA, for a digital file. SHA1 is much more accurate than DNA. This allows an investigator to see files being traded on a P2P system, that are previously known to be child pornography, and know they are the same just by looking at the digital signature, or SHA1 value." Id., Bates p. 30.

Sgt. Hanson stated that an administrative subpoena was sent to Midcontinent Communications for IP address 96.2.123.120. Id. Midcontinent reported that the IP address was registered to a Wayne Burns at XXXX 3rd St W, Zimmerman, Minnesota, 55398-9597. Id. According to Midcontinent, the registrant had been assigned IP address 96.2.123.120 from October 4, 2013, to January 27, 2014. Sgt. Hanson searched Sherburne County records and located a Wayne Bruce Burns at XXXX 3rd St W, Zimmerman, Minnesota. Id. Sgt. Hanson then searched the Minnesota Predatory Offender Registration and found a Levi Wayne Burns listed to the same address. Id.

On March 13, 2014, Sgt. Hanson traveled to XXXX 3rd St W, Zimmerman, Minnesota, to determine whether a wireless signal was available around the residence

[5] "While there are several P2P networks currently operating, the most predominant is the Gnutella 1 network." Id., p. 3.

and whether that signal was password protected. Id. "From the street adjacent to the front of the residence [Sgt. Hanson] was able to detect only wireless signals that were password protected." Id.

On March 17, 2014, the Sherburne County District Court, Judge Thomas D. Hayes, issued a warrant to search the residence at XXXX 3rd St W, Zimmerman, Minnesota. Sgt. Hanson executed the search warrant on March 20, 2014, and seized evidence from the premises.

B. Hearing Testimony

On February 20, 2015, the Court conducted a hearing and took testimony from Sgt. Hanson and Officer Hanson. Sgt. Hanson confirmed that the descriptions of the sample of files downloaded came from the report prepared by Officer Hanson that was delivered to Sgt. Hanson with the CD.

Officer Hanson testified that he was able to partially download files from defendant's computer. One of the partial downloads contained a video file, of which approximately 3 to 3 1/2 minutes were viewable. Officer Hanson played the file and concluded that it showed children engaging in sexual acts. Officer Hanson testified that the remainder of the files downloaded from defendant's computer were not viewable, and, therefore, he had no personal knowledge that the files he downloaded contained child pornography. Instead, the descriptions of the files in the affidavit were taken from previous investigations conducted by Officer Hanson, and were descriptions of files with the same payload hash values as those samples identified in Sgt. Hanson's affidavit. Officer Hanson also explained that he estimated the ages of the females in the videos based on his experience and training.

In response to questioning by the Court, Officer Hanson explained the following as to each of the five paragraphs in Sgt. Hanson's Affidavit (Gov't Ex. 1, Bates pp. 29-30), describing the samples of files downloaded from defendant's computer:

- The phrase "Payload Hash" refers to a numerical value assigned by the P2P network to identify a particular file or folder downloaded from the host (i.e. defendant's) computer. The hash value corresponds with a file or folder previously known to contain child pornography.

- The "Content Folder Name" or "Content File Name" is the name automatically given to files downloaded from the host computer, based on instructions from the host computer.

- The paragraph "Download Status" indicates how many pieces defendant's computer (i.e. "Host") possessed of the file referenced by the Payload Hash number and how many pieces of that file Officer Hanson was able to download.

- The reference to "Date(s) Downloaded" sets forth each date Officer Hanson downloaded from defendant's computer any portion of the file referenced by the Payload Hash number.

- The phrase "Complete Payload Description" refers to Officer Hanson's own description of the content of the complete files, which he compiled from other investigations.

Thus, the sample described in Sgt. Hanson's affidavit by Payload Hash number 519814bc620eb52d8babb54b7f7b086f7d5196ab, (Gov't Ex. 1, Bates p. 29), uniquely described a download containing a folder called "Young Russian Lesbian Arina & Nelia" that included four video files running between 6 to 15 minutes each of 10-14 year old nude females in front of the camera that are performing oral sex on each other or are shown masturbating in front of the camera. Defendant's computer possessed all 741 pieces of this file and Officer Hanson downloaded 149 of the 741 pieces, which he viewed and concluded showed child pornography.

Sgt. Hanson testified that he had received a CD from Officer Hanson, which contained video files. Sgt. Hanson personally viewed the files, including the reference files and the 3 1/2 minute video viewed by Officer Hanson, and personally believed that the files contained child pornography as defined in Minn. Stat. § 617.247. Sgt. Hanson explained that the video descriptions in the affidavit were not prepared by him, but were set out in the report by Officer Hanson. Sgt. Hanson did, however, view the videos referenced by each of the Payload Hash numbers set forth in paragraphs 1-5 of his affidavit, (Gov't Ex. 1, Bates pp. 29-30), and verified that the descriptions set forth in the "Complete Payload Description" were accurate. Sgt. Hanson testified that he did not know, with 100% accuracy, the ages of the females in the videos, but he agreed with the estimates provided by Officer Hanson.

C. Defendant's Motion to Suppress Evidence

In support of his motion to suppress evidence found during the search of his residence located at XXXX 3rd St. W, Zimmerman, Minnesota, defendant argued that Sgt. Hanson's affidavit in support of the search warrant was misleading. Memorandum in Support of Motion to Suppress Evidence Obtained as a Result of Search and Seizure ("Def.'s Mem."), p. 3 [Docket No. 42]. Specifically, defendant contended that,

> reading the affidavit as a whole, and without the specialized training these officers possess, one is lead [sic] to believe that the sexual activity described in the five files was, in fact, downloaded from the defendant's "host" computer and that download was viewed by Sgt. Hanson. That is not true. It is at the end of the day misleading. The affidavit does not tell the Judge that the officers couldn't get any distributed viewable video images from the defendant's computer except for a sketchy three minutes of one video.

Id., pp. 3-4.

Defendant also contended that Sgt. Hanson's affidavit was misleading because "the allegations that the females are underage and the videos have been judicially determined to be child pornography are unsupported, unverified conclusory opinions of either Sgt. Hanson or some unknown, unidentified third person." Id., p. 4. Defendant asserted that the affidavit contained "boilerplate" descriptions of typical computer investigations into child pornography, which constituted "bare conclusions" and were not sufficiently particularized to defendant. Id., pp. 4-5. Defendant also maintained that the affidavit provided no information as to how the ICAC compiled its list of child pornography files or how the ICAC determined that the files contained child pornography. Id., p. 5. Therefore, the issuing judge had no independent basis to evaluate whether the reference files met the legal definition of child pornography. Id., pp. 5-6.

Further, defendant argued that even as to the one video file found on defendant's computer, which depicted females engaged in sexual activities, the affidavit did not indicate how Sgt. Hanson determined that they were between the ages of 10 and 14. Id., p. 6. For example, no evidence of an examination by a pediatrician or other qualified expert was provided. Id. Instead, the affidavit contained only the bare statement by Sgt. Hanson, based on his general training and experience, that the females shown in the video were underage, which was facially insufficient. Id.

Finally, defendant took exception to the affidavit's conclusion that the file contained child pornography, as defined by Minn. Stat. § 617.247, maintaining there was no probable cause stated in the affidavit to meet the elements of the statute. Id.

In response, the Government maintained that the "four corners" of the affidavit established sufficient probable cause to believe that defendant possessed and distributed child pornography. Government's Post-Hearing Response to Defendant's Motion to Suppress ("Gov't Mem."), p. 5 [Docket No. 44]. According to the Government, probable cause may exist even if no law enforcement officer ever viewed the files allegedly containing child pornography. Id., pp. 6-7 (discussing United States v. Cartier, 543 F.3d 442 (8th Cir. 2008); United States v. Harner, Crim. No. 09-0155 (PJS/FLN), 2009 WL 2849139 (D. Minn. Sept. 1, 2009), aff'd, 628 F.3d 999 (8th Cir. 2011)). The Government also noted that "[f]ile names are often indicative of their content and informative to the person who maintains or possessed them." Id., p. 7. Further, the Government contended that Sgt. Hanson's personal opinion that the females depicted in the files were minors was sufficient to support a finding of probable cause. Id., pp. 7-8.

As to defendant's assertion that Sgt. Hanson misrepresented facts in the affidavit, the Government argued that the Court is precluded from invalidating the warrant on that ground because defendant has not brought a motion under Franks v. Delaware, 438 U.S. 154 (1978). Id., pp. 9-10. Lastly, the Government maintained that even if the search warrant was not supported by probable cause, the Court should nonetheless uphold it under the good-faith exception set forth in United States v. Leon, 486 U.S. 897 (1984). Id., pp. 10-11.

II. DISCUSSION

A. Probable Cause

When a search is executed pursuant to a warrant, a court must determine whether the warrant was supported by probable cause. United States v. Proell, 485 F.3d 427, 430 (8th Cir. 2007) (citing Walden v. Carmack, 156 F.3d 861, 870 (8th Cir. 1998)). "Probable cause exists when, given the totality of the circumstances, a reasonable person could believe there is a fair probability that contraband or evidence of a crime would be found in a particular place." United States v. Fladten, 230 F.3d 1083, 1085 (8th Cir. 2000) (citing Illinois v. Gates, 462 U.S. 213, 238 (1983)).

The task of a court issuing a search warrant is to "'simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place.'" United States v. Williams, 477 F.3d 554, 557 (8th Cir. 2007) (quoting Gates, 462 U.S. at 238); see also United States v. Hyer, 498 F. App'x 658, 660 (8th Cir. 2013) ("[P]robable cause is a practical, factual, and nontechnical concept, dealing with probabilities. 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.") (internal quotation marks and citations omitted); United States v. Howe, 591 F.2d 454, 457 (8th Cir. 1979) ("For federal agents to establish probable cause to search it is necessary only to demonstrate with some degree of reasonableness that federal criminal activity is 'probable,' not that it exists beyond a reasonable doubt.") (citations omitted).

When reviewing the decision of the issuing judge, a district court must ensure that the magistrate had a substantial basis for concluding that probable cause existed. Gates, 462 U.S. at 238-39 (citation omitted); see also United States v. LaMorie, 100 F.3d 547, 552 (8th Cir. 1996) ("Our duty as the reviewing court is to ensure that the issuing judge had a 'substantial basis' for concluding that probable cause existed . . . .") (citation omitted). In doing so, a reviewing court must give "great deference to the magistrate's probable cause determination." United States v. Caswell, 436 F.3d 894, 897 (8th Cir. 2006); LaMorie, 100 F.3d at 552 ("[W]e owe substantial deference to the determination of probable cause by the issuing judge."). Accordingly, "[i]n doubtful or marginal cases, the resolution of the Fourth Amendment question should be determined to a large extent by the preference accorded to searches based upon warrants." United States v. Leichtling, 684 F.2d 553, 555 (8th Cir. 1982) (quoting United States v. Christenson, 549 F.2d 53 (8th Cir. 1977)).

At the same time, the Eighth Circuit has warned that "[c]onclusory statements made by affiants fail to give the issuing magistrate a substantial basis for determining that probable cause exists." United States v. Summage, 481 F.3d 1075, 1077-78 (8th Cir. 2007) (quoting Caswell, 436 F.3d at 897-98). "Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others." Id. (quoting Gates, 462 U.S. at 239).

"When the [issuing judge] relied solely upon the supporting affidavit to issue the search warrant, only that information which is found within the four corners of the affidavit may be considered in determining the existence of probable cause."

United States v. O'Dell, 766 F.3d 870, 874 (8th Cir. 2014) (alteration in original) (quoting United States v. Soloman, 432 F.3d 824, 827 (8th Cir. 2005)).

Based on these principles, the Court concludes that Sgt. Hanson's supporting affidavit provided probable cause to search XXXX 3rd St W, Zimmerman, Minnesota.

First, the affidavit establishes a substantial basis for determining that defendant was engaged in the possession or distribution of child pornography. In particular, the affidavit provided:

- "While there are several P2P networks currently operating, the most predominant is the Gnutella 1 network."
- The Gnutella network uses the SHA1 method to encrypt its files, which "allows an investigator to see files being traded on a P2P system, that are previously known to be child pornography, and know they are the same just by looking at the digital signature, or SHA1 value."
- "Officer Hanson was able to make a direct connection to the IP address of 96.2.123.120 and partially download the content of four files."
- "Officer Hanson reviewed the downloaded files and prepared a description of the downloaded payloads. The payload descriptions marked, complete or partial are from a reference file that was completely or partially downloaded from multiple sources."
- The host computer in this case reported having the . . . files [allegedly containing child pornography] fully or partially downloaded."

Gov't Ex. 1, Bates pp. 28-30.

The affidavit also provided descriptions of the complete reference files, which made it abundantly clear to the reviewing judge that the payloads found on defendant's computer depicted videos of underage females engaged in a variety of sexual acts. Id., Bates pp. 29-30. Furthermore, the affidavit indicated that Sgt. Hanson viewed the

downloaded files and knew them to be child pornography, as defined in Minn. Stat. § 617.247. Id., Bates p. 30.

All of this information provided a substantial factual basis for the issuing judge to conclude that defendant possessed files containing child pornography on his computer and allowed those files to be downloaded to other computers connected to the P2P network.

Second, the affidavit is not conclusory. To the contrary, Sgt. Hanson factually described the steps law enforcement officers took in investigating defendant. According to the affidavit, Officer Hanson established a direct connection to defendant's computer and partially downloaded the contents of four of five files. Officer Hanson found that the SHA1 values of the partially downloaded files matched those of known child pornography files. Although Officer Hanson was able to download only a portion of the files, defendant's computer reported that it possessed the complete files on these four files. Officer Hanson recorded the fully downloaded reference files onto a CD and gave them to Sgt. Hanson, who personally viewed the files and concluded that they contained child pornography.

Defendant's suggestion that "the allegations that the females [depicted in the videos] are underage . . . are unsupported, unverified conclusory opinions of either Sgt. Hanson or some unknown, unidentified third person," (Def.'s Mem., p. 4), is meritless. While it is true that Sgt. Hanson did not know with absolute certainty the ages of the females appearing in the videos, he swore under oath that, based on his experience and training, he knew that they contained child pornography. Gov't Ex. 1, Bates p. 29. "[E]xperience-based factual conclusions are a normal, necessary, and perfectly

acceptable part of an affidavit . . . ." United States v. Smith, 795 F.2d 841, 848 n. 7 (9th Cir. 1986). Further, expert opinion by a pediatrician or other qualified expert is not required to establish probable cause to support the issuance of a search warrant.

> If ordinary citizens serving on a jury can find, based on nothing more than looking at an image, that the image depicts child pornography—and can do so beyond a reasonable doubt—then surely an experienced investigator can provide probable cause for a search warrant based on nothing more than looking at an image. Put differently, if the testimony of a pediatrician or other qualified expert is not necessary to convict, it is surely not necessary to establish probable cause. *Cf. United States v. Koelling,* 992 F.2d 817, 822 (8th Cir.1993) ("Most minors look like minors and most adults look like adults, and most of the time most law enforcement officers can tell the difference. The Constitution requires no greater precision.").

Harner, 2009 WL 2849139, at *2; see also United States v. Grant, 490 F.3d 627, 632 (8th Cir. 2007) ("We agree with the District Court that Lewis, by virtue of his experience as a computer repairman, was 'uniquely able, and properly motivated, to distinguish between child pornography and lawful images.'") (citation omitted). In short, Sgt. Hanson's estimate of the females' ages, based on his training and experience as an investigator with the ICAC, was sufficient to establish probable cause that the files stored on defendant's computer depicted minors.[6]

Similarly, defendant's contention that Sgt. Hanson's conclusory statement that the downloaded files met the statutory definition of child pornography could not be upheld without providing information to the issuing judge "as to how the ICAC compiled

[6] Although the females depicted in the reference files conceivably "'could have been virtual children or adults depicted as children,' . . . merely identifying an alternative, non-criminal explanation for the information in a warrant is not sufficient to render it defective, unless that explanation eliminates the fair probability that evidence of criminal activity will be found at the described location." United States v. Mutschelknaus, 592 F.3d 826, 829 (8th Cir. 2010) (internal citation omitted).

its list of child pornography files or how the ICAC determined that the files on its list meet the legal definition of child pornography under Minnesota or Federal law," (Def.'s Mem., p. 5), has no merit. Such information is not required to determine whether the affidavit provided sufficient information to establish probable cause that the videos on defendant's computer contained child pornography.

"As a general matter, an issuing court does not need to look at the images described in an affidavit in order to determine whether there is probable cause to believe that they constitute child pornography. A detailed verbal description is sufficient." Mutschelknaus, 592 F.3d at 828-29 (quoting United States v. Lowe, 516 F.3d 580, 586 (7th Cir. 2008)); see also Cartier, 543 F.3d at 446 ("Although Cartier correctly asserts that no one reported seeing images of child pornography on his computer prior to the execution of the search warrant, the lack of such evidence does not necessitate a finding that probable cause was lacking.").

In addition, "[a] file's name may certainly be explicit and detailed enough so as to permit a reasonable inference of what the file is likely to depict." United States v. Miknevich, 638 F.3d 178, 185 (3d Cir. 2011).

> As a matter of common sense, the very fact that individuals utilize search terms with P2P software to produce results (i.e., ***file names***) consistent with their chosen search terms suggests a substantial degree of correlation between file names and file content; if file names were, as a general rule, completely random and bearing no relation whatsoever to their content, then there would be no point in conducting a search in the first place and the whole purpose of peer-to-peer file sharing would be frustrated because there would be no meaningful method for locating the sought-after file content.

United States v. Beatty, 2009 WL 5220643, at *7 (W.D. Pa. Dec. 31, 2009), aff'd, 437 F. App'x 185 (3d Cir. 2011) (emphasis in original). Here, the names of the partially

downloaded files, such as "Young Russian Lesbian Arina & Nelia," and "Nelia (11Yo) & Arina (12Yo)," strongly suggest that the files contained child pornography.[7]

In this case, the supporting affidavit provides the names of the reference files, as well as detailed descriptions of their contents. These descriptions do not merely declare that the files contain child pornography. Rather, they provide the length of each video, the age of the females depicted (as estimated by a person with training and experience in child pornography investigation), the physical actions of the females, and the focus point of the cameras. Because the files were described with particularity, the issuing judge had sufficient factual grounds to find probable cause, even without knowing how the ICAC compiled its list of child pornography files or determined that the files met the statutory definition of child pornography.

Finally, the Court rejects defendant's argument that the supporting affidavit misled the issuing judge "to believe that the sexual activity described in the five files was, in fact, downloaded from the defendant's 'host' computer and that [the] download was viewed by Sgt. Hanson." Def.'s Mem., p. 3.

> Where an issuing judge's probable cause determination was premised on an affidavit containing false or omitted statements, the resulting search warrant may be invalid if the defendant can prove by a preponderance of evidence "(1) that the police omitted facts with the intent to make, or in reckless disregard of whether they thereby made, the

[7] Of course, "file names are not always a definitive indication of actual file content and, therefore, only after downloading and viewing a particular file can one know with certainty whether the content of the file is consistent with its designated name. However, [c]ertainty has no part in a probable cause analysis. On the contrary, probable cause requires only a probability or substantial chance of criminal activity, not an actual showing of such activity." Miknevich, 638 F.3d at 184-85 (alteration in original) (internal citations and quotation marks omitted). Here, the affidavit set forth a substantial probability that defendant was engaging in the possession or distribution of child pornography. No greater showing is required under the Fourth Amendment.

> affidavit misleading ... and (2) that the affidavit, if supplemented by the omitted information would not have been sufficient to support a finding of probable cause."

Williams, 477 F.3d at 557 (citations omitted). However, "[a] separate hearing is required to invalidate a warrant on this basis." United States v. Andolini, Crim. No. 11-196 (JRT/JSM), 2011 WL 4842545, at *4 (D. Minn. Oct. 12, 2011). To receive a hearing on this issue (known as a Franks hearing), a defendant must make a "'substantial preliminary showing' of deliberate falsehood or reckless disregard for the truth." United States v. Carnahan, 684 F.3d 732, 735 (8th Cir. 2012) (quoting Williams, 477 F.3d at 557-58). "Because '[t]here is ... a presumption of validity with respect to the affidavit supporting the search warrant[, t]o mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine.' The substantiality requirement is not lightly met." Williams, 477 F.3d at 558 (alterations in original) (internal citation omitted) (citing United States v. Wajda, 810 F.2d 754, 759 (8th Cir. 1987).

Here, defendant did not request a Franks hearing, nor did he make an initial (or any) showing of deliberate or reckless falsehood by Sgt. Hanson or other law enforcement officers. Therefore, defendant's contention that Sgt. Hanson's affidavit was misleading is rejected. In any event, the Court finds that the affidavit was not misleading. Nowhere does the affidavit suggest that the complete reference files were acquired from defendant's computer and independently viewed by Sgt. Hanson. To the contrary, the affidavit apprised the Court that "[t]he payload descriptions marked, complete or partial are from a reference file that was completely or partially downloaded from multiple sources. This was done to identify the content of each payload." Gov't Ex. 1, Bates p. 29. The affidavit also indicated that Officer Hanson was only able to

"partially download the content of four files" from defendant's computer. Id. (emphasis added). Given this explanation by Sgt. Hanson, the Court finds no grounds to suggest that the affidavit was misleading.

For all of these reasons, the Court concludes that the issuing judge had a substantial basis for concluding that probable cause existed to issue the search warrant.

C. The Leon Exception

Because the search warrant was supported by probable cause, the Court need not determine whether the Leon good-faith exception should apply. However, even if the warrant lacked probable cause, the Court notes that officers' reliance on the warrant would have been reasonable under Leon.

> Under the [Leon] good-faith exception, evidence seized pursuant to a search warrant that lacked probable cause is admissible if the executing officer's good-faith reliance on the warrant is objectively reasonable. The good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal despite the [issuing judge's] authorization.

United States v. Perry, 531 F.3d 662, 665 (8th Cir. 2008) (citing Proell, 485 F.3d at 430-31 (alterations in original) (internal quotations omitted).

In Leon, the Supreme Court explained that "'searches pursuant to a warrant will rarely require any deep inquiry into reasonableness,' for 'a warrant issued by a magistrate normally suffices to establish' that a law enforcement officer has 'acted in good faith in conducting the search.'" 468 U.S. at 922 (citations omitted). Nevertheless, "in some circumstances the officer will have no reasonable grounds for believing that the warrant was properly issued." Id. at 922-23 (footnote omitted).

> Leon identified four situations in which an officer's reliance on a warrant would be unreasonable: (1) when the affidavit

> or testimony supporting the warrant contained a false statement made knowingly and intentionally or with reckless disregard for its truth, thus misleading the issuing judge; (2) when the issuing judge wholly abandoned his judicial role in issuing the warrant; (3) when the affidavit in support of the warrant is 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 no police officer could reasonably presume the warrant to be valid.

Perry, 531 F.3d at 665 (quoting Proell, 485 F.3d at 431). With respect to the third exception, the Eighth Circuit explained: "'Entirely unreasonable' is not a phrase often used by the Supreme Court, and we find nothing in Leon or in the Court's subsequent opinions that would justify our dilution of the Court's particularly strong choice of words." Proell, 485 F.3d at 432 (quoting United States v. Carpenter, 341 F.3d 666, 670 (8th Cir. 2003)).

In this case, the Court does not find that the affidavit was intentionally or recklessly misleading, or that the issuing magistrate judge wholly abandoned his judicial role in issuing the search warrant. As to the remaining exceptions, the Court has already concluded that the affidavit provided an adequate factual basis for the issuing judge to have found probable cause. Therefore, based on all the facts and circumstances of this case, it was not "entirely unreasonable" for Sgt. Hanson and other law enforcement officers to rely on Judge Hayes' issuance of the search warrant.

III. RECOMMENDATION

For the reasons set forth above, IT IS HEREBY RECOMMENDED that:

Defendant's Motion to Suppress Evidence Obtained as a Result of Search and Seizure [Docket No. 32] be **DENIED**.

Dated: March 10, 2015

s/ Janie S. Mayeron
JANIE S. MAYERON
United States Magistrate Judge

NOTICE

Under D. Minn. LR 72.2(b) any party may object to this Report and Recommendation by filing with the Clerk of Court, and serving all parties by **March 24, 2015**, a writing which specifically identifies those portions of this Report to which objections are made and the basis of those objections. A party may respond to the objecting party's brief within ten days after service thereof. All briefs filed under this Rules shall be limited to 3500 words. A judge shall make a de novo determination of those portions to which objection is made. This Report and Recommendation does not constitute an order or judgment of the District Court, and it is therefore not appealable directly to the Circuit Court of Appeals.