

and computer media in violation of Title 18 U.S.C. § 2252(a)(4)(B) and (b)(2) (Count 2).¹ Moreover, a forfeiture allegation was made in the Indictment regarding any matter and material that Defendant may have an interest in that was or could have been used to commit and promote the commission of Counts 1 and 2.

II. GROUNDS FOR PROBABLE CAUSE ALLEGED BY SEARCH WARRANT AFFIANT IN SUPPORT OF SEARCH WARRANT ISSUED ON OCTOBER 6, 2004

On August 4, 2004, Special Agent (hereinafter SA) Robin Andrews, an FBI member of the Innocent Images Task Force–Sexual Assault Felony Enforcement (SAFE) Team in Tucson, Arizona, in an undercover capacity used an internet-connected computer to launch a peer-to-peer (hereinafter "P2P") file sharing program called LimeWire. (Affidavit for Search Warrant (hereinafter "Affidavit"), ¶31) This software program enables internet users utilizing it to link together to share and download digital files among themselves. The user of P2P software opens it on his or her computer and conducts a search by keyword of files being shared on the network. The result of the keyword search is displayed on the user's computer allowing the user to select a download file directly from the computer containing such file. (Affidavit, ¶¶9, 10) A P2P transfer is assisted by reference to an Internet Protocol Address (hereinafter "IPA") particular to a specific computer which provides a unique location for the transfer of data between the respective computers. (Affidavit, ¶12)

On August 4, 2004, from 11:35 a.m. to 5:30 p.m., SA Andrews conducted a keyword search using the term "zadoom" which in her experience is associated with child pornography. SA Andrews observed multiple files available for viewing and downloading from IPA 68.225.148.246 (hereinafter "IPA-.246"). She downloaded two files, one titled "PTHC Ultra Hard Pedo Child Porn Pedofilia (New) 057(2).jpg" (hereinafter File 1) depicting a prepubescent female being kissed on the lips by an adult male; and the other titled

¹Title 18 U.S.C. §2252, *et seq.* "criminalize[s] the possession, receipt and transmission of child pornography." *United States v. Gourde*, 440 F.3d 1065, 1067 (9th Cir. 2006) (en banc), *petition for cert. filed July 7, 2006.*

"PTHC Ultra Hard Pedo Child Porn Pedofilia (New) 058(1).jpg" (hereinafter File 2) depicting a nude prepubescent female's vaginal area in contact with an adult's erect penis. (Affidavit, ¶31)²

A sampling of other files available for downloading from IPA-.246 listed by SA Andrews in the search warrant affidavit were:

BB-gay preteen 2 boys 8yo&9yo vintage porn
Zadom pedo man fuck boy 8yo
Zadom Pedo Julia 7yo Hot Lick
7yo suck lolita underage illegal kiddy incest Vicky mclt preteen
PTHC-babyJ-babycum
TMPR@ygold-babyJ-5yo loving the dick, child porn sex

(Affidavit, ¶32)

On August 6, 2004 from 2:50 p.m. to 3:30 p.m. SA Andrews again conducted a keyword search using "zadom" and observed a file titled "(Hussyfan) (Pthc) Zadom Pedo Age 6yr-3 (Demo).mpg" (hereinafter "File 3"). She attempted but was unable to download this file from IPA-.246 having received an error message of "need more sources." (Affidavit, ¶33) She queried the P2P LimeWire FAQs (Frequently Asked Questions) and received information that:

If the person who has the file your're [sic] trying to download has too many people requesting files, he won't be able to serve any more file requests, and your connection will be refused.

(Affidavit, ¶33) SA Andrews then conducted a parallel query of the exact same file title at a different IPA. She was able to download a movie file depicting a prepubescent female engaged in vaginal intercourse with an adult male. (Affidavit, ¶33) SA Andrews sought other files available from IPA-.246 but could not view such, surmising that the user was banning other users from gaining access to files. (Affidavit, ¶¶ 33, 34)

²An image file is given a title. It can contain a single image or multiple images. ".JPG" is a file extension at the end of a title that identifies graphic images encoded and stored in compressed form. ".MPG" is a file extension at the end of a title that identifies encoded data streams containing audio and video information. (Affidavit, ¶29)

SA Andrews utilized online database *checkdomain.com* to determine ownership of IPA-.246 and found that it was registered to Internet Services Provider Cox Communications. An administrative subpoena served on Cox Communications for IPA-.246 provided her with information that it was used on August 4, 2004 from 11:35 a.m. to 5:30 p.m. and on August 6, 2004 from 2:50 p.m. to 3:30 p.m. and was assigned to the Defendant herein at 5400 South Wembly Road, Tucson, Arizona 85746 with a telephone number of (520) 272-1810. (Affidavit, ¶35)

Other investigative data utilized and submitted by SA Andrews as grounds for probable cause were that: (1) on August 16, 2004, an administrative subpoena served on Cox Communications provided her with information that on August 4 and August 6, 2004 IPA-.246 used high speed data internet service at 5400 South Wembly Road, Tucson, Arizona 85746; (2) on August 19, 2004, Anthony Hibble, a senior computer support systems analyst employee at the University of Arizona Office of Student Computing Resources, was receiving electrical service from Tucson Electric Power Company at 5400 South Wembly Road, Tucson, Arizona 85746; (3) on August 20, 2004, postal records of the U.S. Postal Inspector's Office was delivering mail to a Tony Hibble at 5400 South Wembly Road, Tucson, Arizona 85746 and to a business name of Humingbird [sic] Computer Services at the same address; (4) an Arizona driver's license query disclosed Anthony David Hibble with a date of birth of October 8, 1958 residing at 5400 South Wembly Road, Tucson, Arizona 85746. (Affidavit, ¶¶37-40)

Based on the above described computer transmissions and factual information, Magistrate Judge Nancy F. Fiora on October 6, 2004 issued a search warrant after finding probable cause to believe that Defendant Anthony David Hibble, residing at 5400 South Wembly Road, Tucson, Arizona 85746 was involved in transmitting child pornography in violation of Title 18 U.S.C. §2252. The search warrant was executed on October 7, 2004. A list of property seized pursuant to the search warrant was returned on October 13, 2004. (See October 13, 2004 Return of Search Warrant) The property seized from Defendant at

5400 South Wembly Road, Tucson, Arizona, consisting of computers, digital cameras, computer related equipment, storage media, paperwork and photographs, is the object of Defendant's Motion to Suppress.

III. DEFENDANT'S ALLEGATIONS OF MATERIALLY FALSE STATEMENTS OR OMISSIONS IN THE AFFIDAVIT FOR SEARCH WARRANT MADE KNOWINGLY AND INTENTIONALLY OR IN RECKLESS DISREGARD FOR THE TRUTH

A. Files Downloaded

Defendant argues that SA Andrews could not have downloaded Files 1 and 2 on August 4, 2004 from Defendant's IPA-.246 because his witness, computer forensics expert Ms. Tami L. Loehrs, states by affidavit that after several hours of work she could not find Files 1 and 2 on Defendant's hard drive designated as hard disk drive (hereinafter "HDD") QPX8_1 on Defendant's computer designated QPX8. (*See* Loehrs Affidavit attached to Defendant's Motion as Exhibit 2)

The Government's expert witness, FBI certified computer forensic examiner Mr. Christopher L. Pahl responds by affidavit that when SA Andrews downloaded Files 1 and 2 from IPA-.246 and File 3 from another IPA, each such file was assigned an output value in the form of a 128 bit hash value "fingerprint" unique to each. (*See* Pahl Affidavit attached to the Government's Response as Attachment 2) Moreover, he found hash value "fingerprints" utilizing a Microsoft access database containing information of files examined by him for Files 2 and 3 matching hash value "fingerprints" in HDD QPX9_2 seized from Defendant's home which utilized different titles.

Defendant maintains that these different-titled files had creation dates of September 15 and 18, 2004: dates after SA Andrews download days of August 4 and August 6, 2004. Furthermore, Defendant's expert witness maintains that neither File 2 nor 3 were found in the computer in which the P2P file sharing program was housed.

The Government's expert witness states that creation dates may not be trustworthy or accurate because: (1) the user can manually change dates and times; (2) dates and times may indicate when a file was relocated; or (3) current privacy software allows a user to change, mask, or hide dates. Furthermore, the Government's expert witness cannot corroborate Defendant's expert witness' creation dates claim.

B. Files Available for Downloading

Defendant argues that SA Andrews' list of six files available for downloading from IPA-.246 is intentionally misleading, unreliable, and in reckless disregard for the truth in that the titles were simply "names" and may have been otherwise empty, deleted, corrupted, or incomplete files unless actually opened, viewed, and downloaded. Moreover, because these files were not found on Defendant's hard drive by Defendant's expert witness they were listed by SA Andrews to "inflate the issue of probable cause." (Defendant's Motion p.6)

The Government's expert witness responds that because the six files listed by SA Andrews as available for downloading were never actually downloaded by her, no hash value "fingerprint" was created for each of them and their file names could have been changed.

C. Attempted Downloading, Parallel Query and Download

Defendant argues that SA Andrews' failed attempt to download File 3 due to "too many people requesting" this file intentionally misled the issuing Magistrate Judge because she omitted other possible explanations provided by P2P LimeWire FAQs including that "If the person who has the file you're trying to download has since deleted the file or moved it, you may encounter problems downloading the file." (Defendant's Motion, p.7) Defendant's expert witness maintains that (1) such file had a create date of September 18, 2004 subsequent to when SA Andrews "supposedly downloaded the file from Defendant's computer" (Defendant's Motion, Ex. 2, ¶16); (2) was not found on the computer identified as QPX8_1; and (3) was found in deleted space on a hard drive identified as QPX9_1.

The Government responds that File 3 was downloaded from a parallel query of the exact same file title at a different IPA at which time a hash value "fingerprint" was obtained.

Moreover, at a later time the Government's expert witness utilized a Microsoft access database and found a matching hash value "fingerprint" renamed "age6-3.mpg" with modified and last-accessed dates of March 26, 2001 and October 6, 2004 respectively.

Defendant argues that SA Andrews, failing to download File 3 on August 6, 2004 from the Defendant's IPA, should have ceased investigating and not resorted to a parallel query and download from another IPA.

D. Banning Other Users' Access to Files

Defendant argues that SA Andrews provided misleading and unreliable information and omitted innocuous reasons for why she could not search for other files including: (1) that the error message "could not browse host" as disclosed by the Government does not imply that Defendant is banning people from viewing his material; or (2) Defendant may be using software that does not have the option to "browse host."

E. Matters Beyond the Affidavit for Search Warrant

Defendant cites to an FBI cyberletter; to Congressional testimony by Mr. James E. Farnan, Deputy Assistant Director, Cyber Division-FBI; to an FBI press release; and to a U.S. Department of Justice press release relating that P2P systems can be the subject of intrusions by computer hackers, or that computer hackers can "spoof" unwitting victims to provide information from unsolicited e-mails, or that wireless equipment can be intruded upon by hackers. Defendant states that SA Andrews "must have known" these potentialities and it should have prompted her to investigate further for probable cause rather than "downloading 2 files that do not exist on the Defendant's hard drive."³ (Defendant's Motion, p.9); that she should have downloaded the list of six files she cited as a sampling of files available for downloading from IPA-.246; that she could have engaged in an internet "chat"

³As noted *supra* at section III.A, the Government was able to download Files 2 and 3 from Defendant's computer and, therefore, such files arguably exist.

in the LimeWire sharing program⁴; or made attempts to contact Defendant's neighbors to discover that his neighbor and passers by had access to his internet connection and thus IPA-.246.

In summary, the issuing Magistrate Judge was provided materially false statements or material omissions were made in the Affidavit for Search Warrant knowingly and intentionally or in reckless disregard for the truth because computer technology is vulnerable to hacking, "spoofing", identity theft, tampering, viruses and destruction.

IV. DISCUSSION

The Fourth Amendment requires that the trial court conduct an evidentiary hearing to determine the validity of a search warrant when a defendant has made a substantial preliminary showing that a materially false statement or a material omission was made knowingly and intentionally or with reckless disregard for the truth by a search warrant affiant in establishing probable cause. *Franks v. Delaware*, 438 U.S. 154 (1978). To make a substantial preliminary showing which entitles a defendant to a *Franks* hearing, the following five requirements must be met:

- (1) the defendant must allege specifically which portions of the warrant affidavit are claimed to be false;
- (2) the defendant must contend that the false statements or omissions were deliberate or recklessly made;
- (3) a detailed offer of proof, including affidavits, must accompany the allegations;
- (4) the veracity of only the affiant must be challenged; and
- (5) the challenged statements must be necessary to find probable cause.

⁴Curiously, Defendant cites SA Andrews' description in the Affidavit of the ability of pornographers to communicate anonymously.

Id., at 171; *United States v. Dicesare*, 765 F.2d 890, 894 (9th Cir. 1985), *as amended* 777 F.2d 543 (9th Cir. 1985); *United States v. Kiser*, 716 F.2d 1268, 1271 (9th Cir. 1983).

There is a presumption of validity with respect to the affidavit supporting the warrant. *Franks*, 438 U.S. at 171. Moreover, a magistrate judge's determination of probable cause "should be paid great deference." *Illinois v. Gates*, 462 U.S. 213, 236 (1983) (*quoting Spinelli v. United States*, 393 U.S. 410, 419 (1969)). A totality of the circumstances test is applied and probable cause means "fair probability", not certainty or preponderance of the evidence. *Id.*, at 246.

In short, a magistrate judge is only required to answer the "commonsense, practical question of whether there is 'probable cause' to believe that contraband or evidence is located in a particular place" before issuing a search warrant.

United States v. Gourde, 440 F.3d 1065, 1069 (9th Cir. 2006) (en banc), *petition for cert. filed* July 7, 2006, (*quoting Gates*, 462 U.S. at 230).

Herein, the affidavit for search warrant contained sufficient facts to support the Magistrate Judge's finding that there was a "fair probability" that Anthony David Hibble's computer, related devices and media contained evidence that he violated Title 18 U.S.C. § 2252. *See Gourde*, 440 F.3d at 1067 (“[A]ll data necessary to show probable cause for the issuance of a search warrant must be contained within the four corners of a written affidavit given under oath.”) SA Andrews, relying on her specialized training as a member of the FBI Innocent Images Task Force–Sexual Assault Felony Enforcement (SAFE) Team, conducted a keyword search using the term "zadood". In her experience this term is associated with child pornography files. As a result of her search she downloaded two files from IPA-.246: one titled "PTHC Ultra Hard Pedo Child Porn Pedofilia (New) 057(2).jpg" which depicted a prepubescent female being kissed on the lips by an adult male⁵; the other titled "PTHC

⁵This file for purposes of the instant Report and Recommendation has been referred to as File 1. It was downloaded by SA Andrews from IPA-.246 on August 4, 2004 and consequently a hash value "fingerprint" was obtained for it. It is alleged in Count 1 of the

Ultra Hard Pedo Child Porn Pedofilia (New) 058(1).jpg" which depicted a nude prepubescent female's vaginal area being touched by an erect adult penis.

It is unequivocal that the two aforementioned files by title or the images they depict as described in the affidavit provide a "fair probability" that they were child pornography in violation of Title 18 U.S.C. §2252 when the affidavit for search warrant was submitted to the Magistrate Judge on October 6, 2004. *See Gourde*, 440 F.3d at 1070 ("...the evidence is unequivocal that [the website itself] was a child pornography site whose primary content was in the form of images.") There is nothing that indicates that SA Andrews' actions in finding, reviewing, downloading and describing the contents of the files were actually false and that they were made knowingly and intentionally in reckless disregard for the truth. Any shortcomings by the Government alleged by Defendant regarding the existence or non-existence of illegal images in Defendant's property is, if anything, a question of how images may be retrieved from a computer, related devices or media and more suitably presented at trial.

SA Andrews provided the Magistrate Judge with a sampling list of six files available, but not downloaded, on August 4, 2004 from IPA-.246. Based on two other files downloaded on the same date coupled with the six files' descriptive titles there was a "fair probability" that they too would be found in Defendant's possession when the warrant issued on October 6, 2004. Neither certainty nor a preponderance is required at this point. The fact or allegation that these six files have not been found does not indicate that they never existed and that SA Andrews knowingly and intentionally submitted to the Magistrate Judge materially false statements that they did exist. They may have been expurgated or relocated.

Indictment as one of two computer images Defendant attempted to mail, transport and ship in interstate or foreign commerce by means of a computer. A review of the affidavit by Government expert witness Mr. Christopher L. Pahl reveals that a matching hash value "fingerprint" in Defendant's computer, related devices and media has not been found as of the unknown date of his affidavit.

Moreover, "[i]n the electronic context, a person can receive and possess child pornography without downloading it, if he or she seeks it out and exercises dominion and control over it." *United States v. Romm*, ___ F.3d. ___, 2006 WL 2042827 (9th Cir. July 24, 2006). Any opposition to the introduction of the list of six titles, which could suggest a person's inclinations or proclivities, is more appropriately addressed at trial by a motion in limine or as part of the defense against the charges.

On August 6, 2004, SA Andrews again conducted a keyword search using "zadoom". IPA-.246 was observed to have a file, referenced for purposes of this Report and Recommendation as File 3, which by a commonsense and practical reading would indicate child pornography as its contents. *See Gourde*, 440 F.3d at 1069 (affirming district court's "common sense approach to conclude" that the "recitations in the affidavit supported a fair probability that evidence of a crime would be found on [the defendant's] computer.") Unable to download this file, SA Andrews conducted a parallel query and download of the exact same file title from another IPA. It too contained images of a prepubescent female engaged in sexual vaginal intercourse with an adult male. Defendant posits that probable cause was lacking in this instance and in the instance of the six aforementioned files because SA Andrews did not download them directly from IPA-.246 in order to establish with certainty that they existed therein. Probable cause only requires a "fair probability" that the illegal images exist at the time a search warrant application is made.⁶ The circumstances that led to SA Andrews performing a parallel query and download of File 3 is not unlike one obtaining information that Person A has the current month's issue of *Field and Stream* in his home, going to a magazine shop and purchasing that same issue and later finding the same issue in Person A's home.

⁶As noted *supra* at III.C, the Government's expert later found File 3 under a new title in Defendant's property because of its distinctive hash value "fingerprint."

SA Andrews submitted the facts and information she had that child pornography was accessed through the internet from IPA-.246. She set out information that would support a fair probability as to who was accessing and had access to the illegal images. Outlining in cogent and reasonable fashion she linked the keyword "zadoom" associated with child pornography to IPA-.246 -- IPA.246 to Cox Communications -- to the dates and times IPA-.246 was used -- to IPA-.246 being assigned to Defendant at a particular address. Then by cross-reference and cross-confirmation through Tucson Electric Power Company, the U.S. Postal Service, and the Arizona Department of Motor Vehicles she substantiates that Defendant lives at the residential address of the IPA-.246 assignee and confirms that he is employed at the University of Arizona as, of all things, a senior computer systems analyst.

SA Andrews in her affidavit went to great lengths to describe how evidence of child pornography is accessed, obtained, stored and sought to be secreted and that such illegal images are still capable of being retrieved by FBI computer forensics experts. As *Gourde* recognized:

[t]hanks to the long memory of computers, any evidence of a crime was almost certainly still on [the defendant's] computer, even if he had tried to delete the images. FBI computer experts, cited in the affidavit, stated that "even if ... graphic image files [] have been deleted ... these files can easily be restored." In other words, his computer would contain at least the digital footprint of the images. It was unlikely that evidence of a crime would have been stale or missing, as less than four months had elapsed between the closing of the Lolitagurls.com website and the execution of the search warrant. *See United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1977) (holding that the nature of the crime involving child pornography, as set forth in the affidavit, "provided 'good reason[']' to believe the computerized visual depictions downloaded by Lacy would be present in his apartment when the search was conducted ten months later").

Gourde, 440 F.3d at 1071. Likewise, the Affidavit herein also indicated that "the search of a computer system...is designed...to recover even 'hidden,' erased, compressed, password-protected, or encrypted files." (Affidavit, ¶15; *see also* Affidavit, ¶¶ 8 13, 14, 16) SA Andrews establishes with "fair probability" that Defendant had illegal images; that he had accessed and was offering access to these illegal images; and that they were still retrievable from his computer and that was the only reasonable inference that the Magistrate Judge could

draw. *Gates*, 462 U.S. at 240. (A magistrate judge may “draw such reasonable inferences as he will from the material supplied to him by applicants for a warrant.”); *See Gourde*, 440 F.3d at 1071 (“Given this triad of solid facts—the site had illegal images, Gourde intended to have and wanted access to these images, and these images were almost certainly retrievable from his computer if he had ever received or downloaded them—the only inference the magistrate judge needed to make to find probable cause was that there was a ‘fair probability’ that Gourde had, in fact, received or downloaded images.”)

Defendant argues that there are a myriad of explanations that could account for the images of child pornography in his computer, related devices and media: hacking, “spoofing”, tampering, theft, destruction, or viral infections by others. Defendant argues that SA Andrews could have had an internet “chat” to identify the suspect. The Defendant argues that SA Andrews could have investigated further to discover that his neighbor was accessing his open wireless router, although he offers no identifying information as to who this neighbor might be or how he would know that his neighbor had done this. All these issues are more suitably addressed at trial by way of his defense. An affidavit may support probable cause even when the Government fails to obtain potentially dispositive information. *Gourde*, 440 F.3d at 1073 n.5 (citing *United States v. Miller*, 753 F.2d 1475, 1481 (9th Cir. 1985)).

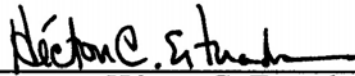
V. RECOMMENDATION

For the foregoing reasons, Defendant has failed to make a substantial preliminary showing warranting a *Franks* hearing and a review of the Affidavit for Search Warrant establishes by a totality of the circumstances the requisite probable cause. Therefore, the Magistrate Judge recommends that the District Court deny Defendant's request for a *Franks* hearing and deny Defendant's Motion to Suppress Evidence Illegally Seized (Doc. No. 27).

Pursuant to 28 U.S.C. §636(B) and Rule 59 of the Federal Rules of Criminal Procedure, any party may serve and file written objections within ten days after being served with a copy of this Report and Recommendation. If objections are filed, the parties should use the following case number: CR 05-1410-TUC-DCB.

Failure to file objections in accordance with Fed.R.Cr.P. 59 will result in waiver of the right to review.

DATED this 8th day of August, 2006.



Héctor C. Estrada
United States Magistrate Judge