IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA, **Plaintiff,** **vs.** **TIMOTHY DE FOGGI,** **Defendant.**	**8:13CR105** **FINDINGS AND RECOMMENDATION**

This matter is before the court on three pretrial motions filed by defendant Timothy DeFoggi (DeFoggi). DeFoggi seeks suppression of any evidence obtained through interception of electronic communications pursuant to a November 18, 2012, Order. **See** Filing No. 97. Additionally, DeFoggi seeks suppression of evidence obtained during the search of DeFoggi's residence on April 9, 2013, pursuant to a search warrant. **See** Filing No. 105. DeFoggi contests the sufficiency of probable cause alleged in the affidavit supporting the search warrant by challenging the officers' reliance on two particular usernames. ***Id.*** Finally, in a related motion, DeFoggi's Motion in Limine seeks to prevent the government from referencing the "fantasy chat private messages sent to and from" those two particular usernames, arguing the messages are irrelevant or overly prejudicial to him. **See** Filing No. 95.

DeFoggi is charged in the Indictment with knowingly engaging in a child exploitation enterprise, in violation of 18 U.S.C. § 2252A(g) (Count I); conspiracy to advertise child pornography, in violation of 18 U.S.C. § 2251(d)(1) and (e) (Count II); conspiracy to distribute child pornography, in violation of 18 U.S.C. § 2252A(a)(2) and (b)(1) (Count III); and knowingly accessing a means or facility of interstate commerce to view child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B) (Counts IV-VII). **See** Filing No. 1. Additionally, the Indictment alleges forfeiture of any property used to commit or promote the commission of the crimes alleged is warranted.

The court held an evidentiary hearing on DeFoggi's motions on March 25, 2014. DeFoggi was present for the hearing along with his counsel, John S. Berry, Jr. The United States was represented by Assistant U.S. Attorney Michael P. Norris and U.S.

AUTHENTICATED U.S. GOVERNMENT INFORMATION GPO

Department of Justice attorneys Keith A. Becker and Sarah Chang. During the hearing, the court received into evidence: a certified wiretap application (Ex. A - SEALED), a letter to Deborah Gilg (Ex. 1 - SEALED), Pedobook private messages (Ex. 2), Pagefile messages (Ex. 3), iMGSRC comments (Ex. 4), and Pedobook rules (Ex. 6). A transcript of the hearing (TR.) was prepared and filed on March 31, 2014. **See** Filing No. 133.

FINDINGS OF FACT

The twenty-three page April 2, 2013, affidavit in support of the search warrant for DeFoggi's residence contains descriptions of the affiant's law enforcement experience, Website A, and the investigation of Website A leading to DeFoggi and his residence. **See** Filing No. 122-1 Sealed. Generally, the affiant alleged an internet website, designated "Website A" for the purposes of the affidavit, was established for the primary purposes of advertising and distributing child pornography and providing a bulletin board for the discussion of matters pertinent to the sexual abuse of children, including the facilitation of anonymous communications and the prevention of detection by law enforcement. Website A is alleged to have operated from March of 2012 until December of 2012. Law enforcement seized the computer server hosting Website A from a web-hosting facility in Bellevue, Nebraska, on November 18, 2012. It is alleged Website A remained operational from November 19, 2012, through December 8, 2012. Law enforcement officers documented and examined the contents of Website A. The name of Website A contained a term referring to a sexual interest in children. The site contained rules, which were accessible from the main page, pronouncing the site a tool for communication among pedophiles to discuss their interests and share "content." In the affiant officer's experience the term content in this context referred to child pornography. The site listed over 8,100 members. A user was able to register with a username and password. Once registered, a user could set up a profile with a picture and is given access to private groups and messages not available to other users. Website A compiled files posted by members into one section, which contained 17,000 images and 120 videos depicting minor children engaging in sexually explicit conduct or child erotica. Website A users were able to set up groups for specific interests or subcategories for postings of distinct types of child pornography on the site. One such

subcategory was pedophilic videos with "no limits," which in the affiant officer's experience referred to violent sexual activity.

Website A operated on a computer network designed to facilitate anonymous communication over the internet. Software required to access the Network prevented the site from learning the user's physical location by routing communications through other computers, which made traditional IP (Internet Protocol) identification techniques ineffective. After connecting to the Network, a user could only access Website A with a specific web address unavailable by conducting a traditional internet search.

One Website A user registered on April 18, 2012, with the username "fuckchrist" and display name "PTasseater." PT in the affiant officer's experience commonly refers to pre-teen in child pornography forums. This user accessed Website A groups titled, "Anything Goes -- Hardcore Child Fucking" and "Babies & Toddlers" on more than one occasion, accessing images depicting adults engaging in sexually explicit conduct with children. These groups also contained other thumbnail images of child exploitation materials visible to members or users allowed access to the group. Law enforcement reviewed private messages sent by "PTasseater"/"fuckchrist" to other Website A users. Dozens of those messages advocated and described an interest in the violent rape of children, including infant and toddler-aged children, in graphic language and detail. Multiple private messages also described the user's location as in or near "DC" and stated he normally accessed the Network between 4:00 a.m. and 6:00 a.m. Eastern Time and again between 4:30 p.m. and 6:00 p.m.

Law enforcement officers discovered an account created in July 2007 with the username "ptasseater" on an image hosting website also known to be used for uploading and distributing child exploitation images. The username was associated with two email addresses: "ptasseater@gmail.com" and "jsnparsons@yahoo.com." The username had been locked due to indecent comments. The "ptasseater" account bore numerous similarities to the "PTasseater"/"fuckchrist" account on Website A, including comments of a sexual nature advocating violent rape and murder of underage individuals. Law enforcement officers identified an IP address used 469 times between May and December 2011, by the "ptasseater" account user. The IP address resolved to Verizon Internet Services, which identified Tim DeFoggi, his address, and cellular

telephone number, as the individual assigned to the IP address from May 2011 to May 2012.

The registration IP address used for the "jsnparsons@yahoo.com" email address, registered with the name of Jason Parson in 2007, was also used in 2006 by the email addresses "notaboo_69@yahoo.com," registered with the name Jack Parsons, and "luvemskinny@yahoo.com," registered with the name Jock Hoff. Also in the fall of 2006, the individual identified as "Jeff" and using the "notaboo_69@yahoo.com," "luvemskinny@yahoo.com," and "ptasseater@hotmail.com" email addresses was a member of "boylover.net," a website known for underage male exploitation material. The individual identified as Jeff personally met another individual, who was a subject under investigation by the FBI, and said his real name was Tim and he worked in the Washington DC area. Additionally, individual known as Jeff or Time carried a cellular telephone with the same number registered to Timothy DeFoggi.

An individual also used PTasseater as a profile on the website dickflash.com. The profile was associated with the username "showgenitals," an America Online (AOL) Instant Messenger (AIM) username ptasseater, and the email address "genericaddr@yahoo.com." The email address was associated with the name Jack Parsons. The AIM username was a member since September 11, 2013, using the screen name luvemskinny@yahoo.com, and was still in use as of November 21, 2012. The IP addresses derived from the AOL log information were assigned to Tim DeFoggi.

Law enforcement officers obtained a pen register/trap trace to monitor the internet service account at DeFoggi's address. The monitoring revealed internet connections to IP addresses associated with the Website A Network primarily in the early morning or late evening hours, consistent with statements made by "PTasseater"/"fuckchrist" to other Website A users.

LEGAL ANALYSIS

A. Interception of Electronic Communications

DeFoggi seeks suppression of any evidence obtained through interception of electronic communications pursuant to a November 18, 2012, Order. **See** Filing No. 97. DeFoggi contends the application failed to identify an official specially designated by the

Attorney General of the United States who authorized the application in accordance with 18 U.S.C. § 2518(1)(a). ***Id.*** DeFoggi notes the application "alludes to a memorandum identifying an authorized official who approved the application, but the memorandum was not attached." ***Id.*** at 2. DeFoggi argues this failure renders the application fatally facially deficient. ***Id.*** DeFoggi filed a brief (Filing No. 98) and an index of evidence (Filing Nos. 99 and 114 - Sealed) in support of this motion to suppress. The government opposes the motion to suppress, filing a brief (Filing No. 117) and an index of evidence (Filing No. 119- Sealed), stating a copy of the approval memorandum was inadvertently omitted from discovery.

The record in this matter reflects, on November 18, 2012, upon application of the United States in sealed case 8:12WT11, the Chief Judge of the U.S. District Court for the District of Nebraska authorized the interception of electronic communications, ultimately including DeFoggi's communications. **See** Ex. A - Sealed. The application submitted in connection with that authorization included, as an exhibit, a copy of a memorandum signed by Kenneth A. Blanco, Deputy Assistant Attorney General for the Criminal Division of the Department of Justice, authorizing the application, as required by 18 U.S.C. § 2518(1)(a). **See** Ex. A - Sealed. A Deputy Assistant Attorney General for the Criminal Division is empowered to authorize an application for interception of electronic communications pursuant to 18 U.S.C. § 2516(1). Because the record reflects the application included the identity of an official specially designated by the Attorney General of the United States who authorized the application in accordance with 18 U.S.C. § 2518(1)(a), DeFoggi's motion to suppress (Filing No. 97) evidence obtained through interception of electronic communications pursuant to a November 18, 2012, Order should be denied. Accordingly, the court finds the authorizing judge in the instant case had the name of the actual, statutorily designated official who had indeed authorized the application. **See *United States v. Lomeli***, 676 F.3d 734, 741-42 (8th Cir. 2012).

B. Search Warrant

DeFoggi seeks suppression of evidence obtained during the search of DeFoggi's residence on April 9, 2013, pursuant to a search warrant. **See** Filing No. 106 - Brief.

DeFoggi filed a brief (Filing No. 106) and an index of evidence (Filing Nos. 107 and 111 - Sealed) in support of the motion. DeFoggi contests the sufficiency of probable cause alleged in the affidavit supporting the search warrant by challenging the officers' reliance on two particular usernames. ***Id.*** Specifically, DeFoggi argues there is no direct connection between the usernames and DeFoggi's address. **See** TR. 26. Similarly, DeFoggi contends the usernames may be prevalent on the internet, rather than unique to DeFoggi or the address. ***Id.***

The government opposes DeFoggi's motion. The government filed a brief (Filing No. 120) and an index of evidence (Filing No. 122 - Sealed) in opposition to the motion. The government argues several pieces of evidence link DeFoggi's residence and identity to the usernames appearing in chats on Website A, providing a fair probability evidence of a crime would be found at the residence, despite other possible individuals with the same usernames. **See** TR. 27-28. Moreover, additional independent police investigation corroborated such evidence. ***Id.***

An affidavit for a search warrant must contain probable cause of four ingredients: time, crime, objects, and place. 2 Wayne R. LaFave, Search & Seizure § 3.7(d) at 412 (4th ed. 2004). When reviewing the sufficiency of an affidavit the court applies "a common sense approach and consider[s] all relevant circumstances." ***United States v. Vore***, 743 F.3d 1175, 1179 (8th Cir. 2014). "Probable cause sufficient to justify a search exists where, in the totality of the circumstances, there is a fair probability that contraband or evidence of a crime will be found in a particular place." ***Id.*** More specifically, "the warrant application and affidavit must describe circumstances showing that, based on practical experience and common sense, there is a fair probability that [the object of the search warrant] will be found in the targeted place." ***United States v. Vega***, 676 F.3d 708, 717 (8th Cir. 2012) (internal quotation and citation omitted); **see** ***United States v. Romo-Corrales***, 592 F.3d 915, 919 (8th Cir. 2010).

As the Supreme Court stated in ***Illinois v. Gates***:

> The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the "veracity" and "basis of knowledge" of persons supplying hearsay information, there is a fair probability that

> contraband or evidence of a crime will be found in a particular place.

Illinois v. Gates, 462 U.S. 213, 238 (1983). When relying on an affidavit to establish probable cause, "the probable cause determination must be based upon only that information which is found within the four corners of the affidavit." ***United States v. Stults***, 575 F.3d 834, 843 (8th Cir. 2009). "Probable cause must exist when a warrant is issued, not merely at some earlier time, but there is no bright-line test for determining when information is stale . . . ." ***United States v. Morrison***, 594 F.3d 626, 631 (8th Cir. 2010). "[S]taleness is a case-specific inquiry, and probable cause cannot be judged by simply counting the number of days between the occurrence of the facts supplied and the issuance of the affidavit." ***United States v. Darr***, 661 F.3d 375, 378 (8th Cir. 2011) (internal quotation omitted). "[T]he lapse of time is least important when the suspected criminal activity is continuing in nature and when the property is not likely to be destroyed or dissipated." ***United States v. Lemon***, 590 F.3d 612, 614 (8th Cir. 2010) (alteration in original and citation omitted) (noting evidence presented in affidavit not stale where eighteen-month gap between uploading child pornography images and application for search warrant); **see *United States v. Needham***, 2013 WL 4519414, at *4 (D. Minn. Aug. 26, 2013) (one-year gap).

The search warrant application in this case supports a finding of probable cause. **See, e.g.**, ***United States v. Kinison***, 710 F.3d 678, 683-84 (6th Cir. 2013). From the search warrant application, one can reasonably infer DeFoggi employed the username "ptasseater" from 2003 through December 2012 and the usernames "PTasseater"/"fuckchrist" with respect to Website A within a few months of the warrant's issuance. The government investigation revealed DeFoggi had one or more memberships, connected to the relevant usernames, in websites known to contain child pornography and one or more IP addresses connected the membership to DeFoggi and his location at his residence. Further the affidavit provided evidence DeFoggi continued to use the IP addresses associated with the Network during the early morning hours after Website A ceased operations. The court concludes the information in the affidavit raised a fair probability that a search of DeFoggi's residence would result in the

discovery of child pornography and DeFoggi's participation in a child exploitation enterprise.

C. Motion in Limine

DeFoggi's Motion in Limine seeks to prevent the government from referencing the "fantasy chat private messages sent to and from" particular usernames from Website A, arguing the messages are irrelevant or overly prejudicial to him. **See** Filing No. 95. DeFoggi filed a brief (Filing No. 96) in support of the motion. DeFoggi argues the fantasy chats are not sufficiently relevant to the charges filed against him and should be excluded pursuant to Fed. R. Evid. 401. **See** Filing No. 96 - Brief p. 2. Specifically, he argues the fantasy chats are merely fantasy conversations pleasing to DeFoggi rather than evidence indicative of participation in a child exploitation enterprise. ***Id.*** at 2-3. Additionally, DeFoggi contends any probative value in the chats is substantially outweighed by the danger of unfair prejudice under Fed. R. Evid. 403. ***Id.*** at 3. DeFoggi acknowledges the chats are highly graphic and describe the violent sexual torture and killing of children. ***Id.***; **see** Ex. 2. DeFoggi argues the chats contained fantasy and as such they are overly prejudicial because they describe murder, maiming, and decapitation, which are outside the crime of exploitation of children. **See** TR. 56. DeFoggi asserts the content of these chats creates a likelihood jurors may base a decision of guilt on improper bias or an emotional reaction to the messages. ***Id.*** Moreover, DeFoggi argues suppression of the chats does not deprive the government of vital evidence in the case in light of evidence the individual using the particular usernames clicked on images portraying child pornography. ***Id.*** at 4.

Opposing DeFoggi's motion in limine, the government filed a brief (Filing No. 126) contending the content of the chats are integral to showing DeFoggi knowingly entered into a conspiracy and intended for it to succeed. **See** Filing No. 126 - Brief p. 8. Additionally, the government argues the chats are evidence linking DeFoggi to Website A through the usernames and his intent to view and distribute child pornography. ***Id.*** at 8-11.

"Evidence is relevant if: (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in

determining the action." Fed. R. Evid. 401. Nevertheless, a "court may exclude relevant evidence if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence." Fed. R. Evid. 403. Evidence of chats between a defendant and another may be admissible to show the defendant's state of mind, his intention to possess child pornography, and his knowledge of the illegal nature of the images. **See *United States v. Brumfield***, 686 F.3d 960, 963 (8th Cir. 2012). Chats may be "admissible for an additional reason: as circumstantial evidence (i.e., a non-hearsay purpose) associating [the defendant] with the child pornography found on his computer." ***United States v. Manning***, 738 F.3d 937, 943 (8th Cir. 2014); **see *United States v. Christie***, 624 F.3d 558, 570 (3d Cir. 2010) (noting notebooks and posts to website suggesting the defendant was a predator not unduly prejudicial where they indicated the defendant visited a child pornography website with the purpose of exchanging child pornography); ***United States v. Hite***, 916 F. Supp. 2d 110, 117, 122 (D.D.C. 2013) (finding chats of a graphic nature not unfairly prejudicial when they were "relevant evidence of intent, knowledge, and absence of mistake in that it is probative of his sexual attraction to young children, and reflects [they had] previous conversations about similar topics"). In fact, images of child pornography, themselves, may not be unfairly prejudicial to a defendant, despite his willingness to stipulate to the content of the clips, to demonstrate a representative sample of images found to have been downloaded by a particular user to a computer. ***United States v. Worthey***, 716 F.3d 1107, 1114-15 (8th Cir. 2013).

The court will not recommend limiting the government's evidence to exclude the chats. Here, the content of the chats, while graphic and aberrant, has some tendency to make certain facts more or less probable than it would be without the evidence. Such facts are of consequence in this action. In particular, the chats, both the existence of them and the content, tend to show the identity, intent, and knowledge of the participants. The prejudicial nature of the chats' content does not outweigh the probative value. Essentially the nature of the chats enhances their probative value particularly with respect to the identity and intent of the participant. Upon consideration,

IT IS RECOMMENDED TO DISTRICT JUDGE JOSEPH F. BATAILLON that:

1. DeFoggi's Motion to Suppress Evidence Obtained Through Interception of Electronic Communications (Filing No. 97) be denied.

2. DeFoggi's Motion to Suppress Evidence Obtained Through Search of Defendant's House (Filing No. 105) be denied.

3. DeFoggi's Motion in Limine (Filing No. 95) be denied.

ADMONITION

Pursuant to NECrimR 59.2 any objection to this Findings and Recommendation shall be filed with the Clerk of the Court within fourteen (14) business days after being served with a copy of this Findings and Recommendation. Failure to timely object may constitute a waiver of any objection. The brief in support of any objection shall be filed at the time of filing such objection. Failure to file a brief in support of any objection may be deemed an abandonment of the objection.

Dated this 9th day of June, 2014.

BY THE COURT:

s/ Thomas D. Thalken
United States Magistrate Judge