IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF KANSAS

UNITED STATES OF AMERICA, Plaintiff,	)	**CRIMINAL ACTION**
v.	)	No. 13-10016-MLB
ELIAS BARTHELMAN, Defendant.	)	

MEMORANDUM AND ORDER

This case comes before the court on defendant's motion to suppress. (Doc. 28). The motion has been fully briefed (Docs. 31, 32, 35, 36, 37) and the court conducted an evidentiary hearing on June 18, 2013. The motion to suppress is granted in part and denied in part for the reasons herein.

I. Facts

On February 23, 2012, the mother of Jane Doe, an 11 year old girl, contacted the Ohio Internet Crimes Against Children (ICAC) and reported that Jane Doe was having a conversation on Google Plus with an adult male.[1] Rick McGinnis, an investigator with the Cuyahoga County prosecutor's office, went to Jane Doe's home and interviewed the minor. McGinnis received permission from Jane Doe and her mother to search Jane Doe's email account with Google and Jane Doe's Ipod touch, an electronic device used to send text messages. The Ipod touch contained five thumbnail images of a nude female. Jane Doe

[1] The adult male referenced in the initial call was not defendant. At the time he prepared the affidavit, officer McGinnis had knowledge that the adult male was not "John," the male who is later identified in the emails and eventually as defendant.

identified those images as ones she took of herself. The Ipod device also contained three thumbnail images of what "appeared to be" an adult male penis. Jane Doe's mother informed McGinnis by email that Jane Doe sent nude images to an individual identified as "John" and that this individual sent images of his penis to Jane Doe.

After reviewing the emails in Jane Doe's account, McGinnis determined that Jane Doe sent five videos to an individual with an email account of johnsmith19910@yahoo.com ("johnsmith") on January 17, 2012, between 7:46 and 7:48 p.m. The emails did not contain written text. There were no emails from "johnsmith" to Jane Doe prior to Jane Doe's transmission of the videos. On January 18, "johnsmith" sent an email to Jane Doe which said "hey, unblock me on textplus please." (Def. exh. A at 5). On January 19, Jane Doe responded "no!" (Id.) On January 20, "johnsmith" stated "awww, come on, that was a lot of fun, lets have sum [sic] more fun ;)." (Id.) Jane Doe responded "No! No! No! You are not dragging me into that - if you reply to this, I will seriously consider reporting you to the police." (Id.) That same evening, "johnsmith" sent a response asking "r u gonna sho them the vids u sent me? cuz I will!" (Id. at 6)(sic throughout). The last email between Jane Doe and "johnsmith" occurred at 7:44 p.m. on January 20 and was sent by Jane Doe stating "no...I'm eleven years old. seriously. stop emailing me and get a nonsexual life." (Id. at 5).

On March 20, 2012, McGinnis met with Jane Doe and her mother to verify the videos in the emails. Jane Doe confirmed that the videos were taken by her and that she appears in the videos. On March 21, 2012, a grand jury subpoena was sent to Yahoo Inc. requesting account

and IP address information for the Yahoo mail user "johnsmith19910@yahoo.com." The return provided information which led McGinnis to subpoena Cox Communications for the account information for the specific IP address identified by Yahoo. The account was registered to defendant at 422 East Quivira Street in Kechi, Kansas.

On May 3,[2] McGinnis applied for a search warrant for the "johnsmith" email account from Judge Corrigan of the Cuyahoga County District Court in Ohio. On the application for the warrant, McGinnis swore to the following:

> Affiant has exhibited probable cause necessary to search the below listed property/stored electronic information, wherein affiant avers that he has reasonable cause to believe, and does believe, that said property/stored electronic information, to wit: Yahoo profiles for johnsmith19910@yahoo.com. That is currently in the possession of Yahoo Inc., Sunnyvale, California, and the said property/stored electronic information to be searched being located in the possession of Yahoo Inc. Sunnyvale, California, there is now being kept, concealed, and possessed the following evidence of a criminal offense:
>
> Any and all information for Yahoo! ID "johnsmith19910" or Yahoo! email account "johnsmith19910@yahoo.com"to include name and address; Yahoo! email address; alternate email address; IP address and date and time of registration;
>
> For the subscriber identified above, the contents of any and all emails stored in the subscriber's Yahoo! account from November 1, 2011 through present day;
>
> Any and all contents of electronic files that the subscriber has stored in the subscriber's Briefcase and/or Flickr account;
>
> Any and all Yahoo! IDs listed on the subscriber's Friends list;

[2] The application is dated March 3, but was applied for on May 3. The search warrant, however, states the correct date of May 3. The court finds that the incorrect date on the application is merely a typo and not material.

Any and all methods of payment provided by the subscriber to Yahoo! for any premium services;

The identity of the moderators and members of the Yahoo! Group known from the above Yahoo ID, including the date the Group was created, the Group ID, the dates that members joined the group, and the delivery options for the current members;

The current contents of the Files, Photos, Links, and Polls section of the Yahoo! Group associated with the above Yahoo ID and the archived message posts, and all records relating to the activities of the Group members, as reflected in the Group Activity Log.

Any and all evidence of communications used in the furtherance of the violation of laws of the State of Ohio, to wit: Ohio Revised Code Chapter 2907 and any and all other fruits and instrumentalities of crime at the present time unknown.

The facts upon which affiant bases such belief is as follows:

1. Affiant avers that he has been a certified peace officer in the State of Ohio for approximately twenty years. Affiant avers that he has been in law enforcement for the past twenty years and has been assigned to the Internet Crimes Against Children Task Force for the past five years.

2. Affiant avers that he has received training in the investigation of felony and misdemeanor offenses, including sex offenses and offenses involving compu1ers and/or the Internet and child exploitation.

3. Affiant avers that he has conducted and/or participated in investigations into felony and misdemeanor offenses which have resulted in state and/or federal prosecutions, including, but not limited to, investigations into sex offenses and offenses involving computers and/or the Internet.

4. Affiant avers that on February 23, 2012, [Jane Doe's mother] contacted the Ohio ICAC Task Force and reported that her 11 year-old daughter (hereinafter identified as Jane Doe), was having a chat conversation on Google Plus with an **adult male**. Your affiant interviewed [Jane Doe's mother] and Jane Doe and [Jane Doe's mother] consented to the forensic examination of her daughter's Ipod Touch. Your affiant received permission from [Jane Doe's mother] and Jane Doe to take over "Jane Doe's" Gmail and Google Plus accounts.

5. Your affiant knows that on February 27, 2012, Investigator Jeff Rice completed a forensics examination on the Ipod used by Jane Doe. Investigator Rice's forensics examination identified five nude thumbnail images found of a young female and three thumbnail images of what appears to be an adult male's penis.

6. Affiant avers that on March 20, 2012, he re-interviewed [Jane Doe's mother] and Jane Doe regarding the images discovered on the IPod. Jane Doe advised your affiant that she had taken the image entitled ""_1 05ZU K_1" in her bathroom at her house. This image depicted Jane Doe in a state of nudity with her breasts exposed.

7. Affiant avers that on March 21, 2012 he received an email from [Jane Doe's mother] stating that her daughter admitted to taking all of the images identified by Investigator Rice on the IPod which depicted a minor female child in a state of nudity, specifically displaying her breasts and genitals.

8. Affiant avers that on March 22, 2012, he received additional information from [Jane Doe's mother] stating that her daughter had sent these images and videos to an individual identified only as John and that this individual did send images of his penis to Jane Doe.

9. On March 23, 2012, your affiant logged into "Jane Doe's" Gmail account and discovered five videos sent from "Jane Doe's" Gmail account to an individual using the Yahoo email account of "johnsmith19910@yahoo.com." The videos depicted Jane Doe in a state of nudity and were sent individually on January 17, 2012 at 7:48pm, January 17, 2012 at 7:47pm, January 17, 2012 at 7:46pm, January 17, 2012 at 7:46pm, and January 17, 2012 at 7:48pm.

10. Additionally, your affiant discovered email conversations **from January 17, 2012 thru January 20, 2012 during which time Jane Doe advised the suspect that she was 11 years of age and transmitted nude images of herself to "johnsmith19910@yahoo.com" at his request. Affiant also knows that during these conversations, "johnsmith19910@yahoo.com" threatened Jane Doe to produce and send videos of herself naked and that she filmed herself naked at his request and sent these videos to him.** Your affiant learned that Jane Doe attempted to delete these videos from her Ipod after she produced them.

11. The above information has led Affiant to believe that probable cause exists to believe that the items listed herein (i.e. property/stored electronic information, including information stored by Yahoo, Inc.) are evidence

> of a crime and are now being unlawfully kept, concealed, and/or possessed in the said property/stored electronic information: Yahoo profiles for "johnsmith19910" in violation of Revised Code of Ohio, to wit: R.C. 2907.

(Exh. 2A) (Emphasis added to reflect the statements found to have been falsely made).

The first several paragraphs include language which is taken from the Yahoo compliance manual. This manual is authored by Yahoo for law enforcement and contains sample language which Yahoo requests that officers use in the search warrants. The Yahoo search warrant signed by Judge Corrigan included these paragraphs.

On April 23, 2012, McGinnis contacted the Wichita Police Department's Exploited Missing Child Unit and relayed the information from his investigation. Detective Jennifer Wright received the materials and followed up with McGinnis who later sent her the search warrant and affidavit. Wright did not do an independent investigation but had several conversations with McGinnis.

Wright applied for a search warrant for defendant's home from a judge in Sedgwick County District Court. On the application for the warrant, Wright related the following:

> Affiant is a detective with the Wichita Police Department currently assigned to the Exploited and Missing Child Unit; Internet Crimes Against Children Task Force. In that capacity Affiant was assigned to the follow up investigative duties of case number 12C03 8616. This case involves the allegations of Sexual Exploitation of a Child, KSA 21-5510 where the email account johnsmith19910@yahoo.com used at IP address 68.102.165.185 was utilized to have contact with a known 11 year old unmarried white female, M.S. and to received movie files of M.S. performing sexual acts. After reviewing reports and/or conducting interviews the Affiant has learned the following information:
>
> On Monday, June 4, 2012 Affiant spoke with Investigator Rick McGinnis, Cuyahoga County Prosecutor's

Office, Cleveland, Ohio. McGinnis investigated a case involving an eleven (11) year old unmarried white female, M.S. who had sent five self produced pornography movies to a male using the email account johnsmith19910@yahoo.com on January 17, 2012. McGinnis received a report from M.S.'s mother on February 23, 2012 after she located information that M.S. had engaged in conversations using Google Plus with an adult male. McGinnis obtained a waiver to search for the electronic device used by M.S. to have contact with johnsmith19910@yahoo.com with this device being an Apple I-pod touch. McGinnis said he requested a forensic examination be conducted on this device and received these results from Investigator Jeff Rice on February 27, 2012. Investigator Rice's forensic examination identified five nude thumbnail images found of a young female and three thumbnail images of what appears to be an adult male's penis. McGinnis interviewed M.S. on March 20, 2012, regarding these images found on M.S.'s I-pod touch. M.S. said the images of the young female were of her and that she had taken them at her residence in Ohio. The image titled "_105ZUK_l" is of her nude with her breasts exposed and she advised she took that in the bathroom at her residence in Ohio. M.S. said she sent those pictures to a male named "John" using her Google email account, stannaggie2000@gmail.com. M.S. identified the pictures of the adult male's penis as pictures she received from "john" a male using the email account johnsmith19910@yahoo.com. McGinnis advised in the pictures of the adult male penis he could see in the background light tan linoleum or tile floor with a brown trim and a gray vent cover on the floor itself.

On March 23,2012, Investigator McGinnis logged into M.S.'s email account starmaggie2000@gmail.com after obtaining a waiver for this activity. McGinnis discovered five videos sent from this email account to an individual using the Yahoo email account of johnsmith19910@yahoo.com. These videos were sent individually on January 17, 2012 between 1946 and 1948 hours. McGinnis also located an email conversation from January 17, 2012 to January 20, 2012 during which time M.S. advised this male she was 11 years old and transmitted these five self produced pornography movies to this male at his request. McGinnis also located information during this email conversation that where M.S. had blocked this male on the chat conversation venue utilized by the two of them "textplus" and that she told this male she was 11 years old and to stop emailing her and to get a nonsexual life and that she was considering reporting him to the police. This male replied to this by asking M.S. if she was going to show them (the police) the videos she had sent him because he would and asked

for another video. M.S . told this male no and he replied that it had been fun and to have some more fun. M.S. sent another email stating "no" and that was the last email located on the email account for M.S. by McGinnis.

McGinnis said he viewed all five videos. McGinnis said all five were of M.S. and that he confirmed this with M.S. after she identified them to be movies of her that she produced at the request of the male using email account johnsmith19910@yahoo.com.

[The affidavit then describes the images and actions of the nude female in the videos.]

McGinnis requested and obtained a court order to Yahoo for the subscriber information for the email account johnsmith19910@yahoo.com with this subscriber information including IP connection logs. According to this subscriber information provided by Yahoo the email account johnsmithl9910@yahoo.com utilized the IP address 68.102.165.1 85 during the time the emails sent by M.S. were requested by the male using this email account and also when the emails were sent by johnsmith19910@yahoo.com asking for more and if she was going to show the movies to the police.

The name given for this Yahoo account was John Smith with a zip code of 66610, which is for Topeka, Kansas.

McGinnis verified that this IP address is used by Cox Communications to give customer's internet access and he requested and obtained a court order for Cox Communication regarding the subscriber infom1ation for the IP address 68.102.165.185 during the date(s) and time(s) it was used to communicate with M.S. McGinnis said be received the results of this court order from Cox Communications on April 11, 2012 with the subscriber for this account being ELl BARTHELMAN, 422 QUIVIRA STREET, KECHI, KANSAS 67067-8817.

Affiant verified that Eli Barthelman currently resides at 422 Quivira Street, Kechi, Sedgwick County Kansas.

Affiant knows from training and experience that when an individual who is involved in a computer facilitated sexual exploitation crime has a high level of expertise in the computer technology field those users will utilize means to hide or destroy data regarding the criminal activities they are involved in. Mr. Barthelman's network at his residence was used to commit the above mentioned crime and Mr. Barthelman has a bachelor's degree in computer engineering and maintains employment in this

field. Affiant knows that through the use of mobile devices and other connections to the Internet it is possible to gain access to the computer media connected to the Internet within the residence located at 422 E Quivira, Kechi, Kansas and destroy information prior to officers making entry and securing this media. Affiant believes it is necessary to make contact with Mr. Barthelman prior to the execution of this search warrant to ensure he has no access to the home just before and during the execution of the search warrant.

(Exh. 9).

Wright applied to search the residence for the following items:

1. Images or visual depictions representing the exploitation of children.

2. Computers.

3. Digital communications devices allowing access to the Internet or to cellular digital networks to include cellular telephones, email devices and personal digital assistants.

4. Digital input and output devices to include but not limited to keyboards, mice, scanners, printers, monitors, network communication devices, modems and external or connected devices used for accessing computer storage media.

5. Digital storage media and the digital content to include but not be limited to floppy disks, hard drives, tapes, DVD disks, CD-ROM disks, flash storage or other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data or images of child pornography as defined by K.S.A. 21-5510.

6. Digital software and application software installation and operation media.

7. Contents of volatile memory related to computers and other digital communication devices that would tend to show the current and recent use of the computer, use of encryption, use of other communications devices, routes of internet and other digital communications traffic and passwords, encryption keys or other dynamic details necessary to preserve the true state of running evidence.

8. Computer software, hardware or digital contents related to the sharing of internet access over wired or wireless networks allowing multiple persons to appear on

the Internet from the same IP address.

9. If computers or other digital devices are found in a running state the investigator may acquire evidence from the devices p1ior to shutting the devices off. This acquisition may take several hours depending on the volume of data.

10. Manuals and other documents (whether digital or written) which describe operation of items or software seized.

11. Items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized.

12. Correspondence or other documents (whether digital or written) pertaining to the possession, receipt, collection, origin, manufacture or distribution of images involving the exploitation of children as described in K.S.A. 21-5510.

13. Correspondence, "trophies", grooming aids or other items demonstrating an interest in the exploitation of children as described in K.S.A. 21-5510.

14. Items or digital infom1ation that would tend to establish ownership or use of computers and Internet access equipment and ownership or use of any Internet service accounts and cellular digital networks to participate in the exchange, receipt, possession, collection or distribution of child pornography as described by K.S.A. 21-5510.

15. Items that tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.

16. Pictures of the residence.

17. Any and all correspondence involving the Yahoo ID johnsmith19910@yahoo.com and starmaggie2000@gmail.com.

18. Any and all documents involving the Yahoo ID johnsmith19910@yahoo.com.

(Exh. 9).

The search warrant was executed on June 11, 2012. Detective Wright knocked on the door and identified herself. Defendant stepped

outside and officer Shawn Bostick performed a pat down of defendant's person. Bostick removed defendant's Iphone and discovered that it was locked. Wright asked defendant for the passcode so that the phone could be placed in airplane mode to prevent the phone from being accessible from a computer. Defendant gave his passcode information to Wright. Investigator Michael Randolph performed the search inside the home and located a computer which was running. According to paragraph 9 of the warrant, Randolph was to first secure any evidence from the computer if it was in a running state prior to shutting the computer off. Randolph determined that the computer screen was locked and that he could not access the computer without a passcode. Wright asked defendant for the passcode and he told her his passcode. All electronic devices, including the computer, were seized from defendant's residence. The devices were later searched in a laboratory setting by Detective Hans Asnussen. Asnussen did not need to utilize the passcodes to retrieve the data from the devices.[3]

On August 21, 2012, McGinnis applied for a search warrant (referred to as the Apple warrant) for the "ebarthelman@mac.com" email account from a district judge of the Cuyahoga County District Court in Ohio. On the application, McGinnis included the information contained in the May 3 application for the Yahoo email account and provided the following additional information:

> 13. Affiant knows that upon viewing the email content of Yahoo ID "johnsmith19910@yahoo.com," an email account named "ebarthelman@mac.com," was sending emails containing child pornography which included sexual activity involving prepubescent females engaged in

[3] Therefore, the motion to suppress the statements by defendant during the search is denied as moot.

masturbation.

(Exh. 4A).

On January 29, 2013, the grand jury returned an indictment against defendant charging five counts of child pornography occurring on various dates with five different Jane Does. Defendant moved to suppress the search warrants executed on his residence and email accounts. (Doc. 28).

II. Analysis

A. Yahoo and Apple Search Warrants

Defendant challenges the Yahoo and Apple search warrants on the basis that there were false statements contained in the affidavits. The government responds that defendant did not make a sufficient showing for a hearing under Franks v. Delaware because he failed to submit affidavits establishing an omission or falsehood. (Docs. 31 at 6; 35 at 4).

The parties are well aware of the standards announced in Franks v. Delaware, 438 U.S. 154, 171-2 (1978).

> "Under Franks, a hearing on the veracity of the affidavit supporting a warrant is required if the defendant makes a substantial showing that the affidavit contains intentional or reckless false statements and if the affidavit, purged of its falsities, would not be sufficient to support a finding of probable cause." (Citations omitted). "The standards of deliberate falsehood and reckless disregard set forth in Franks apply to material omissions, as well as affirmative falsehoods." (Citations omitted). If, after considering the evidence presented at a Franks hearing, the district court concludes by a preponderance of the evidence that the affidavit contains "intentional or reckless false statements," (citations omitted), or "material omissions," (citations omitted), "then the district court must suppress the evidence obtained pursuant to the warrant." (Citations omitted). If, however, the district court concludes that the omitted information would not have altered the magistrate judge's decision to authorize

> the search, then the fruits of the challenged search need not be suppressed. (Citations omitted).

United States v. Avery, 295 F.3d 1158, 1166-67 (10th Cir. 2002). Defendant must show that the affiant made intentional or reckless omissions as opposed to omissions negligently made or by innocent mistake. United States v. Artez, 389 F.3d 1106, 1116 (10th Cir. 2004).

In order to be entitled to an evidentiary hearing under Franks v. Delaware, "the defendant must allege deliberate falsehood or reckless disregard for the truth, and those allegations must be accompanied by an offer of proof." United States v. Artez, 389 F.3d 1106, 1116 (10th Cir. 2004) (citing Franks v. Delaware, 438 U.S. 154, 171 (1978)). To support such allegations, a defendant should provide affidavits of witnesses or satisfactorily explain their absence. See id. In addition, a defendant seeking an evidentiary hearing must show that, after the challenged portions of the affidavit are stricken, the remaining content of the affidavit is not sufficient to support a finding of probable cause. See id.; United States v. Nelson, 450 F.3d 1201, 1213-14 (10th Cir. 2006).

Defendant's motion alleges that there are date discrepancies in the application and the warrant of the May 3 Yahoo search warrant. Defendant further alleges that paragraph 10 in the applications was false because the email conversations did not occur prior to the videos being sent. (Doc. 28 at 5-6). The Tenth Circuit cases, citing Franks, require a defendant to make a "substantial preliminary showing" to be entitled to a hearing. However, this phrase is undefined and subject to "interpretation" in the event of appellate

review which, in a worst case scenario, could result in a reversal after a trial. Since a request for a Franks hearing is a motion under Fed. R. Crim. P. 12(b)(3)(C), the decision to hold a hearing was consistent with the goals of Rule 2 and forecloses any claim on appeal that the court erred by not holding a hearing. Moreover, the government does not allege that it has been prejudiced by the discretionary decision to have the hearing.

1. False Statements

The evidence at the Franks hearing established that the first two sentences of paragraph 10 of McGinnis' affidavit contained false and misleading statements. The first sentence states that "[a]dditionally, your affiant discovered email conversations from January 17, 2012 thru January 20, 2012 during which time Jane Doe advised the suspect that she was 11 years of age and transmitted nude images of herself to "johnsmith19910@yahoo.com" at his request." This sentence is false because there is no evidence that Jane Doe sent pictures in response to a request by "johnsmith." This sentence is also misleading because Jane Doe did not advise "johnsmith" of her age until the final email on January 20, after the transmission of the videos on January 17.

The second sentence states that "Affiant also knows that during these conversations, "johnsmith19910@yahoo.com" threatened Jane Doe to produce and send videos of herself naked and that she filmed herself naked at his request and sent these videos to him." The emails, however, do not support this sentence. McGinnis testified that he believed that this was true based on his communications with Jane Doe's mother. However, viewing the emails in the correct

timeline, there is no evidence that "johnsmith" threatened Jane Doe or that she sent pictures to him at his request.

While Jane Doe's emails as shown in McGinnis' report are confusing because they are not in chronological order, the emails do show the date and time prior to the written text in the message. McGinnis testified that he had experience with the way Google displayed messages and explained this to the prosecutor in the case prior to the application for the warrant. Therefore, McGinnis had an obligation to ensure that the messages were displayed in the correct order and disclosed to the judge the correct timeline of events. He did not. The court finds that the false statements in paragraph 10 were made deliberately with knowledge of their falsity for the clear purpose of misleading the Ohio judge.

Additionally, defendant contends that the reference to an adult male in paragraph 4 is misleading. Paragraph 4 discusses the initial investigation and references Jane Doe having a conversation with an "adult male." Both Ohio affidavits are written in a way which leads the reader to presume that the adult male is "johnsmith." McGinnis knew that the male referenced in paragraph 4 was not "johnsmith." The government disingenuously contends that this is a "negligent inaccuracy" and defendant has not shown that it was intentional or made with a reckless disregard for truth. (Doc. 35 at 6). On the contrary, the court does not believe that this reference to an adult male was negligent or an innocent mistake. The court finds that McGinnis intentionally withheld his knowledge that the adult male in paragraph 4 was not "johnsmith" even though he was seeking a search warrant for John Smith's Yahoo and Apple accounts.

The court finds McGinnis not to be a credible witness. McGinnis repeatedly stated that he did not have the "johnsmith" emails until the warrant was returned but that was not true. McGinnis then "remembered," after several minutes of questioning, that he had been given permission to view Jane Doe's account and retrieve the emails. All in all, McGinnis was the most ill-prepared, unprofessional law enforcement witness this court has encountered.

The findings of false statements in the affidavits does not lead to an automatic suppression of the Yahoo and Apple emails, however. The evidence may be used in the government's case in chief as long as probable cause exists without the inclusion of the false statements in the affidavits. United States v. Karo, 468 U.S. 705, 719 (1984) ("However, if sufficient untainted evidence was presented in the warrant affidavit to establish probable cause, the warrant was nevertheless valid." (citing Franks v. Delaware, 438 U.S. 154, 172 (1978))); United States v. Cusumano, 83 F.3d 1247, 1250 (10th Cir. 1996) ("In our review, we may disregard allegedly tainted material in the affidavit and ask whether sufficient facts remain to establish probable cause.").

2. Probable Cause

Therefore, the question before the court is whether probable cause existed for the issuance of the Yahoo and Apple search warrants even without the statements concerning an adult male and the email conversations. A finding of probable cause is to be determined from the "totality of the circumstances." United States v. Basham, 268 F.3d 1199, 1203 (10th Cir. 2001). "Probable cause to issue a search warrant exists only when the supporting affidavit sets forth facts

that would lead a prudent person to believe there is a fair probability that contraband or evidence of a crime will be found in a particular place." Id.

Defendant contends that there is no evidence of "importuning" after exclusion of the tainted portions of the affidavits. (Doc. 31 at 1-2). The court must only find that there is probable cause that evidence of a crime will be found in the place to be searched. Illinois v. Gates, 462 U.S. 213, 238 (1983). The search warrants identified the sex crimes section of the Ohio Revised Code and, as more particularly described in the affidavits, images of child pornography. Possession of child pornography is a crime in this district and in the states of Ohio and Kansas. The Ohio Revised Code provision criminalizes the viewing and possessing of material depicting children in a state of nudity for other than "proper purposes." Osborne v. Ohio, 495 U.S. 103, 116 (1990). Therefore, because the May 3 Ohio affidavit concerning the email account of "johnsmith" and the August 27, 2012, affidavit concerning the "ebarthelman" email account establish probable cause that the email accounts contained material depicting children in a state of nudity without the excised portions, the search warrants must be upheld. See United States v. Colonna, 360 F.3d 1169, 1175 (10th Cir. 2004)(holding that the search warrant established probable cause of possession of drugs after the tainted portions were excised even though the warrant was initially sought for drug trafficking)(quoting Gates, 462 U.S. at 238 ("[T]he Supreme Court has held that all that is required for a valid search warrant is a 'fair probability that contraband or evidence of a crime will be found in a particular place.' We see no

reason to distinguish between drug use and all other crimes for which a warrant is appropriate."))

3. Particularity

The Fourth Amendment requires not only that warrants be supported by probable cause, but that they "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The particularity requirement "ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." Maryland v. Garrison, 480 U.S. 79, 84, 107 S. Ct. 1013 (1987).

> A description is sufficiently particular when it enables the searcher to reasonably ascertain and identify the things authorized to be seized. Even a warrant that describes the items to be seized in broad or generic terms may be valid when the description is as specific as the circumstances and the nature of the activity under investigation permit. However, the Fourth Amendment requires that the government describe the items to be seized with as much specificity as the government's knowledge and circumstances allow, and warrants are conclusively invalidated by their substantial failure to specify as nearly as possible the distinguishing characteristics of the goods to be seized.

United States v. Leary, 846 F.2d 592, 600 (10th Cir. 1988).

Defendant contends that the warrants are broad because they allow the search of all emails, pictures, friends, and groups. (Doc. 28 at 5). The government responds that the warrants were limited to a specific account, "johnsmith" or "ebarthelman," a specific time frame (six months) and directed towards offenses in Ohio Revised Code 2907.

In Leary, the Tenth Circuit instructed that a "proper warrant must allow the executing officer to distinguish between items that may

and may not be seized." 846 F.2d at 602. "An unadorned reference to a broad federal statute does not sufficiently limit the scope of a search warrant. Absent other limiting factors, such a warrant does not comply with the requirements of the Fourth Amendment." Id. (citing Andresen v. Maryland, 427 U.S. 463, 480–82 (1976)). In this case, the warrant sought all emails, pictures, friends and groups. There was no limitation on these requests to Yahoo and Apple. The only implied limitation to the executing officer is the reference to "any and all evidence of communications used in the furtherance of the violation of laws of the State of Ohio, to wit: Ohio Revised Code Chapter 2907 and any and all other fruits and instrumentalities of crime at the present time unknown." (Exhs. 2A, 4A).

This language, however, does not sufficiently limit the scope of the warrant. Chapter 2907 includes a variety of sex offenses, including rape, battery and prostitution. The government makes no effort to explain how a reference to a general statute concerning numerous crimes satisfies the Fourth Amendment's particularity requirement. See Leary, 846 F.2d at 600 (general reference to violations of the Arms Export Control Act and the Export Administration Act were not sufficiently particular).

The government seems to recognize this defect and attempts to cure it by stating that the affiant conducted the searches and was aware of the parameters. The government, however, fails to provide any authority for the position that a warrant that fails to describe items to be seized with particularity is nevertheless upheld when the affiant is the person conducting the search. Moreover, there is no language in the warrants which would incorporate the affidavits nor

is there any evidence that the affidavits were attached to the warrants.

In summary, although the court finds that the Yahoo and Apple affidavits provide probable cause that evidence of a crime would be found in the contents of the email accounts, the court finds that the warrants were overbroad and not as particular as the Fourth Amendment requires.

The government argues that the court should apply the "good faith" exception to the exclusionary rule. The exception, however, does not apply when the affidavits contained false statements. United States v. Tuter, 240 F.3d 1292, 1299 (10th Cir. 2001). Therefore, the items seized pursuant to the Yahoo and Apple warrants must be suppressed.[4]

B. Kansas Search Warrant

1. False Statements

Jennifer Wright's affidavit to search defendant's residence innocently incorporates the same false statements which were previously discussed, supra. There are no allegations that the Wright affidavit included any additional false statements. The evidence at the hearing was that Wright relied on the information she received from McGinnis and had no knowledge that the statements were false at the time she prepared the affidavit. The fact that the affiant had no knowledge of the falsity of the statements does not, however, mean that the warrant withstands scrutiny. See United States v. Kennedy,

[4] The court notes, however, that if the government obtained the emails through otherwise lawful means, i.e. the Kansas warrant as discussed infra, those emails would be admissible in the government's case in chief.

131 F.3d 1371, 1376 (10th Cir. 1997); see also Franks, 438 U.S. at 164, n. 6 ("police could not insulate one officer's deliberate misstatements merely by relaying it through an officer-affiant personally ignorant of its falsity.")

The findings of false statements in the Ohio affidavit do not lead to an automatic suppression of the items seized at defendant's residence, however. The evidence may be used as long as probable cause exists without the inclusion of the false statements in the affidavits. United States v. Karo, 468 U.S. 705, 719 (1984)

2. Probable Cause

The Wright affidavit specifies the crime allegedly committed by defendant as sexual exploitation of a child in violation of K.S.A. 21-5510. Section 21-5510 criminalizes the conduct of any person who possesses a visual depiction of a child under 18 engaging in sexually explicit conduct with intent to arouse or satisfy the sexual desires or appeal to the prurient interest of the offender.

The Wright affidavit contains far more detail and allegations than the Ohio Yahoo and Apple affidavits. The Wright affidavit explains in excruciating detail the contents of the videos sent by Jane Doe to "johnsmith." Possession of these videos would satisfy the provisions of section 21-5510. Additionally, the affidavit states that the IP address for the subscriber information of "johnsmith" is defendant and the address at which the computer was accessed is 422 Quivira Street in Kechi, Kansas. Several circuits have held that evidence a particular IP address possessed or transmitted child pornography can support a search warrant for the physical premises linked to that IP address. See, e.g., United States v. Vosburgh, 602

F.3d 512, 526-27 (3rd Cir. 2010); United States v. Perez, 484 F.3d 735 (5th Cir. 2007).

Therefore, the court finds that the Wright affidavit, excluding the false statements in the Ohio affidavits, establishes probable cause that evidence of sexual exploitation of a child would be found in defendant's residence.

3. Computer Search

Finally, defendant asserts that the search of the computers at the forensics laboratory violated his Fourth Amendment. Defendant contends that officers were required to obtain a second warrant to search the contents of the computers after seizing the computers from the residence because the warrant "only addressed a house, not a computer." (Doc. 32 at 6).[5]

---

[5] Detective Wright, who is known to the court from prior cases to be a knowledgeable and thoroughly credible officer in these sorts of cases, testified that the practice in Sedgwick County was to obtain a second warrant to search the contents of a computer. She also testified that the AUSA responsible for this case told her a second warrant was not required.

THE COURT: All right. Now, I want to make sure that I understand. Did you, after you had searched the house, collected all the items on the warrant, did you specifically ask your supervisor if you should go back and obtain an additional warrant to search the contents of the computer?

WRIGHT: Specifically we had that discussion because we have in state court in the past went and obtained a second warrant. When it's been placed back at our office to be looked at.

THE COURT: All right. And your supervisor -- I can't remember his name again.

WRIGHT: Sergeant Chuck Pinkston.

THE COURT: Pinkston. He said no.

WRIGHT: Yes.

THE COURT: Then did you have another conversation with Mr. Hart about the same --

WRIGHT: Yes, I did.

THE COURT: And you said should we go back and get a warrant to search the contents?

WRIGHT: Yeah, I believe I had asked if I needed to get another warrant and was told no.

While the language of the search warrant only explicitly stated that the warrant was to search defendant's residence, there is no question that the warrant authorized officers to search for and seize computers, digital files, pictures, and other digital storage media which would contain child pornography. The question before the court is whether officers could search the computers in order to retrieve the items which were listed in the search warrant. In United States v. Grimmett, 439 F.3d 1263 (10th Cir. 2006), the Tenth Circuit was faced with a similar question. The search warrant in Grimmett authorized the officers to search a residence and to seize computers and digital media, as in this case. Additionally, the affidavit in Grimmett discussed how officers retrieved digital items from computers in a laboratory setting and not while at the residence. The Wright affidavit also contained this language. Moreover, as in Grimmett, the

---

THE COURT: And he told you no?
WRIGHT: Yes.
THE COURT: But you've had experience doing that in cases where you seized a computer but you wanted to see the contents?
WRIGHT: Yes, I have.

(Tr. at 149-150).

The court was startled by this revelation and directed AUSA Hart to file a written explanation. He has done so (Doc. 36). The AUSA's "explanation" is that the second warrant policy was required by a now-retired Sedgwick County District Attorney whose practices and customs are not required to be followed by the U.S. Attorney's office. The AUSA further asserts that another Kansas county and the Kansas Attorney General do not have a "second warrant" policy. These responses overlook the fact that the AUSA intended to use the expertise and actions of a Sedgwick County law enforcement officer to bring a case in federal court where her failure to follow Sedgwick County practices and policies conceivably could be used to damage her credibility. The fact that other counties in Kansas may not follow Sedgwick County's practices and policies, as well as the AUSA's prior experiences as a state prosecutor in other counties, is both irrelevant and unimpressive.

Wright search warrant incorporated the affidavit by referring to the "evidence under oath before me." 439 F.3d at 1269. Ultimately, the Tenth Circuit upheld the search of the defendant's computer in Grimmett.

The Grimmett affidavit, however, included an additional statement that the "application is to search any computer media found therein." Id. at 1270. Defendant contends that the failure to include this statement is fatal. The court disagrees. There is no dispute that the search warrant in this case authorized the officers to search the residence for certain items. These items included digital storage media, digital correspondence, digital images, computer software, etc. Those items are contained inside computers. The affidavit explains how the digital items are retrieved from the computers. Therefore, the affidavit clearly contemplated searching the computers after the seizure. Moreover, the last sentence of the warrant stated that the officers were "commanded forthwith to search the persons, place, thing, or means of conveyance herein." (Exh. 8). This sentence would indicate that the items listed in the search warrant would be subject to a search.

In United States v. Simpson, 152 F.3d 1241, 1248 (10th Cir. 1998), the Tenth Circuit also upheld a search of computers seized from a residence pursuant to a search warrant and rejected defendant's argument that a second warrant was required. The search warrant in Simpson authorized a search of the defendant's residence and person and allowed the seizure of computer disks and hard drives, as in this case.

The court finds that a second warrant to search the computers

would have provided additional justification but was not required by the Fourth Amendment under the facts of this case.[6] The search warrant and affidavit provided the officers with authorization to search the computers for the digital media listed in the search warrant. See Grimmett, 439 F.3d at 1269 (citing cases); United States v. Campos, 221 F.3d 1143, 1147 (10th Cir. 2000) (upholding seizure of "computer equipment which may be, or is used to visually depict child pornography"); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (holding that second warrant for search of computer not required, stating that "[a] sufficient chance of finding some needles in the computer haystack was established by the probable-cause showing in the warrant application; and a search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for a weapon or drugs" and upholding seizure of "[a]ny and all computer software and hardware, . . . computer disks, disk drives" in a child pornography case); United States v. Lacy, 119 F.3d 742, 746 (9th Cir. 1997) (warrant permitting "blanket seizure" of computer equipment from defendant's apartment was not insufficiently particular when there was probable cause to believe that computer would contain evidence of child pornography offenses); United States v. Henson, 848 F.2d 1374, 1382–83 (6th Cir. 1988) (permitting seizure of "computer[s], computer terminals, . . . cables, printers, discs, floppy discs, [and] tapes" that could hold evidence of the defendants' odometer tampering scheme).

---

[6] The government should not assume that a second search warrant is never required to search the contents of computers and similar devices. This is an evolving area because of the ever-changing nature of devices used to record, store, process and transmit information.

The evidence obtained in the search was also consistent with the original justification for the search. There is no evidence that the procedure used in this case was improper or that the officers obtained evidence of something other than child pornography. Therefore, the cases cited by defendant are not applicable. See United States v. Riccardi, 405 F.3d 852, 863 (10th Cir. 2005)(the search warrant did not limit the search to a specific crime); United States v. Carey, 172 F.3d 1268, 1272 (10th Cir. 1999)(same).[7]

Defendant's motion to suppress the Kansas warrant is accordingly denied.

III. Conclusion

Defendant's motion to suppress is granted in part and denied in part. Defendant's motion to suppress the Yahoo and Apple warrants is granted. Defendant's motion to suppress the Kansas warrant is denied.

IT IS SO ORDERED.

Dated this 31st day of July 2013, at Wichita, Kansas.

s/ Monti Belot
Monti L. Belot
UNITED STATES DISTRICT JUDGE

[7] Defendant also offered United States v. Christie, 2013 WL 2477252, for the proposition that a warrant should have been obtained to search the computers. Christie, however, is distinguishable. The issues in Christie were whether a delay in the seizure of the computer and the warrant was unreasonable and a claim that the warrant did not list the items to be seized with particularity.