

**IN THE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF OKLAHOMA**

IN RE:)	
)	
SEARCH WARRANT(S))	Case No. M-17-192-SM
EXECUTED ON PREMISES KNOWN AS:)	
)	
Facebook and Facebook Messenger)	
Account of: User ID: brian.tilley.714)	
Screen name: Brian Tilley)	
Stored at the Premises of:)	
Facebook, Inc.)	
1601 California Avenue)	
Palo Alto, CA 94304)	

APPLICATION TO UNSEAL

COMES NOW the plaintiff, United States of America, by Mark A. Yancey, United States Attorney for the Western District of Oklahoma, K. McKenzie Anderson and Brandon Hale, Assistant United States Attorneys, and moves the Court to unseal the above-captioned affidavit and search warrant, which was ordered sealed by this Court on May 1, 2017. The United States is attaching a redacted version of the affidavit to be unsealed. (Attachment).

In support of this application, the government would show the Court that there is no longer any necessity for the search warrant to remain sealed, except as redacted.

WHEREFORE, the United States prays this Court to enter an Order unsealing the search warrant and the redacted version of the affidavit for Magistrate's Docket No. M-17-192-SM, in order that these matters may be filed as a part of the public record.

Respectfully submitted,

MARK A. YANCEY
United States Attorney

s/Brandon Hale

Assistant U.S. Attorney
Bar Number: 19819
210 Park Avenue, Suite 400
Oklahoma City, Oklahoma 73102
(405) 553- 8700(Office)
(405) 553-8888 (Fax)
Brandon.Hale@usdoj.gov

s/ K. McKenzie Anderson

Assistant U.S. Attorney
OBA# 30471
210 Park Avenue, Suite 400
Oklahoma City, Oklahoma 73102
(405) 553-8781 (Office)
(405) 553-8888 (Fax)
McKenzie.Anderson@usdoj.gov

UNITED STATES DISTRICT COURT

for the
WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search and Seizure of)
)
Content of, and records relating to)
Facebook and Facebook Messenger account of:)

User ID: brian.tilley.714)

Screen name: Brian Tilley)

Stored at the Premises of:)

Facebook, Inc.)

Attn: Security Department/Custodian of)
Records)

1601 California Avenue)

Palo Alto, CA 94304)

Case No: M-17- **192-SM**

FILED

MAY - 1 2017

CARMELITA REEDER SHINN, CLERK
U.S. DIST. COURT, WESTERN DIST. OKLA.
BY [Signature], DEPUTY

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property (*identify the person or describe property to be searched and give its location*):

See Attachment A, which is attached and incorporated by reference.

There is now concealed (*identify the person or describe the property to be seized*):

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is(*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. § 1591 (a)(1), b(2) and (c)

Child Sex Trafficking

18 U.S.C. § 2252A(a)(5)(B) and b(2)

Possession of Child Pornography

18 U.S.C. § 2252

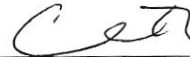
Distribution of Child Pornography

The application is based on these facts:

See attached Affidavit of Special Agent Charles Thumann, Federal Bureau of Investigation, which is incorporated by reference herein.

☒ Continued on the attached sheet(s).

☐ Delayed notice of _____ days (give exact ending date if more than 30 days) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).



Applicant's signature

CHARLES THUMANN

Special Agent

Federal Bureau of Investigation

Sworn to before me and signed in my presence.

Date: May 1, 2017



Judge's signature

City and State: Oklahoma City, Oklahoma

SUZANNE MITCHELL, U.S. Magistrate Judge

Printed name and title

**THE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF OKLAHOMA**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Charles W. Thumann, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent with the FBI since July 2004. I am currently assigned to the Norman Resident Agency, Oklahoma City Division. I have received training in the area of child pornography and child exploitation, and have experience in investigating the sexual exploitation of children.

2. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States. I also have participated in the execution of multiple federal search warrants, many of which have involved child exploitation and/or child pornography offenses.

3. I make this affidavit in support of an application for a search warrant for information associated with a certain Facebook user ID that is stored at premises owned, maintained, controlled, or operated by Facebook Inc. ("Facebook"), a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts referenced in this affidavit and further in Attachment A, including the contents of the communications.

4. I have probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of 18 U.S.C. § 1591 (sex trafficking of children), 18 U.S.C.

§ 2252 (distribution of child pornography), and 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography) are stored at premises owned, maintained, controlled, or operated by Facebook headquartered in Menlo Park, California. The information and accounts to be searched are described in the following paragraphs and in Attachments A and B.

5. The statements contained in this affidavit are based in part on information provided by FBI Special Agents and Moore Police Department Officers, written reports about this and other investigations that I have received—directly or indirectly—from other law enforcement agents, the results of surveillance conducted by law enforcement agents, and my experience, training and background as a Special Agent (SA) with the FBI. Because this affidavit is being submitted for the limited purpose of securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish probable cause for the requested warrant.

6. This investigation, described more fully below, has revealed that there is probable cause to believe that the Facebook account associated with user ID “brian.tilley.714”, violated the federal statutes referenced in paragraph 3 above and that there is probable cause to believe that evidence, fruits, and instrumentalities of such violations are located in this Facebook account.

STATUTORY AUTHORITY

This investigation concerns alleged violations of Title 18, United States Code, Sections 1591, 2252, and 2252A relating to material involving the sexual exploitation of minors:

7. 18 U.S.C. § 1591 prohibits a person from recruiting, enticing, harboring, transporting, providing, maintaining, advertising, patronizing, soliciting, or obtaining a minor, by any means, in and affecting interstate commerce, when that person has a reasonable opportunity to observe the minor and knows or recklessly disregards the fact that the person will be caused to engage in a

commercial sex act.

8. 18 U.S.C. § 2252 prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce.

9. 18 U.S.C. § 2252A prohibits a person from knowingly mailing, transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child pornography, as defined in 18 U.S.C. § 2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

DEFINITIONS

10. A “sexual act” under 18 U.S.C. § 2246 includes the penetration, however slight, of the genital opening of another by a hand or finger with an intent to abuse, humiliate, harass, degrade, or arouse or gratify the sexual desire of any person. A “sexual act” also includes the intentional touching, not through the clothing, of the genitalia of another person who has not attained the age of 16 years with the intent to abuse, humiliate, harass, degrade, or arouse or gratify the sexual desire of any person.

11. The term “minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

12. The term “sexually explicit conduct,” 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.

13. The term “visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film

and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

14. The term “computer,” as defined in 18 U.S.C. §1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

15. The term “child pornography,” as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where

- a. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
- b. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
- c. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct

16. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

17. “Internet Service Providers” (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

18. “Internet Protocol address” (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet.

19. “Domain names” are common, easy to remember names associated with an IP address. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

20. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND EMAIL

I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:

21. Computers and computer technology have revolutionized the way in which child pornography and other depictions of children being sexually abused is produced, distributed, stored, and utilized. It has also revolutionized the way in which such collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs

involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

22. The development of computers has added to the methods used by collectors of child abuse images to interact with and sexually exploit children. Computers serve four functions in connection with child pornography/child abuse images. These are production, communication, distribution, and storage.

23. Child pornographers can now transfer photographs from a camera onto a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography and other depictions of child sexual abuse can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem.¹ Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

24. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography and other depictions of child sexual abuse. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has

¹ The File Transfer Protocol (FTP) is a protocol that defines how to transfer files from one computer to another. One example, known as "anonymous FTP," allows users who do not have a login name or password to access certain files from another computer, and copy those files to their own computer.

grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

25. The Internet and its World Wide Web afford collectors of child pornography/depictions of children being sexually abused several different venues for obtaining, viewing, and trading such images in a relatively secure and anonymous fashion.

26. Collectors and distributors of child pornography or other visual depictions of children being sexually abused also use online resources to retrieve and store such images, including services offered by Internet Portals such as Yahoo!, Google, Inc., and AOL.com among others. The online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet.

27. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others).

TECHNICAL INFORMATION REGARDING FACEBOOK

28. In my training and experience, I have learned that Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

29. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the

user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

30. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

31. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

32. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social

occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

33. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

34. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

35. If a Facebook user does not want to interact with another user on Facebook, the first user can “block” the second user from seeing his or her account.

36. Facebook has a “like” feature that allows users to give positive feedback or connect to particular pages. Facebook users can “like” Facebook posts or updates, as well as webpages or content on third-party (*i.e.*, non-Facebook) websites. Facebook users can also become “fans” of particular Facebook pages.

37. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

38. Each Facebook account has an activity log, which is a list of the user’s posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as “liking” a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user’s Facebook page.

39. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs (“blogs”), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

40. The Facebook Gifts feature allows users to send virtual “gifts” to their friends that appear as icons on the recipient’s profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other “pokes,” which are free and simply result in a notification to the recipient that he or she has been “poked” by the sender.

41. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

42. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications (“apps”) on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

43. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications.

44. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

45. Social networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical

problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

46. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's "Neoprint," IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to

either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

47. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

CHARACTERISTICS OF CHILD PORNOGRAPHERS

Based upon my training and experience, as well as upon information provided to me by other law enforcement officers, I am aware of the following general characteristics of people involved with child pornography, which may be exhibited in varying combinations:

48. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses (such as in person, in photographs, or other visual media), or from literature describing such activity.

49. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

50. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer, social networking account, and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or at the click of a computer mouse, to enable the individual to view the collection, which is valued highly.

51. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

52. Individuals whose sexual interest in children or images of children has led them to purchase access to paid websites or other commercial sources of child pornography frequently maintain the financial records of those transactions at their residences or within their social networking accounts.

53. I know from personal experience or speaking to other law enforcement agents that child pornography collectors often store their collections in a personal email account or in cloud storage associated with an email account so that their collections are accessible wherever they go and from a multitude of devices. All that is required is a computer or smart phone and an Internet connection. Further, a child pornography collector may think that, because child pornography stored on a social networking account is not saved directly to his device, he is not technically "possessing" it. Based on the information described below, I believe that Ralph Shortey is a child pornography collector.

BACKGROUND OF INVESTIGATION

The facts establishing probable cause to support the issuance of a search warrant are as

follows:

54. On March 9, 2017, Moore Police officers identified Ralph Allan Shortey in hotel room 120 at the Super 8 Hotel located at 1520 N. Service, Moore, Oklahoma. Shortey was present inside the room alone with a 17-year-old male juvenile, hereafter referred to as [REDACTED]. During the investigation inside the hotel room, officers learned of a conversation on a smartphone and tablet between Shortey and [REDACTED] using messaging application "Kik". The conversation took place between [REDACTED] and an account with Shortey's online pseudonym "Jamie Tilley" with the Kik ID of "Brinokc4u". [REDACTED] advised officers that "Jamie Tilley" was Shortey. Shortey also told officers he used the profile name "Jamie". Shortey also told officers he used messaging apps to communicate with [REDACTED]. When [REDACTED] was interviewed on March 9, 2017, he said Shortey's user name was "Brian Tilley."

55. During their conversation on Kik, [REDACTED] told Shortey "I need money for spring break." Shortey replied, "I don't really have any legitimate things I need help with right now. Would you be interested in "sexual" stuff?" [REDACTED] responded "Yes." The conversation continued with both discussing logistics of how and where [REDACTED] and Shortey were going to meet. [REDACTED] told Shortey "Hey keep updated cause I want you bad daddy." Shortey responded, "I'm gonna fuck you like a good little boy if you keep calling me daddy." The message included a smiley face emoji after "boy." [REDACTED] made the statement, "I want your vim all in .my man pussy." [REDACTED] corrected himself and stated, "Cum." Shortey stated, "Boy pussy, baby boy." The message included a smiley face emoji after "boy."

56. On March 9, 2017, at approximately 0005 hours, Shortey sent a message to [REDACTED], "K, I'll be down the street a couple houses in about 10 minutes or so." At approximately 0006 hours, Shortey stated, "I35 about to exit 4th." At approximately 0013 hours, Shortey sent another

message to ■■■ "I'm here." Shortly after that message, a witness observed ■■■ enter a white Jeep Cherokee driven by an unknown male. The witness followed the Cherokee to the Circle K at S.E. 4th and Eastern, then to the Super 8 Hotel where both ■■■ and the unknown adult male entered the hotel to rent a room. The witness then observed ■■■ and the unknown adult male enter room 120 of the Super 8 Hotel.

57. The unknown male that entered room 120 of the Super 8 Hotel was later identified by officers as Shortey. The white Jeep Cherokee that he drove to the hotel was registered through the State of Oklahoma to Shortey. Room 120 was reserved by Ralph Allan Shortey using a credit card in his name and the business name Precision Strategy Group.

58. Inside the hotel room, officers found an opened box of condoms, a laptop, and a bottle of hydrocodone in Shortey's backpack, and a bottle of lotion in the backpack of ■■■. Officers observed that both beds had been unmade and there were four wet stains on one of the beds. During his interview with police, ■■■ advised that "Jamie Tilley" was Shortey, and the Kik user name "Brinokc4u" was also Shortey. ■■■ advised he brought approximately 1 gram of marijuana to the hotel, and Shortey brought approximately 1 gram of marijuana to the hotel. ■■■ said he and Shortey were smoking marijuana when officers knocked on the door. ■■■ confirmed that he and Shortey intended to have sexual contact and that they had agreed Shortey would pay him for that contact.

59. ■■■ and Shortey both stated they had known each other for approximately one year. ■■■ advised that he originally met Shortey through a Craigslist personal encounter ad. ■■■ advised that before May 2016, he and Shortey had exchanged photos of their penises. ■■■ advised that Shortey was aware early in their contact that he was 16 years old at the time. ■■■ also advised that they had smoked weed at Shortey's coffee shop, Wholly Grounds, on the second floor, two or

three times.

60. [REDACTED] provided his tablet to Moore Police Department officers. The tablet contained the conversation between [REDACTED] and Shortey, using the pseudonym Jamie Tilley, on the Kik application.

61. On March 13, 2017, Moore Police Department officers conducted a voluntary interview with Ralph Allan Shortey after contacting him on his cell phone and asking him to come to the station. During the interview, Moore Police officers asked Shortey if they could take possession of his cell phone. Shortey explained that he had placed his cell phone on top of his vehicle when he came to the Moore Police Department and lost it. In addition, Shortey stated he did not use Kik and did not know why [REDACTED] referred to him as Jamie. Shortey declined to allow Moore Police officers to search his vehicle for his cell phone.

62. On March 13, 2013, a Moore Police detective entered the cell phone number 405-219-9346 into the search field of Facebook's homepage. This was the same cell phone number Shortey provided to Moore Police on March 9, 2017, at the Super 8 motel. Facebook returned account "brian.tilley.714". This Facebook page is currently unavailable.

63. On March 16, 2017, the FBI sent a preservation request to Facebook for the username brian.tilley.714. Facebook confirmed receipt of the preservation request.

64. On March 20, 2017, Homeland Security Investigations (HSI) found the Kik username "brinokc4u" was registered with Kik on July 24, 2012. The account was registered under the name Jamie Tilley.

65. On March 21, 2017, I reviewed the body cam video of a Moore Police officer who spoke with Shortey at the Super 8 motel on March 9, 2017. Shortey told the officer that he had known [REDACTED] for approximately one year and messaged him through an app. Shortey also told the officer that he communicated with [REDACTED] using his profile name "Jamie".

66. On March 21, 2017, Moore Police provided the FBI with two Craigslist postings, 5935310341 and 5864483134, which identified the poster as someone who used the Kik profile “brinokc4u”. Both ads were similarly titled “Need a boy or bromance – m4m” and contained similar descriptive information on what brinokc4u was seeking, but had some slight differences. Both ads stated “Looking for younger the better (legal) white or mixed”. “Easiest way to communicate is with kik. Brinokc4u is my kik name”. Both ads also offered that anyone interested could email the poster (Shortey) at the randomized email address provided by Craigslist. I know based on my experience that the anonymized email address will simply forward the email to the account holder’s email address on file with Craigslist.

67. Craigslist ad 5935310341 was posted on December 27, 2016. The ad stated, “Brinokc4u is my kik name or you can text me at 4 oh 5, two five 6, eight zero 2 one.” (405-256-8021) On April 12, 2017, I confirmed through electronic telephone number services (eTNS) the phone number 405-256-8021 was provided by Google Voice.

68. On March 28, 2017, Moore Police provided the FBI with additional Craigslist ads obtained pursuant to the search warrant issued by the District Court of Cleveland County, Oklahoma. These ads are very similar to what is described above—Shortey was attempting to solicit young males for sexual contact. Several of the ads were posted during the six-month period when [REDACTED] was in a rehabilitation facility. One of those ads said Shortey was looking for 5-10 men under the age of 40 and that he was “offering this young tight twink” for a “straight or bi gang bang.” The post explains that the person he was offering “is 21 (looks 18)” and has “an amazing boy pussy.” He described the “boy” to be small and fit, “an amazing cock sucker and even better at getting fucked,” and explained that he was “trying to get 5-10, he can last and everyone will have their turn (or multiple turns). . . . My kik name is brinokc4u.” Law enforcement has not identified that

person.

69. Craigslist provided Moore Police with subscriber information. The registered email account was brinokc4u@aol.com and phone number 405-219-9346.

70. On March 23, 2017, AT&T provided subscriber information for phone number 405-219-9346 to Moore Police as well as the phone's International Mobile Equipment Identifier (IMEI) 3550720605134034. AT&T identified Jennifer H. Shortey as the financially liable party, billing party, and user information for 405-219-9346. Jennifer H. Shortey is the wife of Ralph Shortey. From March 7, 2017, through March 13, 2017, the IMEI number listed a Samsung SM-N915A model phone on the AT&T account. The AT&T records further showed the IMEI number changed from 3550720605134034 to 3574170773706804 on March 14, 2017, indicating a different phone was used for phone number 405-219-9346 after March 14, 2017.

71. A search of Samsung's website for phone model SM-N915A identified the model as a Samsung Galaxy Note Edge phone that operates on the Android mobile operating system. Typically, in order for a user to access and use an Android based phone, the user is required to have a valid Google email address.

72. On March 28, 2017, FBI interviewed Samantha Flores from the AT&T store located at 1413 W. Interstate 240 Service Road, Oklahoma City, Oklahoma. On March 13, 2017 (the same day Shortey was interviewed by Moore Police), Flores assisted Ralph Shortey with changing SIM cards from his old phone to his new phone. Shortey changed SIM cards on a Samsung phone with phone number 405-219-9346.

73. On March 31, 2017, the FBI and Moore Police interviewed Ralph Shortey's former executive assistant at the Oklahoma Senate. William Claybrook stated he had worked for Shortey from September 2013 through March 2017. Claybrook confirmed Shortey used cell phone

number 405-219-9346 in the time period he knew and worked for Shortey.

74. On April 14, 2017, AOL provided a DVD that contained emails and subscriber information for AOL email account brinokc4u@aol.com pursuant to a federal search warrant issued on April 4, 2017. The account was registered under the name Brian Tilley and listed an additional email address of brinokc4u@gmail.com. The AOL account included an email confirmation from June 2012 for the creation of a Facebook account under the pseudonym "Brian Tilley," with user ID "brian.tilley.714". The investigation has also revealed that Shortey had two other Facebook accounts: one for Shortey's real name, with the account under the name "Ralph SHortey" (sic), located at <https://www.facebook.com/rshortey>, and another for Shortey's role as an Oklahoma State Senator (since removed). The AOL account contained emails from a Gmail account linked to Shortey that included photographs of Shortey and his wife. Shortey then attached the photos of himself and his wife to emails sent to various individuals in connection with arranging sexual encounters.

75. A review of Shortey's AOL email address account contained two emails that had been sent in October 2013 from his AOL account, brinokc4u@aol.com to Chubbybuddy6@hotmail.com and usmclpu87@yahoo.com. The first email from Shortey's AOL account to Chubbybuddy6@hotmail.com contained a video of a prepubescent female who was penetrated vaginally by a Sharpie marker and then later penetrated vaginally and anally with an adult's penis. The second email was sent to usmclpu87@yahoo.com and it contained four video attachments of young, prepubescent boys engaged in various sexual activities, including oral sex, masturbation, and anal intercourse. That second email contained the subject line "kik", suggesting that the recipient was a contact from the Kik messaging app. The first email, to Chubbybuddy6@hotmail.com, does not contain any text to explain how the users were otherwise

in contact. In my experience, individuals frequently connect to each other through various mediums, including text messages, different messaging applications, message boards, and different social media networks. The inbox of the AOL account included hundreds of pornography emails and communications with individuals encountered via Craigslist, as well as emails referring to Kik communications and attaching pornographic videos. The AOL account included communications with male individuals who have been identified as 16 and 17 years old at the time, in 2012, in which Shortey sent them commercial pornography and received, in exchange, videos of the boys masturbating. One of those boys, who was 17 at the time, sent six such videos, including three videos in which he inserted a zucchini into his rectum.

76. The investigation has shown that Shortey used both pseudonyms Brian Tilley and Jamie Tilley. The Tilley pseudonyms were connected to Shortey's Craigslist account, his email accounts at AOL and Gmail, and his Kik account. Based on a review of the AOL email account and the postings on Craigslist, Shortey used those pseudonyms almost exclusively for illicit and illegal sexual interests or encounters, several of which included communications and exchanges of pornography with underage males, and/or the sharing of child pornography. The AOL email account contains hundreds of emails addressed to "Brian." The AOL account also included hundreds of emails related to Shortey's Facebook account for "Brian Tilley."

77. Based on my training, experience, and facts of this investigation, I believe probable cause exists that the fruits, instrumentalities, and evidence of the above-stated crimes will be found in the Facebook account associated with user ID "brian.tilley.714". Accordingly, I submit that there is probable cause to search the account.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

78. I anticipate executing this warrant under the Electronic Communications Privacy Act, in


particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

79. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the computer systems in control of Facebook there exists evidence of a crime, contraband and/or fruits of a crime. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that the Facebook account described in Attachment A contain the fruits, instrumentalities, and evidence of crimes described in Attachment B, specifically, that the accounts were used to solicit children for commercial sex and/or to receive, distribute, possess, and/or access child pornography or other depictions of children being sexually abused. Accordingly, a search warrant is requested.

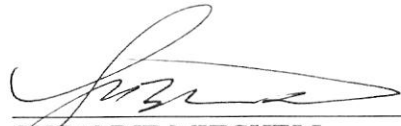
80. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711(3) and 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(I).

81. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.



 Charles W. Thumann
 Special Agent
 Federal Bureau of Investigation

SUBSCRIBED AND SWORN to before me this 5th day of May, 2017.

A handwritten signature in black ink, appearing to read 'Suzanne Mitchell', is written over a horizontal line.

SUZANNE MITCHELL
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF ITEMS TO BE SEARCHED

This warrant applies to the Facebook account associated with user ID “brian.tilley.714”, which is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a company headquartered in Menlo Park, California.

ATTACHMENT B

LIST OF ITEMS AND INFORMATION TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely, violation of 18 U.S.C. § 1591, 18 U.S.C. § 2252, and 18 U.S.C. § 2252A(a)(5)(B) and (b)(2):

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook Inc. (“Facebook”), including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment A:

- (a) All contact and personal identifying information, including: full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All activity logs for the account and all other documents showing the user’s posts and other Facebook activities;
- (c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them, as well as any photos and videos sent or received by that user ID on Facebook or Facebook Messenger;

- (d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;
- (e) All other records of communications and messages made or received by the user, including all private messages, Facebook Messenger content, chat history, video calling history, and pending "Friend" requests;
- (f) All "check ins" and other location information;
- (g) All IP logs, including all records of the IP addresses that logged into the account;
- (h) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";
- (i) All information about the Facebook pages that the account is or was a "fan" of;
- (j) All past and present lists of friends created by the account;
- (k) All records of Facebook searches performed by the account;
- (l) All information about the user's access and use of Facebook Marketplace;
- (m) The types of service utilized by the user;
- (n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

- (o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
- (p) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

1. All information described above in Section I, including correspondence, records, documents, photographs, videos, electronic mail, chat logs, and electronic messages that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2252, 2252A, and 1591 including, for each account or identifier listed on Attachment A, the following matters, and information pertaining to the following matters:

- i. Evidence of the trafficking of children, selling or buying of children, and production, transportation, or possession of child pornography.
- ii. Evidence of preparatory steps taken in furtherance of the scheme, such as the possession or conspiracy to possess controlled substances.
- iii. Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;
- iv. Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;
- v. The identity of the person(s) who created or used the user IDs, including records that help reveal the whereabouts of such person(s).

- vi. The identity of the person(s) who communicated with the user IDs about matters relating to crimes listed under section II, including records that help reveal their whereabouts.
- 2. Passwords and encryption keys, and other access information that may be necessary to access the accounts or identifiers listed on Attachment A and other associated accounts.