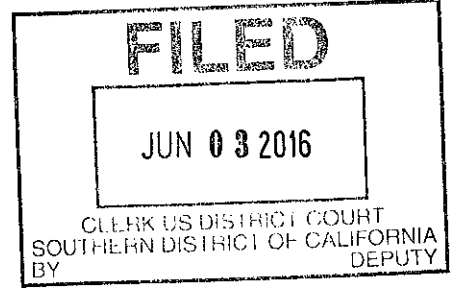


UNITED STATES DISTRICT COURT

for the Southern District of California



In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))
Facebook Inc., at 1601 Willow Road, Menlo Park, CA)
94025)
Facebook.com/profile.php?id=10002025941957,)
Facebook.com/profile.php?id=100011439746688,)
Facebook.com/profile.php?id=100011638875220)

Case No.

'16MJ1596

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Northern District of California (identify the person or describe property to be searched and give its location): see Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized): see Attachment B

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

- [x] evidence of a crime;
[x] contraband, fruits of crime, or other items illegally possessed;
[x] 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 18 U.S.C. § 2250 & 2252, and the application is based on these facts: See attached affidavit

[x] Continued on the attached sheet.

[] 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.

Signature of Chad N. Worgen

Special Agent Chad N. Worgen, HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: 6/3/16

Signature of Mitchell D. Dembin

Judge's signature

City and state: San Diego, CA

Honorable Mitchell D. Dembin, U.S. Magistrate Judge
Printed name and title

ALGER

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Chad Worgen, being first duly sworn, hereby depose and state as follows:

1. I am a Special Agent (SA) with Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) within the Department of Homeland Security (DHS), having been so employed since February 2007. I am currently assigned to the HSI Special Agent in Charge (SAC) San Diego, CA Cyber Crimes group. I have attended and successfully completed the Criminal Investigator Training Program (CITP) and the Immigration and Customs Enforcement Special Agent Training (ICESAT) located at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. I am currently assigned to the Internet Crimes Against Children (ICAC) Task Force in San Diego. This task force includes members of the San Diego Police Department, San Diego County Sheriff's Department, U.S. Postal Inspection Service, Federal Bureau of Investigations, Naval Criminal Investigative Service, U.S. Attorney's Office and the San Diego County District Attorney's Office. Prior to becoming a SA, I was employed as a United States Customs and Border Protection (CBP) Officer at the San Ysidro, CA and Otay Mesa, CA Ports of Entry for approximately four (4) years. I have previously received training from the FLETC and other law enforcement agencies in the area of child pornography investigations. As an HSI SA assigned to the Cyber Crimes group, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251 and 2252. I have participated in the service of numerous search warrants involving child exploitation and/or child pornography offenses and have had the opportunity to observe and review numerous examples

1 of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media.
2 As a federal agent, I am authorized to investigate violations of laws of the United
3 States and I am a law enforcement officer with the authority to execute warrants
4 issued under the authority of the United States. In preparation of this affidavit, I
5 have discussed the facts of this case with other law enforcement agent and officers
6 within HSI and ICAC task force.

7 2. This affidavit is made in support of an application for a warrant to
8 search for and seize evidence related to potential violations of 18 U.S.C. §§ 2250
9 and 2252, at the location described in Attachments A, for evidence described in
10 Attachment B.

11 3. This affidavit is based upon information I have gained through
12 training and experience, as well as upon information relayed to me by other
13 individuals, including law enforcement officers. Since this affidavit is being
14 submitted for the limited purpose of securing a search warrant, I have not included
15 each and every fact known concerning this investigation but have set forth only the
16 facts that I believe are necessary to establish probable cause to believe that
17 evidence relating to potential violations of 18 U.S.C. §§ 2250 and 2252, described
18 in Attachment B, are in the location described in Attachment A.

19 4. Based upon the following information, I believe there is probable
20 cause to believe that currently at the location described in Attachment A, there is
21 evidence, fruits and instrumentalities of receipt, distribution, and/or possession of
22 evidence, fruits and instrumentalities of receipt, distribution, and/or possession of
23 visual depictions, and other related materials, involving minors engaging in
24 sexually explicit conduct (child pornography), in violation of 18 U.S.C. § 2252,
25 more particularly described in Attachment B. I also believe there is evidence and
26 instrumentalities regarding the location and claimed residence of the user of the
27
28
29

1 accounts identified in Attachment A which would establish a violation of 18
2 U.S.C. § 2250.

3 **BACKGROUND INFORMATION ON FACEBOOK & NCMEC**

4 5. Facebook is a corporation that owns and provides a free-access online
5 social networking service and is headquartered in Menlo Park, California.
6 Facebook allows its users to establish accounts with Facebook, and users can then
7 use their accounts to share written news, photographs, videos, and other
8 information with other Facebook users, and sometimes with the general public.

9 6. Facebook asks users to provide basic contact and personal identifying
10 information to Facebook, either during the registration process or thereafter. This
11 information may include the user's full name, birth date, gender, contact e-mail
12 addresses, Facebook passwords, Facebook security questions and answers (for
13 password retrieval), physical address (including city, state, and zip code),
14 telephone numbers, screen names, websites, and other personal identifiers.
15 Facebook also assigns a user identification number to each account.
16

17 7. Facebook users may join one or more groups or networks to connect
18 and interact with other users who are members of the same group or network.
19 Facebook assigns a group identification number to each group. A Facebook user
20 can also connect directly with individual Facebook users by sending each user a
21 "Friend Request." If the recipient of a "Friend Request" accepts the request, then
22 the two users will become "Friends" for purposes of Facebook and can exchange
23 communications or view information about each other. Each Facebook user's
24 account includes a list of that user's "Friends" and a "News Feed," which
25 highlights information about the user's "Friends," such as profile changes,
26 upcoming events, and birthdays.
27
28
29

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

10 9. Facebook users can create profiles that include photographs, lists of
11 personal interests, and other information. Facebook users can also post “status”
12 updates about their whereabouts and actions, as well as links to videos,
13 photographs, articles, and other items available elsewhere on the Internet.
14 Facebook users can also post information about upcoming “events,” such as social
15 occasions, by listing the event’s time, location, host, and guest list. In addition,
16 Facebook users can “check in” to particular locations or add their geographic
17 locations to their Facebook posts, thereby revealing their geographic locations at
18 particular dates and times. A particular user’s profile page also includes a “Wall,”
19 which is a space where the user and his or her “Friends” can post messages,
20 attachments, and links that will typically be visible to anyone who can view the
21 user’s profile.

22 10. Facebook allows users to upload photos and videos, which may
23 include any metadata such as location that the user transmitted when s/he uploaded
24 the photo or video. It also provides users the ability to “tag” (i.e., label) other
25 Facebook users in a photo or video. When a user is tagged in a photo or video, he
26 or she receives a notification of the tag and a link to see the photo or video. For
27
28
29

1 Facebook's purposes, the photos and videos associated with a user's account will
2 include all photos and videos uploaded by that user that have not been deleted, as
3 well as all photos and videos uploaded by any user that have that user tagged in
4 them.

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

15
16 12. If a Facebook user does not want to interact with another user on
17 Facebook, the first user can "block" the second user from seeing his or her
18 account.

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

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

25 15. Each Facebook account has an activity log, which is a list of the user's
26 posts and other Facebook activities from the inception of the account to the
27 present. The activity log includes stories and photos that the user has been tagged
28

1 in, as well as connections made through the account, such as “liking” a Facebook
2 page or adding someone as a friend. The activity log is visible to the user but
3 cannot be viewed by people who visit the user’s Facebook page.

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

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

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

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

20 20. Facebook uses the term “Neoprint” to describe an expanded view of a
21 given user profile. The “Neoprint” for a given user can include the following
22 information from the user’s profile: profile contact information; News Feed
23 information; status updates; links to videos, photographs, articles, and other items;
24 Notes; Wall postings; friend lists, including the friends’ Facebook user
25 identification numbers; groups and networks of which the user is a member,
26 including the groups’ Facebook group identification numbers; future and past
27
28
29

1 event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and
2 information about the user's access and use of Facebook applications.

3 21. Facebook also retains Internet Protocol ("IP") logs for a given user ID
4 or IP address. These logs may contain information about the actions taken by the
5 user ID or IP address on Facebook, including information about the type of action,
6 the date and time of the action, and the user ID and IP address associated with the
7 action. For example, if a user views a Facebook profile, that user's IP log would
8 reflect the fact that the user viewed the profile, and would show when and from
9 what IP address the user did so.

10 22. Social networking providers like Facebook typically retain additional
11 information about their users' accounts, such as information about the length of
12 service (including start date), the types of service utilized, and the means and
13 source of any payments associated with the service (including any credit card or
14 bank account number). In some cases, Facebook users may communicate directly
15 with Facebook about issues relating to their accounts, such as technical problems,
16 billing inquiries, or complaints from other users. Social networking providers like
17 Facebook typically retain records about such communications, including records of
18 contacts between the user and the provider's support services, as well as records of
19 any actions taken by the provider or user as a result of the communications.
20

21 23. Facebook reports any instance of child sexual exploitation that it
22 discovers in its user accounts to the National Center for Missing and Exploited
23 Children (NCMEC). The report that Facebook files with NCMEC includes the
24 screen/user name, email address of the user who posted the images, as well as
25 associated URL and/or IP address at the time that content was uploaded to a
26 Facebook account. This report is called a CyberTipline Report and it is assigned a
27 CyberTipline Report number, which Facebook uses to reference the incident.
28
29

1 24. NCMEC analysts are trained to analyze the information that is
2 reported to them by Facebook. The analysts can identify the ISP from the IP
3 number. The geographical location in which a person's computer connects to the
4 ISP's network is called the Point of Presence (hereafter referred to as PoP).
5 Generally, IP numbers are mapped to PoP's or a geographic area. By analyzing
6 the IP, analysts can often determine the geographical location of the PoP that was
7 accessed at the time the user was online with Facebook and sent the offending
8 content.

9 25. The Federal Government's Office of Juvenile Justice and Delinquency
10 Prevention (OJJDP) provides grants throughout the country to local law
11 enforcement agencies to fund task forces, aimed at combating child sexual
12 exploitation on the Internet. These task forces are referred to as an "ICAC," short
13 for Internet Crimes Against Children. ICAC task forces act as liaisons between
14 NCMEC and other local law enforcement agencies.

15 26. When a NCMEC analyst determines the probable geographical
16 location of a PoP, he or she will route the CyberTipline Report information
17 provided to it by Facebook to the ICAC nearest to the PoP. The San Diego Police
18 Department operates the San Diego ICAC.
19

20 PEER-TO-PEER FILE SHARING

21 27. The Gnutella and the Ares networks are peer-to-peer (P2P) file
22 sharing networks on the Internet. In order to participate in these networks, users
23 must have a software program installed on their computer that allows them to trade
24 electronic files with other users over the Internet.

25 28. A user on the Gnutella and the Ares network may locate desired
26 images or movies by entering a search term. Upon entering the search term, the
27 user receives search results. The search results show files associated with that
28

1 search term and that are publically available for downloading from other users on
2 this network.

3 29. In addition, some software programs on P2P file sharing networks
4 allow a user to view not only the file names publically available for downloading
5 but also what is known as a hash value associated with those file names. The hash
6 value is an identifier of letters and numbers based on a mathematical algorithm. It
7 is essentially a digital signature of a file. If two separate files contain different file
8 names but an identical digital signature, then there is a high degree of probability
9 that the two files contain the same content.

10 30. The Gnutella and the Ares network use these digital signatures to
11 improve network efficiency. These networks allow a user (the recipient user) to
12 select a file (the selected file) to download from another user (the distributing
13 user). In order to improve efficiency, the network may assemble the selected file
14 from different users. The network does so by identifying other publically available
15 files with the same digital signature from other distributing users. By using the
16 digital signature to reassemble the selected file, the network ensures that the
17 recipient user downloads an exact copy of the selected file made publically
18 available by the original distributing user. Depending on how the recipient user
19 sets the software program, the recipient user then may publically advertise the
20 selected file for downloading by other users on the network.

21 31. Law enforcement personnel familiar with child exploitation cases
22 view the Gnutella and the Ares network as a known trading ground for child
23 pornography files. For example, a user who is interested in trading in child
24 pornography files need only enter terms associated with child exploitation cases in
25 order to obtain a listing of publically available files suspected of containing child
26 pornography. For example, a user may enter the search term "baby j." "Baby j" is
27
28
29

1 associated with a series of videos of a known pre-pubescent child victim being
2 vaginally penetrated by an adult male. Other terms associated with child
3 exploitation cases include but are not limited to: “pthc” or pre-teen hardcore,
4 “lolita” after a novel about an adult male sexually aroused by pubescent girls under
5 the age of 18; “tara” after a known sexually abused pre-pubescent child victim; or,
6 “vicky” after a known sexually abused pre-pubescent child victim. In addition, a
7 user may enter a search term associated with the age of a child such as “6yo.”

8 32. Upon entering a term, the recipient user will receive a listing of files
9 associated with the term that are publically available for downloading from other
10 distributing users. The recipient user may select a file (the selected file) that also
11 has a digital signature known to law enforcement personnel that is identical to a
12 file containing child pornography. Once the recipient user selects the file for
13 downloading from the distributing user, the network may assemble the selected file
14 from not only the original distributing user but also other distributing users that
15 have files with the same digital signature. The recipient user now has downloaded
16 a file known to law enforcement personnel as containing child pornography
17 because that file has the same digital signature of a previously identified child
18 pornography file. Depending on the recipient user’s software program settings, the
19 recipient user now may publically advertise the child pornography file for
20 distribution to any other users, including law enforcement users, over these
21 networks.
22

23 33. Law enforcement personnel conduct undercover operations on the
24 Gnutella and the Ares network using a program that identifies users suspected of
25 publically advertising and/or trading in child pornography within certain
26 jurisdictions. A law enforcement user utilizes a program that enables that user to
27 view a user who is publically advertising for downloading, files that have digital
28
29

1 signatures previously identified by law enforcement personnel as containing
2 content including child pornography. A program may allow a law enforcement
3 user to download the file from the distributing user or view the distributing user's
4 shared directory of files that are publically available for downloading by any other
5 user. Depending on several factors including configuration and available
6 resources, the program may not allow law enforcement personnel to engage in
7 either option.

8 34. Law enforcement users may identify a distributing user according to
9 an Internet Protocol (IP) address. An IP address is a numeric label assigned to a
10 computer or digital device that is logged onto the Internet. A program utilized by
11 the law enforcement user may list one or more physical addresses. A law
12 enforcement user, however, identifies the Internet service provider associated with
13 a specific IP address according to a specified date and time (the specified IP
14 address). The Internet service provider then provides the law enforcement user
15 with subscriber information associated with that specified IP address. From that
16 subscriber information, law enforcement users may be able to identify the physical
17 address associated with the advertising of child pornography files for downloading.
18 There may be instances in which technologically savvy distributors use
19 "anonymizers" to mimic other IP addresses or where individuals use internet
20 connections subscribed to another location in an effort to avoid law enforcement
21 detection.
22

23 35. Based on the above information, a law enforcement user may
24 conclude the following: a user with a software program compatible with the
25 Gnutella and the Ares network that is installed on that user's computer or other
26 digital device, which has an IP address located in a region, is publically advertising
27 to any other users, including law enforcement users, that it has files available for
28
29

1 downloading that contain digital signatures identical to files known to law
2 enforcement personnel as containing child pornography.

3 36. From my training and experience, I know that any computer that
4 accesses the Internet must do so through an Internet Service Provider (ISP). The
5 ISP identifies the computer during the connection session by assigning it a unique
6 number, called an IP address. This number is attached to all messages that come to
7 and go from the computer.

8 THE INVESTIGATION

9 37. On May 7, 2015, AARRON DRAKE BUCKNER (BUCKNER) was
10 sentenced to six months of confinement at the United States Army Correctional
11 Facility-Europe after pleading guilty to violating the Uniform Code of Military
12 Justice (UCMJ) Article 134-General Article (Knowingly and Wrongfully
13 Possessing Child Pornography). After confinement, BUCKNER was given a Bad-
14 Conduct Discharge for the United States Army. While out processing on October
15 4, 2015, BUCKNER was provided a DD Form 2791 on which he initialed and
16 signed in multiple areas of the form. On this form, BUCKNER certified that he
17 would be residing at 686 Chimney Rock Drive, Oceanside, CA 92058 (SUBJECT
18 PREMISES) and acknowledged that he understood he was required to register as a
19 sex offender. Based on my conversation with Deputy United States Marshal
20 (DUSM) Adam Groff, I know that BUCKNER has failed to register as a sex
21 offender anywhere in California which is a federal crime. The SUBJECT
22 PREMISES is located in the Southern District of California.
23

24 38. On March 9, 2016, DUSM Groff opened an investigation into the
25 whereabouts of BUCKNER due to him failing to register in Oceanside, California.
26 Early in the investigation, Deputy Groff identified the Facebook Account
27 "www.facebook.com/aaron.buk.1" as belonging to BUCKNER. This was done by
28
29

1 photographic comparison of pictures posted for public view and by reviewing the
2 friends list, which revealed numerous known friends and relatives of BUCKNER.
3 While reviewing BUCKNER's Facebook page, Deputy Groff also observed
4 numerous "Facebook posts" by BUCKNER.

5 39. On December 16, 2015, BUCKNER posted a photograph of a screen
6 shot from his computer along with his computer's upload and download speeds.
7 The photograph also included the IP address (172.56.16.50), which was being used
8 by the computer in the photograph. The ISP for IP address 172.56.16.50 was
9 identified as T-Mobile USA. Deputy Groff also observed a large number of what
10 appeared to be underage girls who were Facebook friends with BUCKNER. The
11 girls appeared to be communicating with BUCKNER through Facebook. Several
12 of the girls claimed on their own Facebook pages to be attending Junior High and
13 High schools from across the United States. The communications were in the form
14 of Facebook "posts" and "likes." In several "posts," BUCKNER was asked
15 "Where you at" and "Where have you been," to which BUCKNER responded,
16 "Message Me."

17
18 40. On March 14, 2016, Deputy Groff contacted me in regards to his
19 investigation involving BUCKNER. I conducted law enforcement and open source
20 internet checks regarding IP address 172.56.16.50. I determined that IP address
21 172.56.16.50 was listed on an undercover law enforcement P2P file sharing
22 network. IP address 172.56.16.50 listed several Gnutella and numerous Ares files
23 with associated file names indicative of child pornography. The following are
24 three examples of files with associated file names that IP address 172.56.16.50
25 made available for sharing on the Gnutella and the Ares P2P file sharing programs:

26 **File Name:** "(pthc) 4 yo babj suck.mpg"

27 **File Name:** "pthc - veronika mila 10 yr 13 yr - nice pussy licking &
28 kissing 2 young lesbian.mpeg"

1 **File Name:** "pthc new 2011 12yr pussy and toy.flv"

2 41. I contacted T-Mobile USA to acquire subscriber information
3 regarding address 172.56.16.50. T-Mobile USA stated they were unable to provide
4 any subscriber information regarding IP address 172.56.16.50.

5 42. On March 22, 2016, Deputy Groff submitted a preservation request to
6 Facebook to preserve all material regarding BUCKNER's Facebook account
7 (<https://www.facebook.com/aarron.buckner>) with associated Facebook user ID
8 (<https://facebook.com/profile.php?id=100002025941957>).
9

10 43. Deputy Groff discovered a second Facebook account belonging to
11 BUCKNER by utilizing the same investigative techniques. On March 29, 2016,
12 Deputy Groff submitted a preservation request to Facebook to preserve all material
13 regarding BUCKNER's Facebook account
14 (<https://www.facebook.com/aaron.buk.1>) with associated Facebook user ID
15 (<https://facebook.com/profile.php?id=100011489746688>).
16

17 44. In March and April 2016, Facebook submitted three different
18 NCMEC CyberTipline Reports (report numbers 8958447, 9223406, and 9746798)
19 to the San Diego ICAC taskforce. All three reports were then forwarded to me for
20 investigation.

21 45. CyberTipline Report number 8958447 indicated that from November
22 23, 2015, to November 26, 2015, a female minor, hereinafter referred to as "FS"
23 used her Facebook account to send two images and two videos of herself to
24 BUCKNER via his Facebook account (www.facebook.com/aarron.buckner) with
25 associated Facebook screen name (aarron.buckner), Facebook user ID
26 (100002025941957), and email address (battlefield_dog@yahoo.com). I viewed
27 the two images and determined they depicted child erotica, not child pornography.
28 However, I viewed the videos and determined the two videos depicted child
29

1 pornography. The following is a description of both videos:

Video Description
The video depicts the female minor is exposing her vaginal area in a lewd and lascivious manner, while rubbing her clitoris and vaginal area with her left hand.
The video depicts the female minor is standing fully nude in a shower and continuously rubbing her vaginal area with her right hand.

2
3
4
5
6
7
8
9 46. CyberTipline Report number 9223406 indicated that from November
10 15, 2015, to November 26, 2015, FS used her Facebook account and sent nine
11 images and two videos of herself to BUCKNER via his Facebook account. I
12 viewed the images and determined four of the images depicted child pornography
13 and five of the images depicted child erotica. I viewed the videos and determined
14 one of the videos depicted child pornography and one of the videos depicted child
15 erotica. The following is an example of an image and a video:

Image Description
The image depicts the female minor, positioned on zebra-print material, exposing her clitoris and vaginal area in a lewd and lascivious manner.
Video Description
The video depicts the female minor, exposing her vaginal area in a lewd and lascivious manner, while rubbing her clitoris and vaginal area with her left hand.

16
17
18
19
20
21
22
23 47. CyberTipline Report number 9746798 included Facebook chats
24 between FS and BUCKNER that occurred from November 18, 2015, to November
25 21, 2015. On November 18, 2015, BUCKNER asked FS if she was a virgin in
26 which she responded, "Yes." BUCKNER stated, "Do u want me to use a
27 condom?" "How old r u babe?" FS responded, "17 and if u want to u don't have
28 to." BUCKNER also stated, "Were do you want me to cum?" and FS responded,
29

1 “Everywhere.”

2 48. On November 20, 2015, BUCKNER stated to FS, “I see ur bra :) can
3 us pull it down babe?” FS then sent BUCKNER an explicit image of herself.
4 BUCKNER then asked, “May I see both babe?” and FS again sends an explicit
5 image of herself. BUCKNER then stated, “Can I see ur undies baby? Fuck I want
6 you.” Later in the communication, BUCKNER requests FS to send additional
7 explicit images and videos of herself in which she complies.

8 49. On November 21, 2015, BUCKNER stated to FS, “Hold it still babe.”
9 FS later sends BUCKNER an explicit image of herself. BUCKNER replies,
10 “Mmm yesss fuck.”

11 50. NCMEC also contacted Hamilton, Ohio Police Sergeant Mark Hayes
12 regarding CyberTipline Report numbers 8958447, 9223406, and 9746798.
13 Sergeant Hayes conducted an interview with FS. During the interview, FS stated
14 that she sent explicit images and videos of herself to BUCKNER via Facebook. FS
15 stated she is a minor, and was born in 2001.

16 51. On or about April 9, 2016, law enforcement officers conducted law
17 enforcement and open internet source checks regarding BUCKNER. The
18 investigation revealed two separate Pay Pal accounts registered to BUCKNER.
19 Pay Pal log-in information indicated that BUCKNER used two separate IP
20 addresses while using his Pay Pal accounts. The first IP address, 208.54.4.193, is
21 assigned to T-Mobile as the ISP. The second IP address, 172.10.134.129, is
22 assigned to AT&T as the ISP.
23

24 52. On April 21, 2016, HSI SA Edward Coderes submitted a Department
25 of Homeland Security Summons to AT&T for subscriber and account information
26 regarding IP address 172.10.134.129. On April 26, 2016, AT&T provided the
27 following information regarding the IP address:
28
29

1 Account#: 121487143
2 Name: Renee Buckner
3 Address: 686 Chimney Rock Drive,
4 Oceanside, CA 92058-7420
5 Email: wren2011@gmail.com
6 Phone: (760) 453-1791

7 53. Between March 24, 2016, and March 26, 2016, DUSM Groff
8 conducted surveillance at the SUBJECT PREMISES. DUSM Groff did not see
9 BUCKNER on those days. However, DUSM Groff was able to identify
10 BUCKNER's mother, Tonja Renee Williams, residing at the SUBJECT
11 PREMISES. BUCKNER's mother's driver's license registration lists the
12 SUBJECT PREMISES as her residence. Additionally, BUCKNER's mother is
13 also known to the Department of Motor Vehicles (DMV) as Tonja Renee Buckner
14 and Tonja Renee Elizaldi.

15 54. On or about May 12, 2016, at approximately 9:00 a.m., video
16 surveillance was initiated at the SUBJECT PREMISES. Upon setup of the video
17 equipment, a silver 1996 Ford Mustang (vehicle) with a California license plate
18 number 6ZRV988 was observed parked in front of the SUBJECT PREMISES.
19 DUSM Groff conducted law enforcement checks with the California Department
20 of Motor Vehicles and discovered the vehicle is registered, as of March 8, 2016, to
21 BUCKNER at the SUBJECT PREMISES.

22 55. Between May 12, 2016, and May 16, 2016, video surveillance revealed
23 a male subject, matching BUCKNER's general appearance, departing and
24 returning from the SUBJECT PREMISES on multiple occasions in the vehicle.

25 56. On May 17, 2016, at approximately 8:26 a.m., video surveillance
26 revealed a male subject, identified by DUSM Groff, as BUCKNER exiting the
27 SUBJECT PREMISES. BUCKNER was observed carrying folded packing boxes
28 into the SUBJECT PREMISES.
29

1 57. On and between May 18, 2016, and May 22, 2016, video surveillance
2 revealed BUCKNER departing and returning from the SUBJECT PREMISES on
3 multiple occasions in the vehicle. BUCKNER was also observed performing yard
4 work, taking out trash, departing and returning with shopping bags, and having his
5 young child stay over during a recent weekend visitation.

6 58. DUSM Groff conducted additional open source internet queries and
7 discovered one additional Facebook account for BUCKNER.
8 (<https://www.facebook.com/cody.bruck.7> with associated Facebook user ID
9 <https://facebook.com/profile.php?id=100011638875220>).

10 59. On May 26, 2016, a federal search warrant (16MJ1508) was executed
11 at the SUBJECT PREMISES. The search warrant authorization was sought to
12 search for and seize evidence that relates to the violation of 18 U.S.C. § 2252. On
13 May 26, 2016, BUCKNER was also arrested on a federal arrest warrant
14 (16MJ1504) for violation of 18 U.S.C. § 2250, Failure to Register. Following the
15 search and arrest warrant, Deputy Groff and I interviewed Tonja Renee Williams.
16 She reported that BUCKNER currently has a Facebook account and his user name
17 is “cody bruck.” Ms. Williams indicated that BUCKNER chose the name “cody”
18 because that is the name of his dog and chose the name “bruck” because it may be
19 an abbreviation for Buckner. She stated that BUCKNER changed his Facebook
20 name to “cody bruck” approximately one or two months ago, but BUCKNER
21 never explained why he changed it.
22

23 60. On May 26, 2016, I submitted a preservation request to Facebook to
24 preserve all material regarding BUCKNER’s Facebook account
25 (<https://www.facebook.com/cody.bruck.7>) with associated Facebook user ID
26 (<https://facebook.com/profile.php?id=100011638875220>).

27 61. Based upon the above investigation, it is believed that the user of the
28
29

1 three Facebook accounts identified in Attachment A has a sexual interest in
2 children and is a collector of child pornography. Based upon my training and
3 experience, I know the following:

4 a. Individuals who collect and distribute child pornography tend to be
5 sexually attracted to children, their sexual arousal patterns and erotic imagery
6 focus, in part or in whole, on children. The collection may be exclusively
7 dedicated to children of a particular age, gender, or other set of characteristics, or it
8 may be more diverse, representing a variety of sexual preferences, including
9 children. Child pornography collectors express their attraction to children through
10 the collection of sexually explicit materials involving children as well as other
11 seemingly innocuous material related to children. These individuals may derive
12 sexual gratification from actual physical contact with children as well as from
13 fantasies involving the use of pictures or other visual depictions of children or
14 literature describing sexual contact with children. The overriding motivation for
15 the collection of child pornography and erotica is to define, fuel, and validate the
16 collector's most cherished sexual fantasies involving children. Visual depictions
17 may range from fully clothed children engaged in non-sexual activity to nude
18 children engaged in explicit sexual activity.

19
20 b. Individuals who collect child pornography tend to treat their material
21 as prized possessions and are especially unlikely to part with them. Even if the
22 collector feels threatened by exposure to law enforcement, he will usually seek to
23 preserve his collection by hiding it better, such as in their vehicle, rather than by
24 destroying it. The collection may be culled and refined, but the size of the
25 collection tends to increase over time. This is particularly true since digital storage
26 media have increased in storage capacity as they have decreased in cost.

27
28 c. In fact, many collectors protect their collections by creating back-ups,
29

1 sometimes multiple back-ups, of some or all of the collection. These collections
2 are stored on various electronic media devices, including, but not limited to,
3 external hard drives, thumb drives, cellular telephones, DVDs and CDs, and any
4 electronic media with storage capabilities and/or internet connections. Child
5 pornography, unlike some other kinds of contraband (e.g. drugs), is not
6 "consumed" by the user. The "consumption" of this product results in its
7 proliferation; more copies are generated. The very nature of computers and
8 electronic media as a means of collection, transmission, and/or storage lends itself
9 to permanent preservation of the item. If the collector relocates, his collection
10 almost always moves with him.

11 d. Individuals who collect child pornography tend to maintain and
12 possess their material in the privacy and security of their homes or some other
13 secure location like their vehicles where it is readily available. The collection may
14 include sexually explicit or suggestive materials involving children, such as
15 photographs, digital images, magazines, narratives, motion pictures, DVDs, CD-
16 ROMs, video tapes, books, slides, drawings, computer images or other visual
17 media.
18

19 e. Individuals who have a sexual interest in children or images of
20 children also may correspond with and/or meet others to share information and
21 materials; rarely destroy correspondence from other child pornography
22 distributors/collectors; conceal such correspondence as they do their sexually
23 explicit material; and often maintain lists of names, addresses, and telephone
24 numbers of individuals with whom they have been in contact and who share the
25 same interests in child pornography.
26

27 f. Individuals who have a sexual interest in children or images of
28
29

1 children prefer not to be without their child pornography for any prolonged time
2 period. This behavior has been documented by law enforcement officers involved
3 in the investigation of child pornography throughout the world.

4 62. The person(s) using the Facebook accounts has common
5 characteristics described above of someone involved in the distribution, receipt,
6 and possession of child pornography, as evidenced by the facts that are set forth in
7 this Affidavit. Specifically, this individual is in possession of videos of child
8 pornography and may be distributing these videos over the Internet and using
9 Facebook to receive and possess additional images and videos. This individual
10 engaged in this conduct over several different days as outlined above.

11 **PROCEDURES FOR ELECTRONICALLY STORED INFORMATION**

12 63. Federal agents and investigative support personnel are trained and
13 experienced in identifying communications relevant to the crimes under
14 investigation. The personnel of Facebook are not. It would be inappropriate and
15 impractical for federal agents to search the vast computer network of Facebook for
16 the relevant accounts and then to analyze the contents of those accounts on the
17 premises of Facebook. The impact on Facebook's business would be severe.

18 64. I anticipate executing this warrant under the Electronic
19 Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A)
20 and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the
21 government copies of the records and other information (including the content of
22 communications) particularly described in Section II of Attachment B. Upon
23 receipt of the information described in Section II of Attachment B, government-
24 authorized persons will review that information to locate the items described in
25 Section III of Attachment B.
26
27
28
29


1 65. Based on the foregoing, searching the recovered data for the
2 information subject to seizure pursuant to this warrant may require a range of data
3 analysis techniques and may take weeks or even months. Keywords need to be
4 modified continuously based upon the results obtained. The personnel conducting
5 the segregation and extraction of data will complete the analysis and provide the
6 data authorized by this warrant to the investigating team within ninety (90) days of
7 receipt of the data from the service provider, absent further application to this
8 court.

9 66. Based upon my experience and training, and the experience and
10 training of other agents with whom I have communicated, it is necessary to review
11 and seize all electronic communications that identify any users of the subject
12 account(s) and any electronic mails sent or received in temporal proximity to
13 incriminating electronic mails that provide context to the incriminating mails.
14

15 67. All forensic analysis of the imaged data will employ search protocols
16 directed exclusively to the identification, segregation and extraction of data within
17 the scope of this warrant.

18 **CONCLUSION**

19 68. In conclusion, based upon the information contained in this affidavit, I
20 have reason to believe that evidence, fruits and instrumentalities relating to
21 violations of 18 U.S.C. §§ 2250 and 2252, are located at the location described in
22 Attachments A.

23
24 
25 _____
26 Chad N. Worgen, Special Agent
27 Homeland Security Investigations
28
29

1 SUBSCRIBED and SWORN to before me this 3 day of June 2016.

2
3 

4 HONORABLE MITCHELL D. DEMBIN
5 UNITED STATES MAGISTRATE JUDGE
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29

ATTACHMENT A

1
2 This warrant applies to information associated with the following Facebook
3 user IDs:

- 4 1. <https://facebook.com/profile.php?id=100002025941957>
- 5 2. <https://facebook.com/profile.php?id=100011489746688>
- 6 3. <https://facebook.com/profile.php?id=100011638875220>

7 that are stored at premises owned, maintained, controlled, or operated by Facebook
8 Inc., a company headquartered at 1601 Willow Road, Menlo Park, CA 94025.
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29

ATTACHMENT B

I. Service of Warrant

The officer executing the warrant shall permit Facebook, Inc. as custodian of the computer files described in Section II below, to locate the files and copy them onto removable electronic storage media and deliver the same to the officer.

II. Items subject to seizure

All subscriber and/or user information, all electronic mail, images, GPS tags, text messages, private messages (Messenger), comments, likes, histories, buddy lists included individuals following and individuals followed, profiles, method of payment, detailed billing records, access logs, transactional data and any other files associated with the following accounts and screen names for the following periods of October 4, 2015, to present:

1. <https://facebook.com/profile.php?id=100002025941957>
2. <https://facebook.com/profile.php?id=100011489746688>
3. <https://facebook.com/profile.php?id=100011638875220>

The search of the data supplied by Facebook.com pursuant to this warrant will be conducted as provided in the “Procedures For Electronically Stored Information” of the incorporated affidavit submitted as an attachment to the affidavit submitted in support of this search warrant and will be limited to seizing electronic subscriber and/or user information, photographs and/or attachments, electronic mail and communications tending to show evidence or instrumentalities of violations of 18 U.S.C. §§ 2250 and 2252 including:

- (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),

1 telephone numbers, screen names, websites, and other personal
2 identifiers.

- 3 (b) All activity logs for the account and all other documents showing the
4 user's posts and other Facebook activities;
- 5 (c) All Photoprints, including all photos uploaded by that user ID and all
6 photos uploaded by any user that have that user tagged in them to
7 include EXIF data;
- 8 (d) All Neoprints, including profile contact information; News Feed
9 information; status updates; links to videos, photographs, articles, and
10 other items; Notes; Wall postings; friend lists, including the friends'
11 Facebook user identification numbers; groups and networks of which
12 the user is a member, including the groups' Facebook group
13 identification numbers; future and past event postings; rejected
14 "Friend" requests; comments; gifts; pokes; tags; and information
15 about the user's access and use of Facebook applications;
- 16 (e) All other records of communications and messages made or received
17 by the user, including all private messages, chat history, video calling
18 history, and pending "Friend" requests;
- 19 (f) All "check ins" and other location information;
- 20 (g) All IP logs, including all records of the IP addresses that logged into
21 the account;
- 22 (h) All records of the account's usage of the "Like" feature, including all
23 Facebook posts and all non-Facebook webpages and content that the
24 user has "liked";
- 25 (i) All information about the Facebook pages that the account is or was a
26 "fan" of;
27
28
29

- 1 (j) All past and present lists of friends created by the account;
- 2 (k) All records of Facebook searches performed by the account;
- 3 (l) All information about the user's access and use of Facebook
- 4 Marketplace;
- 5 (m) The length of service (including start date), the types of service
- 6 utilized by the user, and the means and source of any payments
- 7 associated with the service (including any credit card or bank account
- 8 number);
- 9 (n) All privacy settings and other account settings, including privacy
- 10 settings for individual Facebook posts and activities, and all records
- 11 showing which Facebook users have been blocked by the account;
- 12 (o) All records pertaining to communications between Facebook and any
- 13 person regarding the user or the user's Facebook account, including
- 14 contacts with support services and records of actions taken.
- 15
- 16 (p) All email communications to include but not limited to; sent, received,
- 17 deleted, drafted, and stored in the accounts listed above.
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28
- 29