

ORIGINAL

AO 91 (Rev. 11/11) Criminal Complaint

LOGGED

UNITED STATES DISTRICT COURT

2019 NOV 12 AM 10:06

for the
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
RIVERSIDE
Central District of California

BY
CLERK U.S. DISTRICT COURT
CENTRAL DIST. OF CALIF.
RIVERSIDE

2019 NOV 12 AM 10:08

FILED

UNITED STATES OF AMERICA,

v.

STEFANI KASEY MARIE STEVENS,

Defendant.

ED19-0607M

Case No.

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief. In or about November 2018, in the County of San Bernardino in the Central District of California, the defendant violated:

Code Section

18 U.S.C. §§ 2251(a), (e)

Offense Description

Production of Child Pornography

This criminal complaint is based on these facts:

Please see attached affidavit.

Continued on the attached sheet.


Complainant's signature

Jonathan Ruiz, Special Agent,
Homeland Security Investigations

Printed name and title

Sworn to before me and signed in my presence.

Date: November 9, 2019


Judge's signature

City and state: Riverside, California

Hon. Sheri Pym, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

I, Jonathan Ruiz, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against Stefani Kasey Marie Stevens ("STEVENS"), for a violation of Title 18, United States Code, Sections 2251(a), (e) (Production of Child Pornography).

2. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and part only.

II. BACKGROUND OF AFFIANT

3. I am a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations ("HSI") and have been so employed since 2007. From April 2007 to November 2014, I was assigned to the Child Exploitation Investigations Group for the HSI Office of the Special Agent in Charge, Los Angeles, California. In November 2014, I transferred to the Child Exploitation Investigations Group for the HSI Office of the Assistant Special Agent in Charge, Riverside and San Bernardino,

California. My daily duties as a SA include investigating 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, 2252 and 2252A. During the course of these investigations, I have participated in the execution of numerous search warrants and seized evidence of such violations.

4. Through my training and experience, I have become familiar with the methods of operation used by people who sexually exploit children. I have attended training classes and seminars concerning computer crimes and the sexual exploitation of children on the Internet. My training and experience in these investigations has given me an understanding of how people involved with offenses relating to the sexual exploitation of children use the Internet to further those offenses.

III. SUMMARY OF PROBABLE CAUSE

5. On November 8, 2019, law enforcement officers executed two search warrants issued earlier that day. I conducted a *Mirandized* interview of STEVENS. During the interview, STEVENS admitted to using her iPhone to take sexually explicit photographs of a female child's ("MINOR NG")¹ vagina and using her iPhone to send them to other individuals on the Internet using Kik as well as to one other individual via text message.

¹ For privacy reasons, I do not include additional details about MINOR NG's identity in my affidavit. I will provide additional information about MINOR NG at the Court's request.

IV. STATEMENT OF PROBABLE CAUSE

6. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. The Search Warrant Application

7. On November 8, 2019, the Honorable Sheri Pym, United States Magistrate Judge, Central District of California, issued warrants to search (1) 34184 County Line Road, Space #90, Yucaipa, California 92399 (the "SUBJECT PREMISES"), and (2) the person of Stefani Kasey Marie Stevens ("STEVENS") (together, the "Search Warrants"). I have attached as Exhibit 1 the affidavit I submitted to the Court in support of my applications for the Search Warrants. Exhibit 1 is incorporated by reference into this affidavit.

B. The Search Warrant was executed at the Subject Premises

8. On November 8, 2019, at about 1:00 p.m., law enforcement personnel arrived at the SUBJECT PREMISES to execute the Search Warrants. Upon arrival, law enforcement personnel announced their presence and demanded that all individuals inside the SUBJECT PREMISES come outside. STEVENS, MINOR NG, Logan Grimes ("L GRIMES"), and a male maintenance employee of the mobile home park, came out of the SUBJECT PREMISES. Garret Grimes, MINOR NG's father, was not at the mobile home when the search was conducted.

9. Law enforcement personnel then took steps to secure the property. Initially, STEVENS, L GRIMES and the maintenance

employee were put into restraints and brought to an area behind a police car. And MINOR NG was brought to a second police car away from STEVENS and L GRIMES. Then, law enforcement personnel went inside the SUBJECT PREMISES to ensure no other occupants were hiding inside. Once the SUBJECT PREMISES was secured, STEVENS and L GRIMES had their restraints removed and they were taken inside the SUBJECT PREMISES and sat in the living room. The mobile home park management verified the identity of the maintenance employee and law enforcement personnel released him. Next, law enforcement personnel brought MINOR NG to a local police station, where she met with San Bernardino County Department of Children and Family Services before being released to the custody of her mother, Emily Grimes.

10. During the execution of the Search Warrants, I recognized that the master bathroom in the SUBJECT PREMISES is the same location in which two images discussed in Exhibit 1 – “report_4487638173229803249” and “report_12126718075593315792” – were taken. See Exhibit 1 ¶ 44(f). Additionally, in MINOR NG’s bedroom, I saw that the sheets, comforter, and pillow case on MINOR NG’s bed matched those depicted in five images discussed in Exhibit 1: (1) “2019-04-03,” (2) “2019-04-13,” (3) “report_123210111561297029579,” (4) “report_8175760579594825736,” and (5) “report_10812106022160631927.” See Exhibit 1 ¶¶ 44(a)-(e).

C. STEVENS’s *Mirandized* interview

11. At about 1:40 p.m., I read STEVENS her *Miranda* rights. I informed STEVENS that if she decided to answer questions now,

she still had the right to stop the questioning at any time, including for the purposes of consulting an attorney. STEVENS said "okay" while simultaneously nodding her head in the affirmative. I asked STEVENS if she understood the rights I read to her and she said "yes."

12. I interviewed STEVENS about Kik. STEVENS stated that she used her iPhone to communicate on the Kik Messenger platform. STEVENS said that approximately four months ago she traded in her old iPhone (the "Old iPhone") and upgraded to a new iPhone, which she described as an iPhone XS Max (the "New iPhone"). STEVENS admitted to using the Kik account "ONENONLY7210" (the "SUBJECT KIK ACCOUNT") – as well as other Kik accounts – to send and receive child pornography. According to STEVENS, she started viewing child pornography about two years ago. After about one year, STEVENS stopped viewing child pornography for about six months before beginning to view it again.

13. I interviewed STEVENS about the child pornography images discussed in Exhibit 1. *First*, I showed STEVENS a redacted copy of the child pornography image described in paragraph 28 of Exhibit 1 as follows:

The image depicts a nude male adult vaginally penetrating an infant female's vagina. The infant is lying on her back. The infant is wearing "onesie" pajamas that have been partially removed, resulting in her being nude from stomach down to her feet. The camera is closely focused on the child's abdomen and pelvic area as a male adult's erect penis is penetrating the infant.

The redacted version of the image I showed STEVENS had the male adult's penis and child's pelvic area blacked out. In response, STEVENS said that she recognized the image as one she received from another user on Kik and that she subsequently redistributed to other persons on Kik.

14. *Second*, I showed STEVENS a redacted copy of the child pornography image described in paragraph 46 of Exhibit 1 as follows:

The image depicts an infant laying on its back. The infant is wearing a onesie that has been unzipped exposing the infant's bare chest. A male adult's erect penis is exposed and is resting on the lips of the infant. The image is closely focused on the male adult's penis and the child's face and abdomen.

The redacted version of the image I showed STEVENS had the male adult's penis blacked out. STEVENS stated that she recognized the image as one she received from another user on Kik and that she subsequently redistributed to other persons on Kik,

15. *Third*, I showed STEVENS a redacted copy of the child pornography image described in paragraph 48 of Exhibit 1 as follows:

The image depicts an infant laying on their stomach on top of bedding that is grey in color with roses and flowers printed on it. The infant appears to be nude. A white adult person's hand is seen spreading open the buttocks of the infant exposing the infant's anus and vagina to the camera. The camera is closely focused on the child's buttocks and vagina area.

The redacted version of the image I showed STEVENS had the child's anus blacked out. According to STEVENS, she recognized the image as one she received from another user on Kik but was not sure if she redistributed the image to other persons on Kik.

16. *Fourth*, I showed STEVENS redacted copies of the six images described in paragraphs 44(a) through 44(f) of Exhibit 1 that appear to depict MINOR NG, the descriptions of which are repeated below:

The image titled "2019-04-03" depicts a nude prepubescent female, appearing to be under the age of 12 years old, laying on her back on top of a bedsheet that is with a pattern of pastel colored circles. There is a pillow with a pillowcase visible that has a purple butterfly on it. The child is using her hands to hold up both of her legs exposing her vagina and anus to the camera. The child's face is visible in the photo and she closely resembles the same preteen girl depicted in photos found on STEVENS's Facebook profile.

The image titled "2019-04-13" depicts what appears to be the same nude prepubescent female described above. In this particular photo, the nude child is laying on her stomach facing away from the camera. The child is laying on a multi-colored comforter (blue, purple and white) with a pattern of hearts and flowers printed on it. A white person's hand is seen pushing aside one of the child's legs exposing the child's vagina to the camera.

The image titled "report_123210111561297029579" depicts a prepubescent female laying on her back on top of a white sheet with blue and teal hearts printed on it. The child's legs are spread apart, and a white person's left hand is seen touching the child's buttocks

exposing her vagina and anus to the camera. The camera is closely focused on the child's anus and vagina.

The image titled "report_8175760579594825736" depicts a close up of a prepubescent female's vagina. The child is on top of a white sheet with blue and teal hearts printed on it. The child's legs are spread apart, and a white person's right hand is seen touching the child's buttocks exposing her vagina to the camera. The camera is closely focused on the child's vagina.

The image titled "report_10812106022160631927" depicts a close up of a prepubescent female's vagina. The child is laying on the same multi-colored comforter as described above. The child is spreading her legs apart and with her hands is touching her pelvic area.

The images titled "report_4487638173229803249" and "report_12126718075593315792" are visually similar. They depict a nude prepubescent female standing in front of a toilet. The child appears to be wiping her vagina with toilet paper. The child's face is partially visible.

The redacted versions of the images I showed STEVENS each had MINOR NG's genitalia blacked out. STEVENS admitted to taking all six of these images of MINOR NG. STEVENS stated that she took the six images approximately one year ago in the SUBJECT PREMISES on her iPhone – which, based on the timeframe, I understood to mean her Old iPhone. STEVENS said the six images were saved on her iPhone at one time but she has since deleted them.

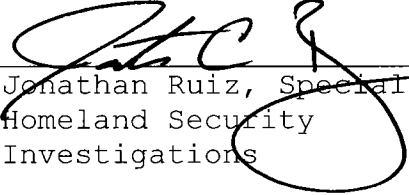
17. I asked STEVENS how many nude pictures she took of MINOR NG. STEVENS stated about eight to ten images. I also asked STEVENS why she took nude photos of MINOR NG. In response, STEVENS stated that she was communicating with a person on Kik who asked her if she had a daughter. After STEVENS told the Kik user that she did, the Kik user asked her for the pictures of her daughter. So STEVENS then took photos of MINOR NG and sent them to the Kik user.

18. Additionally, I asked STEVENS what she told MINOR NG the pictures were for. According to STEVENS, MINOR NG had a rash at the time so STEVENS said she told MINOR NG that the photos were for the doctor to look at. I asked STEVENS if she distributed the images of MINOR NG to other people on platforms besides Kik. STEVENS looked through the six redacted photos of MINOR NG and then identified two of the photos as ones she sent to an unidentified male via text message. The two photos STEVENS identified are described in paragraphs 44(a) and 44(b) of Exhibit 1. See Exhibit 1 ¶¶ 44(a), 44(b).

19. At approximately 3:10 p.m., the interview with STEVENS concluded. After the interview, I met with members of the search team and learned that an iPhone XS Max (with IMEI number 353096102593044) was discovered at the SUBJECT PREMISES, which matched the description of the New iPhone. The New iPhone was seized along with the bedding from MINOR NG's room, two tablets and a desktop computer.

V. CONCLUSION

20. For all the reasons described above, there is probable cause to believe that STEVENS has violated 18 U.S.C. §§ 2251(a), (e) (Production of Child Pornography).


Jonathan Ruiz, Special Agent
Homeland Security
Investigations

Subscribed to and sworn before
me on November 9, 2019.


UNITED STATES MAGISTRATE JUDGE

EXHIBIT 1

**to the Affidavit of
Special Agent Jonathan Ruiz**

AFFIDAVIT

I, Jonathan Ruiz, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of an application for a warrant to search (1) 34184 County Line Road, Space #90, Yucaipa, California 92399 (the "SUBJECT PREMISES"), and (2) the person of Stefani Kasey Marie Stevens ("STEVENS"), as described more fully in Attachments A-1 and A-2, respectively, in connection with a child pornography investigation.

2. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 2251(a) (Production of Child Pornography), 2252A(a)(2) (Receipt and Distribution of Child Pornography), and 2252A(a)(5)(B) (Possession of Child Pornography) (collectively, the "TARGET OFFENSES"), as more fully described in Attachment B-1.

3. The requested search warrant for STEVENS seeks authorization to search her person, including the contents of any bags or containers in her possession, to seize evidence, fruits, and instrumentalities of violations of the SUBJECT OFFENSES, as more fully described in Attachment B-2.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrants,

and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. BACKGROUND OF AFFIANT

5. I am a Special Agent ("SA") with the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations ("HSI") and have been so employed since 2007. From April 2007 to November 2014, I was assigned to the Child Exploitation Investigations Group for the HSI Office of the Special Agent in Charge, Los Angeles, California. In November 2014, I transferred to the Child Exploitation Investigations Group for the HSI Office of the Assistant Special Agent in Charge, Riverside and San Bernardino, California. My daily duties as a SA include investigating 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, 2252 and 2252A. During the course of these investigations, I have participated in the execution of numerous search warrants and seized evidence of such violations.

6. Through my training and experience, I have become familiar with the methods of operation used by people who sexually exploit children. I have attended training classes and seminars concerning computer crimes and the sexual exploitation of children on the Internet. My training and experience in

these investigations has given me an understanding of how people involved with offenses relating to the sexual exploitation of children use the Internet to further those offenses.

III. BACKGROUND REGARDING CHILD EXPLOITATION OFFENSES, COMPUTERS, AND THE INTERNET

7. Based upon my training and experience in the investigation of child pornography, and information given to me by other law enforcement officers involved in the investigation of child pornography, I know the following information about the use of computers and child pornography:

8. Computers. Computers and computer technology have revolutionized the way in which individuals interested in child pornography 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 to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these images on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these images was accomplished through a combination of personal contacts, mailings, and telephone calls.

9. The development of computers has changed this. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage. Child pornographers can now transfer photographs from

a camera onto a computer readable format with a device known as a scanner. 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.

10. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera or smartphone, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them).

11. Media storage devices can easily be concealed and carried on an individual's person. It is particularly common for individuals to regularly carry their smart phones on them.

These devices can store thousands of images of child pornography and connect directly to the Internet as well as other cellular devices.

12. Internet. The Internet is a collection of computers and computer networks which are connected to one another via high-speed data links and telephone lines for the purpose of communicating and sharing data and information. Connections between Internet computers exist across state and international borders; therefore, information sent between two computers connected to the Internet frequently crosses state and international borders even when the two computers are located in the same state.

13. Internet Service Providers. Any individuals and businesses obtain access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account

application information, and other information both in computer data and written record format.

14. IP Addresses. An Internet Protocol address ("IP address") is a unique numeric address used by each computer on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be properly directed from its source to its destination. Most ISPs control a range of IP addresses.

15. When a customer logs into the Internet using the service of an ISP, the computer used by the customer is assigned an IP address by the ISP. The customer's computer retains that IP address for the duration of that session (i.e., until the user disconnects), and the IP address cannot be assigned to another user during that period.

16. The following definitions apply to this Affidavit and Attachments B-1 and B-2:

a. "Child pornography," "visual depiction," "minor," and "sexually explicit conduct," are defined as set forth in Title 18, United States Code, Section 2256.

b. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This

feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors, but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

d. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

e. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

f. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

IV. SUMMARY OF PROBABLE CAUSE

17. Kik Messenger ("Kik"), a Canadian-based instant messaging application for mobile devices, reported to the Royal Canadian Mounted Police ("RCMP") that one of its users, identified as "ONENONLY7210," uploaded an image depicting the sexual abuse of an infant child. Kik provided the RCMP with a copy of the child sexual abuse material uploaded by ONENONLY7210 along with subscriber registration information and login

records. After reviewing the login records for the ONENONLY7210 account, the RCMP learned that the user was utilizing IP addresses assigned to ISPs from within the United States. The RCMP forwarded the investigative materials to HSI where it was subsequently sent to HSI Riverside for further investigation.

18. HSI Riverside's investigation revealed that account registration information and login records for ONENONLY7210 appear to be associated with STEVENS, who resides at the SUBJECT PREMISES.

V. STATEMENT OF PROBABLE CAUSE

A. Background on Kik Messenger

19. Kik is a mobile application designed for chatting or messaging. Prior to October 2019, Kik was owned and operated by Kik Interactive, Inc. a Canadian based company operating from Ontario, Canada. In October 2019, the Kik communications platform was acquired by MediaLab, a multimedia company based in Los Angeles, California.

20. According to the publicly available document, "Kik's Guide for Law Enforcement," to use this application, a user downloads the application to a mobile phone, computer, or other digital device via a service such as the iOS App Store, Google Play Store, Apple iTunes, or another similar provider. Once the application is downloaded and installed, the user is prompted to create an account or login to an existing account by entering the Kik username or email address and the necessary password. To create a Kik account, users are prompted to enter their first name, their last name, a Kik username, their email address,

password, and their date of birthdate. Kik does not verify that the information entered is valid. For example, Kik does not verify that the email address entered is valid or that the birthday entered is the user's actual birthday. Kik allows for the entry of a phone number upon registering but it is not required.

21. Once the user has created an account, the user is able to locate other users via a search feature. While messaging, users can then send each other text messages, images, and videos.

22. According to "Kik's Guide for Law Enforcement," Kik users are also able to create chat groups with a limited number of individuals to communicate in a group setting and exchange text messages, images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. Once the group is created, Kik users have the option of sharing a hyperlink which serves as an invitation to the group. The Kik groups are identified by a hashtag (#) followed by the name of the group. For example, "#Sports" would be used to identify a Kik group for people interested in discussing or sharing information about sports.

23. According to information provided to HSI by a Kik Law Enforcement Response Team Lead, Kik's Terms of Service prohibit Kik users from uploading, posting, sending, commenting on, or storing content that contains child pornography and/or child abuse images. The Terms of Service also provide that Kik may review, screen and delete user content at any time if Kik

believes use of their services are in violation of the law. According to Kik, Kik has a strong business interest in enforcing their Terms of Service and ensuring that their services are free of illegal content, and in particular, child sexual abuse material. Accordingly, Kik reports that it independently and voluntarily takes steps to monitor and safeguard their platform and that ridding Kik products and services of child abuse images are critically important to protecting their users, product, brand, and business interests.

24. Prior to MediaLab's acquisition of Kik in October 2019, Kik was located and operating in Ontario, Canada and governed by Canadian law. According to information contained in the "Kik Interactive, Inc. Child Sexual Abuse and Illegal Material Report and Glossary" ("Kik Glossary"), which Kik provides when reporting information to law enforcement authorities, Kik is mandated to report to the RCMP any images and/or videos that would constitute suspected child pornography under Canadian law which are discovered on the Kik platform. Kik identifies child pornography on its platform by digital hash value matches to previously identified child pornography or through "Abuse Reports" generated from other Kik users or third party moderators on the Kik platform. With respect to the use of digital hash value matches, Kik utilizes "PhotoDNA" software, a product of Microsoft. According to Microsoft:

PhotoDNA creates a unique digital signature (known as a "hash") of an image which is then compared against signatures (hashes) of other photos to find copies of the same image. When matched with a database

containing hashes of previously identified illegal images, PhotoDNA is an incredible tool to help detect, disrupt and report the distribution of child exploitation material.

25. Kik uses PhotoDNA to automatically scan user-uploaded files in order to flag images that may depict suspected child pornography and prevent such images from continuing to circulate through their application. When PhotoDNA detects a suspected child pornography file, it creates a report and sends it to the Kik Law Enforcement Response Team. According to information provided by a Kik Law Enforcement Response Team Lead, all suspected child pornography images and videos reported via PhotoDNA is reviewed by a member of the Kik Law Enforcement Response Team before a report is forwarded to law enforcement authorities. Kik trains employees comprising its Law Enforcement Response Team on the legal obligation to report apparent child pornography. The Law Enforcement Response Team is trained on the Canadian statutory definition of child pornography and how to recognize it on Kik products and services. Kik voluntarily makes reports to law enforcement in accordance with that training. After Kik discovers the suspected child pornography, Kik removes the content from its communications system and closes the user's account.

26. The RCMP has advised HSI that upon receiving reports from Kik related to suspected child pornography, the RCMP reviews the IP addresses of the reported Kik users to determine their geographical location. The RCMP then provides Kik Reports of Kik users in the United States to HSI Office of the Attaché

located in Ottawa, Canada ("HSI Ottawa"). HSI Ottawa then turns over the Kik Reports to the HSI Cyber Crimes Center ("HSI C3") Child Exploitation Investigations Unit located in Fairfax, Virginia for analysis and dissemination to the local HSI field office where the Kik user is believed to be residing. It takes approximately four to five months from the time the Kik user is identified by Kik and the time that the information is provided to the local HSI field office.

**B. HSI Riverside Investigation of Kik Account
ONENONLY7210**

27. In or about August 2019, I received from HSI C3 information showing that in April 2019, Kik identified the user "ONENONLY7210" (the "SUBJECT KIK ACCOUNT") as uploading child exploitation material to its platform through the use of PhotoDNA. Information provided by Kik included a Subscriber Data Report containing the SUBJECT KIK ACCOUNT's subscriber registration and login information, as well as a copy of the child exploitation image identified by PhotoDNA.

28. In or about September 2019, I reviewed the image Kik identified by PhotoDNA. The image depicts a nude male adult vaginally penetrating an infant female's vagina. The infant is lying on her back. The infant is wearing "onesie" pajamas that have been partially removed, resulting in her being nude from stomach down to her feet. The camera is closely focused on the child's abdomen and pelvic area as a male adult's erect penis is penetrating the infant.

29. According to the information provided by Kik, the image was uploaded to the Kik platform by the SUBJECT KIK ACCOUNT on April 14, 2019, at 1:37 a.m. (UTC). When the image was uploaded, the SUBJECT KIK ACCOUNT was utilizing IP address 172.250.146.2 (the "SUBJECT IP 1").

30. I reviewed the Subscriber Data Report, dated April 14, 2019, and learned that the SUBJECT KIK ACCOUNT was created on August 4, 2012, at 7:40 a.m. (UTC). The Subscriber Data Report also contains information relating to changes made to the account. Below is a summary of some of the catalogued changes that were made to the SUBJECT KIK ACCOUNT registration information:

a. On August 23, 2012, at 8:39 a.m. (UTC), the last name of "Stevens" was registered to the SUBJECT KIK ACCOUNT.

b. On February 4, 2014, at 5:04 p.m. (UTC), the first name of "Stefani" was registered to the SUBJECT KIK ACCOUNT.

c. On June 26, 2015, at 4:00 a.m. (UTC), the email address "stevens.stefani515@gmail.com" (the "SUBJECT EMAIL 1") was registered to the SUBJECT KIK ACCOUNT.

d. On August 22, 2018, at 2:18 a.m. (UTC), the email address "Oneandonly7210@gmail.com" (the "SUBJECT EMAIL 2") was registered to the SUBJECT KIK ACCOUNT. Kik reported that this email address was confirmed.

e. On April 14, 2019, the same day the SUBJECT KIK ACCOUNT was identified by Kik as uploading child pornography,

the SUBJECT KIK ACCOUNT holder utilized the Kik Application using an "iPhone."

31. The Subscriber Data Report also contained login records detailing the IP addresses and dates and times the SUBJECT KIK ACCOUNT was accessed. Kik provided login records from April 2, 2019 until April 14, 2019. During that time frame, I found that the SUBJECT KIK ACCOUNT was accessed about 56 times from the SUBJECT IP 1. Additionally, I found that on April 8, 2019, between 12:38 a.m. (UTC) and 11:00 p.m. (UTC), the SUBJECT KIK ACCOUNT was accessed eight times from IP address 23.240.116.88 (the "SUBJECT IP 2"). I also found from April 7, 2019, between 12:30 a.m. (UTC) and April 9, 2019 at 9:21 p.m. (UTC), the SUBJECT KIK ACCOUNT was accessed 17 times from IP addresses beginning with "99.203."

32. On or about September 17, 2019, I conducted a query of the SUBJECT IP 1, SUBJECT IP 2, and the IP addresses beginning with 99.203 within the website Maxmind.com, an online search tool used to identify the internet service provider owning a specific IP address. In response to the search, I learned that the SUBJECT IP 1 and SUBJECT IP 2 are both owned by Charter Communications. Additionally, I learned that IP addresses beginning with 99.203 were owned by Sprint PCS, a provider of wireless internet and voice communications services for mobile devices such as smartphones like the Apple iPhone or wireless enabled tablet.

33. On or about September 24, 2019, I sent a summons (RV-2019-0443) to Charter Communications requesting customer account

information for the SUBJECT IP 1 utilized on April 2, 2019 at 3:51:44 p.m. (UTC), and for the SUBJECT IP 2 utilized on April 8, 2019 at 8:16:17 p.m. (UTC) and at 11:00:55 p.m. (UTC).

34. Charter Communications responded to the summons on or about October 29, 2019, and identified the SUBJECT IP 1 as being assigned to STEVENS at the SUBJECT PREMISES. According to Charter Communications, the SUBJECT IP 1 was assigned to STEVENS at the SUBJECT PREMISES from June 12, 2018 until July 21, 2019. Additionally, Charter Communications identified the SUBJECT IP 2 as being assigned to Robert Stevens at 12520 3rd Street, Yucaipa, California 92399 (the "3rd Street address"). According to Charter Communications, the SUBJECT IP 2 was assigned to the Robert Stevens from June 23, 2018 until September 26, 2019.

35. On or about September 20, 2019, I sent a summons (RV-2019-00447) to Sprint PCS requesting customer account information for three of 18 IP addresses beginning with 99.203. Sprint PCS responded to the summons on or about October 8, 2019 and informed me that they do not maintain IP address logs. More specifically Sprint PCS stated:

logging information is not retained for the IP requested as it is only kept for the length of the session. When the session terminates, the logging information is lost. The data is not stored.

36. The next day, on October 30, 2019, I conducted a search for STEVENS at the SUBJECT PREMISES within Thompson Reuters Consolidated Lead Evaluation and Reporting ("CLEAR"). CLEAR is an online research tool that hosts a vast collection of public and proprietary records such as consumer and credit

bureau data, motor vehicle data, utility, real estate and other business data. The results of the search show that STEVENS has been associated with the SUBJECT PREMISES since July 2016.

CLEAR also reports that Garrett Grimes has been associated with the SUBJECT PREMISES since May 2015 and Logan Grimes has been associated with the SUBJECT PREMISES since July 2018. CLEAR also reports that STEVENS was associated with the 3rd Street address as recently as March 2019. Additional searches within CLEAR show that Robert Stevens at the 3rd Street address is a relative of STEVENS.

37. That day, October 30, I also conducted a search within databases maintained by the California Department of Motor Vehicles (the "DMV") and found that STEVENS was issued California driver's license number E2333009 with an address on file of the 3rd Street address. STEVENS's California driver license shows that her full name is Stefani Kasey Marie Stevens. I also found a California drivers' licenses issued to Garrett Grimes with the SUBJECT PREMISES listed as the address on file and issued to Logan Grimes with an address of 37524 County Line Road, Yucaipa, California listed as the address on file.

38. On or about November 1, 2019, I conducted a search on Google for online profiles associated with "ONENONLY7210." Google results yielded numerous online social media profiles all appearing to be related to STEVENS. For example, a Twitter account for "@onenonly7210," displaying the name "Stefani" was found. The Twitter account is public and shows that it was created in February 2012. The Twitter account contains numerous

postings ("Tweets"), the most recent of which was posted in July 2018. Some of the Tweets contain "selfie" type photos depicting the same female depicted on STEVENS's California driver's license. By way of additional example, an account with the social media platform "Pinterest" has a user registered to "onenonly7210" with a display name of "Stefani Stevens." The account contains a profile picture of the same female depicted on STEVENS's California driver's license.

39. Additionally, I conducted a search within the social media website Facebook.com for "Stefani Stevens Yucaipa, California," and found a user account registered to "Stefani Stevens" containing a profile picture of the same female depicted on STEVENS's California driver's license. In the profile picture STEVENS is standing next to a male minor who appears to be her son. The profile was public and contained multiple pictures of herself, her preteen son, and another preteen female that is believed to be related. I also found multiple photos of STEVENS with a male adult resembling the same male depicted on Garrett Grimes's California driver's license. In reviewing the photos found on STEVENS's Facebook profile, it appears that STEVENS and Grimes are or were romantically involved.

40. I also conducted a search within the social media website Instagram for a user profile containing "ONENONLY7210." I found one user profile for "__ONENONLY7210" that contained the following user information "us (flower emoji) Stefani (flower emoji) us" followed by "Mother (heart emoji) Taurus (Taurus

emoji) Taken (heart emoji).” The account was private and not accessible for review. But the profile did contain a profile picture of a minor female and minor male standing next to each other. Both the male and female minor appear to be the same children depicted in photos found on STEVENS’s Facebook account.

C. NCMEC Cybertip Relating to Stevens

41. On or about October 30, 2019, I requested that the National Center for Missing and Exploited Children (“NCMEC”) conduct a search within their databases for reports and or law enforcement inquiries relating to information associated with STEVENS. More specifically, I requested a search for the following:

Stefani Stevens
909-492-5019
909-633-7319
Onenonly7210
Oneandonly7210
Steven.stefani515@gmail.com
Oneandonly7210@gmail.com

IP addresses
172.250.146.2 between June 12, 2018 and July
21, 2019
23.240.116.88.1.1.1 between June 23, 2018
and September 26, 2019

42. On or about October 31, 2019, NCMEC responded that Cybertip 49677716 was related to some of the information I requested. NCMEC informed me that Cybertip 49677716 was sent to the Los Angeles Police Department (“LAPD”), Internet Crimes Against Children (“ICAC”) Taskforce for further investigation where it was subsequently assigned to Detective Brian Arias, a

LAPD ICAC Taskforce member and Deputy with San Bernardino County Sheriff's Department, for further investigation.

43. On or about November 3, 2019, I obtained a copy of Cybertip 49677716 from Detective Arias and learned that on or about May 17, 2019, Google reported to NCMEC that it discovered that one of its user accounts, registered with the name "SS" (the "SUBJECT GOOGLE ACCOUNT"), had seven images of suspected child pornography stored within its "Google Photos Infrastructure." Google reported that the SUBJECT GOOGLE ACCOUNT is registered with the phone number "909-492-5019" (the "SUBJECT PHONE NUMBER") and the email addresses SUBJECT EMAIL 1 and SUBJECT EMAIL 2. Additionally, Google reported that the SUBJECT EMAIL 1, and the SUBJECT PHONE NUMBER have both been verified by the account holder.

44. On or about November 5, 2019, I reviewed the 7 images that Google provided to NCMEC. They appear to depict the same prepubescent female. The images are described below:

a. The image titled "2019-04-03" depicts a nude prepubescent female, appearing to be under the age of 12 years old, laying on her back on top of a bedsheet that is with a pattern of pastel colored circles. There is a pillow with a pillowcase visible that has a purple butterfly on it. The child is using her hands to hold up both of her legs exposing her vagina and anus to the camera. The child's face is visible in the photo and she closely resembles the same preteen girl depicted in photos found on STEVENS's Facebook profile.

b. The image titled "2019-04-13" depicts what appears to be the same nude prepubescent female described above. In this particular photo, the nude child is laying on her stomach facing away from the camera. The child is laying on a multi-colored comforter (blue, purple and white) with a pattern of hearts and flowers printed on it. A white person's hand is seen pushing aside one of the child's legs exposing the child's vagina to the camera.

c. The image titled "report_123210111561297029579" depicts a prepubescent female laying on her back on top of a white sheet with blue and teal hearts printed on it. The child's legs are spread apart, and a white person's left hand is seen touching the child's buttocks exposing her vagina and anus to the camera. The camera is closely focused on the child's anus and vagina.

d. The image titled "report_8175760579594825736" depicts a close up of a prepubescent female's vagina. The child is on top of a white sheet with blue and teal hearts printed on it. The child's legs are spread apart, and a white person's right hand is seen touching the child's buttocks exposing her vagina to the camera. The camera is closely focused on the child's vagina.

e. The image titled "report_10812106022160631927" depicts a close up of a prepubescent female's vagina. The child is laying on the same multi-colored comforter as described above. The child is spreading her legs apart and with her hands is touching her pelvic area.

f. The images titled "report_4487638173229803249" and "report_12126718075593315792" are visually similar. They depict a nude prepubescent female standing in front of a toilet. The child appears to be wiping her vagina with toilet paper. The child's face is partially visible.

D. Additional Kik leads relating to STEVENS and the SUBJECT PREMISES

45. On November 6, 2019, I received additional Kik leads from C3 that Kik identified and forwarded to law enforcement in May 2019. I reviewed the leads and found that Kik provided a lead relating to the Kik user account "LOVER7210." Kik reported that PhotoDNA identified LOVER7210 as uploading two images of child pornography. Kik reported that LOVER7210 uploaded one of the images on May 8, 2019 at 6:30 p.m. (UTC) while utilizing SUBJECT IP 1. I reviewed the Subscriber Data Report and found the following relevant information indicative of STEVENS:

- a. LOVER7210 was created on April 15, 2019, following the closure of the SUBJECT KIK ACCOUNT.
- b. LOVER7210 was registered with the first name of "Kasey," which is part of STEVENS's middle name.
- c. LOVER7210 was registered with a date of birth of May 16, 1989, the same month and date of STEVENS's birthdate.
- d. Kik identified the devices associated with LOVER7210 as being an iPhone, the same as the SUBJECT KIK ACCOUNT.
- e. IP address logs provided by Kik show that between April 15, 2019 and May 9, 2019, LOVER7210 was accessed

approximately 560 times from the SUBJECT IP 1. Similarly, LOVER7210 was accessed from the SUBJECT IP 2 on approximately 25 instances. I also noticed that the account was accessed more than 150 times from IP addresses beginning with 99.203 which Sprint PCS previously identified as not maintaining logs for.

46. I reviewed the image that Kik reported LOVER7210 uploaded on May 8, 2019. The image depicts an infant laying on its back. The infant is wearing a onesie that has been unzipped exposing the infant's bare chest. A male adult's erect penis is exposed and is resting on the lips of the infant. The image is closely focused on the male adult's penis and the child's face and abdomen.

47. On November 7, 2019, I spoke with HSI personnel within C3 that are assigned to processing the leads from Kik. I was informed that C3 recently obtained additional leads from the RCMP. C3 personnel conducted a search within the leads for Kik users utilizing the SUBJECT IP 1. C3 found one lead within the recently obtained leads in which Kik identified the user "KASEYJ187," via PhotoDNA, as utilizing the SUBJECT IP 1 to upload a child pornography image on May 21, 2019.

48. C3 provided me the information provided by Kik and I reviewed its contents. I found that between May 24, 2019 and June 18, 2019, KASEYJ187 was accessed approximately 55 times from the SUBJECT IP 1. Additionally, the account was accessed five times from IP addresses beginning with 99.203 which Sprint PCS previously identified as not maintaining logs for. I reviewed the image that Kik reported KASEYJ187 uploaded on May

21, 2019. The image depicts an infant laying on their stomach on top of bedding that is grey in color with roses and flowers printed on it. The infant appears to be nude. A white adult person's hand is seen spreading open the buttocks of the infant exposing the infant's anus and vagina to the camera. The camera is closely focused on the child's buttocks and vagina area.

E. Surveillance of the SUBJECT PREMISES

49. On November 4, 2019, at approximately 9:30 a.m., I arrived at the SUBJECT PREMISES and parked on the street directly in front of the SUBJECT PREMISES. I saw parked in the carport of the SUBJECT PREMISES a sage Toyota Rav4 with California license plate number 8LYV053 (the "SUBJECT VEHICLE"). While parked in front of the SUBJECT PREMISES, I utilized my government issued smartphone and conducted a search for wireless internet networks being broadcasted in the area. Nine wireless networks were detected, all of which showed that they were password protected. One of the wireless networks was named "grimes 5G_Extnd." I was parked in front of the SUBJECT PREMISES for approximately 2 minutes before I continued driving and parked at the end of street. I conducted surveillance of the SUBJECT PREMISES for approximately 20 minutes before departing the location. During that time, I did not see anyone enter or depart the SUBJECT PREMISES.

50. Later that same day, I conducted searches for the registered owner of the SUBJECT VEHICLE within databases maintained by the DMV and learned that it is registered to Logan Grimes and Garrett Grimes at the SUBJECT PREMISES, and had a

vehicle identification number of JTMW1RFV2KJ014588. I conducted a search for vehicles registered to STEVENS which showed that no vehicles were registered to her.

51. On November 7, 2019, at approximately 8:45 a.m., SA Ramsey Korban conducted surveillance on the SUBJECT PREMISES. At the time of SA Korban's arrival, the SUBJECT VEHICLE was parked in the carport of the SUBJECT PREMISES. At approximately 9:05 a.m., SA Korban saw the SUBJECT VEHICLE pull out of the carport and exit the mobile home park. The SUBJECT VEHICLE proceed south on County Line Road and onto the 10-freeway traveling westbound. SA Korban followed the SUBJECT VEHICLE until it arrived and parked at San Bernardino Advanced Imaging located at 800 Highland Avenue, San Bernardino, California. SA Korban observed a female adult, appearing to be the same female depicted on STEVENS's California driver's license, exit from the driver's seat of the SUBJECT VEHICLE. SA Korban also observed a female minor, who appeared to be approximately 9 years old, exit the SUBJECT VEHICLE from the rear passenger door. The two then entered the San Bernardino Advanced Imaging building together.

52. On November 7, 2019, at approximately 10:15 a.m., I arrived at the SUBJECT PREMISES. I parked south of the SUBJECT PREMISES approximately 50 yards away. At approximately 10:20 a.m., I saw a white male adult, who appeared to be the same male depicted on Logan Grimes's California driver's license, exit the SUBJECT PREMISES. The male adult walked over to the south side of the SUBJECT PREMISES, unlocked the side gate and took two trash cans out. The male adult walked the two trash cans to a

collection of dumpsters located on the north side of the mobile home park. At approximately 10:40 a.m., I departed from the location.

VI. TRAINING AND EXPERIENCE ON CHILD PORNOGRAPHY INVESTIGATIONS

53. Based on my knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

a. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or 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.

b. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides, and/or drawings or other visual media. Child pornography collectors 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.

c. Collectors of child pornography almost always possess and maintain their "hard copies" of child pornography

material, that is, their pictures, films, videotapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location, and sometimes will keep them in several separate locations. Child pornography collectors typically retain pictures, films, photography, negatives, magazines, correspondence, books, tape recording, mailing lists, child erotica, and videotapes for many years.

d. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area, or on their person, if they are carrying a portable digital device, or in their vehicle. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

e. Child pornography collectors 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, address and telephone numbers of individuals with whom they have been in contact and who share the same interest in child pornography.

f. When collectors of child pornography distribute and receive child pornography through e-mail accounts or other internet communication platforms, they sometimes delete copies

of all such e-mails or correspondences to avoid detection after they have saved the files of child pornography to their computer, digital media, or other online storage service i.e.: external hard drives, thumb drives, and or cloud drive.

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

h. Collectors of child pornography frequently move files of child pornography from one digital device to different digital devices in an attempt to avoid detection. Collectors of child pornography frequently store their collections of child pornography on different digital devices for the increased storage space different digital devices offer over other devices, e.g., laptop computers typically have more storage space than cellphone or iPods.

i. Child pornography collectors rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. The known desire of such individuals to retain child pornography together with the sense of security afforded by using computers, provides probable cause to believe that computer images, especially child pornography and erotic nudity involving minors, will be retained by the collector indefinitely. These individuals may protect their illicit materials by passwords, encryption, and other

security measures. These individuals may also protect their illicit materials by saving it on movable media such as memory cards, memory sticks, CDs, DVDs, flash memory, thumb drives, and removable hard drives, which can be very small in size, including as small as a postage stamp, and easily secreted, or sent to third party image storage sites via the Internet.

VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES¹

54. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are

¹ As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously

develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

55. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

56. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress STEVENS's thumb and/or fingers on the device(s); and (2) hold the device(s) in front of STEVENS's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

57. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VIII. CONCLUSION

58. For all the reasons described above, there is probable cause to believe that the items listed in Attachments B-1 and B-2, which constitute evidence, fruits, and instrumentalities of violations of the TARGET OFFENSES will be found in the SUBJECT PREMISES and on STEVENS, as described in Attachments A-1 and A-2 of this affidavit.

Jonathan Ruiz, Special Agent
Homeland Security
Investigations

Subscribed to and sworn before
me on November __, 2019.

UNITED STATES MAGISTRATE JUDGE