

ORIGINAL

AO 91 (Rev. 11/82)

CRIMINAL COMPLAINT

UNITED STATES DISTRICT COURT		CENTRAL DISTRICT OF CALIFORNIA	
UNITED STATES OF AMERICA v. ARLAN WESLEY HARRELL		DOCKET NO.	FILED CLERK, U.S. DISTRICT COURT MAY 2 1 2017
		MAGISTRATE'S CASE NO.	

Complaint for violation of Title 18, United States Code, Section 2251(a), Production of Child Pornography

NAME OF MAGISTRATE JUDGE	UNITED STATES	LOCATION
HONORABLE JACQUELINE CHOOLJIAN	MAGISTRATE JUDGE	Los Angeles, California

DATE OF OFFENSE	PLACE OF OFFENSE	ADDRESS OF ACCUSED (IF KNOWN)
July 21, 2016, to April 22, 2017	Los Angeles County	11804 Atkinson Avenue, Hawthorne, California 90250

COMPLAINANT'S STATEMENT OF FACTS CONSTITUTING THE OFFENSE OR VIOLATION:

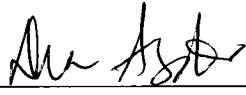
[18 U.S.C. § 2251(a)]

Between on or about July 21, 2016, and April 22, 2017, in Los Angeles County, within the Central District of California, and elsewhere, defendant ARLAN WESLEY HARRELL knowingly employed, used, persuaded, induced, enticed, and coerced a minor to engage in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2)(A), for the purpose of producing a visual depicting of such conduct, knowing and having reason to know that such visual depiction would be transported and transmitted using any means and facility of interstate and foreign commerce and in and affecting interstate and foreign commerce, and which visual depiction was produced and transmitted using materials that had been mailed, shipped, and transported in and affecting interstate and foreign commerce by any means, including by computer, and which visual depiction was actually transported and transmitted using any means and facility of interstate and foreign commerce and in and affecting interstate and foreign commerce

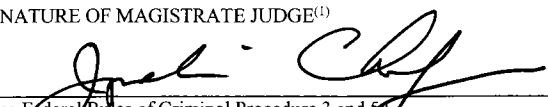
BASIS OF COMPLAINANT'S CHARGE AGAINST THE ACCUSED:

(See attached affidavit which is incorporated as part of this Complaint)

MATERIAL WITNESSES IN RELATION TO THIS CHARGE: N/A

Being duly sworn, I declare that the foregoing is true and correct to the best of my knowledge.	SIGNATURE OF COMPLAINANT	
	OFFICIAL TITLE	Special Agent – Homeland Security Investigations

Sworn to before me and subscribed in my presence,

SIGNATURE OF MAGISTRATE JUDGE ⁽¹⁾	DATE
	May 27, 2017

⁽¹⁾ See Federal Rules of Criminal Procedure 3 and 54

AFFIDAVIT

I, Diane Asato, being duly sworn, declare and state as follows:

I. INTRODUCTION

1. I am a Special Agent ("SA") with the United States Department of Homeland Security ("DHS"), Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI") in Los Angeles, California, and I have been so employed since June 2003. I am currently assigned to the HSI Los Angeles Child Exploitation Investigations Group ("CEIG"), where 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. §§ 2252(a) and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review various examples of child pornography in all forms of media, including computer media. I have also participated in the execution of numerous search warrants, many of which involved child exploitation and/or child pornography offenses.

2. Through my training and experience, I have become familiar with the methods used by people who commit offenses involving the sexual exploitation of children. My training and experience has given me an understanding of how people who commit offenses relating to the sexual exploitation of children use the Internet to facilitate and commit those offenses.

II. PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of:

a. a complaint and arrest warrant charging ARLAN WESLEY HARRELL ("HARRELL") with a violation of 18 U.S.C. § 2251(a), production of child pornography, from on or about July 21, 2016, and continuing to on or about April 22, 2017, in Los Angeles County, within the Central District of California, and elsewhere;

b. an application for a warrant to search the residence located at 11804 Atkinson Avenue, Hawthorne, California 90250, (the "SUBJECT PREMISES"), more fully described below and in Attachment A, which is attached hereto and incorporated herein by reference, and to seize evidence, fruits, and instrumentalities, as specified in Attachment B, which is also attached hereto and incorporated by reference, of violations of 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography); 18 U.S.C. § 2252A(a)(2) (distribution and receipt of child pornography); and 18 U.S.C. § 2251(a) (production of child pornography) (the "SUBJECT OFFENSES").

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from HSI Boston and HSI Philadelphia Special Agents and other law enforcement officials. This affidavit is intended to show merely that there is sufficient probable cause for the requested 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.

III. PREMISES TO BE SEARCHED

5. The SUBJECT PREMISES is a single story residence beige in color, with a brown roof and white trim. The SUBJECT PREMISES is located on Atkinson Avenue and the main entrance to the residence faces south towards 119th street. The numbers "11804" in black is affixed on the right side of the window located on the front of the house. Additionally, "11804" is also identified in black with a white background on the curb of the driveway. The SUBJECT PREMISES includes any parking spaces, garages, storage spaces, and appurtenances that are assigned to or associated with the main house located at 11804 Atkinson Avenue, Los Angeles, California 90250.

IV. ITEMS TO BE SEIZED

6. Based on the foregoing, I respectfully submit that there is probable cause to believe that the items listed in Attachment B, which constitute evidence of violations of the SUBJECT OFFENSES will be found at the SUBJECT PREMISES.

V. SUMMARY OF PROBABLE CAUSE

7. HSI Boston and Philadelphia, along with law enforcement abroad, have been investigating an online forum for trading child pornography since approximately October 2016. Foreign law enforcement recently arrested a suspect abroad (herein referred to as "FS1") who was producing child pornography offered on the forum. FS1 began cooperating with law enforcement and provided information about another individual active on the

forum under the user names of "Soole," "Fritters," and "Kronos." FS1 told investigators that he plays XBOX games with "Soole" and "Soole's" nickname on XBOX is "The War Titan." HSI Boston obtained a court order for subscriber information for the XBOX Live username "The War Titan" from May 23, 2016, to May 23, 2017. According to Microsoft, the gamer tag "The War Titan" was created on or about September 18, 2007, with a customer name listed as ARLAN HARRELL at the SUBJECT PREMISES.

8. Upon receiving the lead from HSI Boston, HSI Los Angeles reviewed images and videos of child pornography recovered from FS1's digital devices that investigators believe "Soole" posted to the forum. In an effort to identify the victims, I compared the children depicted in these images and videos with images found on the publicly available Facebook pages of HARRELL's parents. I was able to determine that a female toddler depicted in the child pornography images associated with "Soole" appeared to be the same minor as that depicted in multiple photographs posted to these Facebook pages. Additionally, agents were able to identify a movie theater depicted in some of the images "Soole" posted to the forum as a Cinemark Theater located in Los Angeles, California. According to record checks, HARRELL is employed by Cinemark.

9. Based on the foregoing, I believe that "Soole" and "The War Titan" are the same individual, and that this individual is HARRELL. I further believe that HARRELL used his minor female relative to produce child pornography, in violation of § 2251(a),

and that evidence of the SUBJECT OFFENSES will therefore be found at his residence, the SUBJECT PREMISES.

VI. BACKGROUND - DEFINITIONS, AND TRAINING AND EXPERIENCE

10. The following terms, as used in this affidavit, have the following meanings:

a. "Minor," "sexually explicit conduct," "visual depiction," "producing," and "child pornography" are defined as set forth in 18 U.S.C. § 2256.

b. "Child erotica" means materials or items that are sexually arousing to persons who have a sexual interest in minors, but that are not, in and of themselves, legally obscene, or do not necessarily depict minors in sexually explicit conduct.

c. "Computer" is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

d. "Computer server" or "server" is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system ("DNS") server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as

www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol address so the computer hosting the website may be located, and the DNS server provides this function.

e. "Internet" is defined as the worldwide network of computers – a noncommercial, self-governing network devoted mostly to communication and research with roughly 500 million users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university, employer, or commercial Internet Service Provider, which operates a host computer with direct access to the Internet.

f. "Internet Service Providers" ("ISPs") are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name (a user name or

screen name), an e-mail address, an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with the ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

g. "Internet Protocol Address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses can also be "static," if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

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

i. "Hyperlink" refers to an item on a webpage which, when selected, transfers the user directly to another location in a hypertext document or to some other webpage.

VII. STATEMENT OF PROBABLE CAUSE

A. BACKGROUND REGARDING NETWORK A AND WEBSITE A

11. On or about May 24, 2017, I received information from HSI Boston group supervisor Richard Sabatini, and HSI

Philadelphia Special Agent Emily Evans regarding an individual utilizing the user names "Soole," "Fritters," and "Kronos" who was seen on a forum¹ on an anonymous network, and on Wickr, a chatting application, discussing the sexual abuse of children.

12. In or about October 2016, HSI agents in Boston and Philadelphia became involved in an ongoing child pornography investigation. At the present time, this investigation involves multiple individuals, believed to be residing across the United States as well as abroad, who are members of an Internet-based website ("herein referred to as website A") that operates on an anonymous online network.

13. Website A is a forum on Network A that is dedicated to the sexual exploitation of children from birth to five years old. Website A is run by three unknown individuals that maintain Website A, approve members to become members of Website A, and provide guidance/support to members of Website A. Website A consists of several sections to include: News, Security/Technology, Boys, and Girls. The boy and girl sections are further broken down into age groups, pictures, and videos.

¹ The actual name of the forum is known to law enforcement. The forum remains active and disclosure of the name of the forum would potentially alert its members to the fact that law enforcement action is being taken against the forum, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the forum will be identified as "Website A."

14. In order to become a member of website A one must apply for membership by creating an account and uploading images/videos of child pornography that is then approved or disapproved by the administrators of Website A. Members that are approved must upload images/videos of child pornography once every 30 days to remain a member of Website A. Once approved members are assigned a "rank" that is based on the amount of participation on Website A, this includes the amount of child pornography they upload/share on the forum.

15. Website A operates on a network ("Network A")² available to Internet users who are aware of its existence. Network A is designed specifically to facilitate anonymous communication over the Internet. In order to access Network A, a user must install computer software that is publicly available, either by downloading software to the user's existing web browser, downloading free software available from the Network's administrators, or downloading a publicly-available third-party application. Using Network A prevents someone attempting to monitor an Internet connection from learning what sites a user visits and prevents the sites the user visits from learning the user's physical location. Because of the way Network A routes

² The actual name of Network A is known to law enforcement. Network A remains active and disclosure of the name of Network A would potentially alert its members to the fact that law enforcement action is being taken against Network A, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the network will be identified as "Network A."

communication through other computers, traditional IP identification techniques are not viable.

16. Websites that are accessible only to users within Network A can be set up within Network A, and Website A is one such website. Accordingly, Website A is not accessible through the traditional Internet. Only a user who has installed the appropriate software on the user's computer can access Website A. In order to access Website A, a user either has to know the exact web address or has to discover its exact web address from other servers on Network A that maintain indexes of known websites. Accessing Website A therefore requires numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon Website A without first understanding its content and knowing that its primary purpose was to view and distribute child pornography.

17. Network A's software protects users' privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the users' actual IP addresses, which could otherwise be used to identify a user.

18. Network A also makes it possible for users to hide their locations while offering various kinds of services, such as web publishing, forum/website hosting, or an instant messaging server. Within Network A itself, entire websites can be set up which operate in the same manner as regular public websites, with one critical exception – the IP address for the web server is hidden and is replaced with a Network-based web address. A user

can only reach such sites if the user is using the Network client and operating in Network A. Because neither a user nor law enforcement can identify the actual IP address of the web server, it is not possible to determine through public lookups where the computer that hosts the website is located. Accordingly, it is not possible to obtain data detailing the activities of the users from the website server through public lookups.

B. INVESTIGATION OF SUSPECT USER "SOOLE"

19. In or about October 2016, HSI Boston started investigating Website A as part of an ongoing undercover operation. As part of this undercover operation HSI Boston has identified numerous members of the forum as producers of child pornography. One such member observed by agents was user "Soole" aka "Fritters" aka "Kronos." During that time, HSI Boston Agents have downloaded numerous images and videos of child pornography of children ages approximately six months old to five years old. The individual using the screen name "Soole" has posted approximately one hundred and thirteen posts on Website A. These posts include:

July 31, 2016:

"When I post my work and see it has 1200 views and 1 comment and 3 thumbs up statistically that means that 1196 people did not like what I shared and should not continue with it because it is undesired"³

August 4, 2016:

"You can never have enough babies around !"

³ Based on my knowledge of Website A and my review of all of "Soole's" posts, I interpret "Soole's" reference to "his work" to mean the child pornography he has produced and posted to the forum.

November 3, 2016:

"For those of you who may not know me. I do not always post here but will forever remain on the site I still wish to attract more fellow producers and contributors to our community to a safe area and for this I needed to create a separate account because not everyone trust big name prods (feel intimidated) so this is the work of my other self. Also as a friendly warning to any who come to leak our VIP and Prod zone remember you never know who is on the other end of your computer screen if you leak or trade our material we will find out When we choose to share it is because we are kind so be thankful as lots of work go into producing and making stuff to share After you watch and fap to material and horniness is gone you can delete but we cannot delete from the internet so we live with the fear one day we make mistake and get caught so be thankful and not petty please we are all here to enjoy and fap to Happy Kids Any and all can be the same people so lets jsut have fun and follow the rules"

November 24, 2016:

"Im not gonna brag but I actually know this producer and I can say is a really nice person If you guys are nice maybe one day I will make an introduction Then again Im a little greedy sometimes so maybe not Take care enjoy stay safe"

December 2, 2016:

"Please be careful with who you trust my friends as my friend T****⁴ (say LEO are getting desperate and times are tough and we all need to be together easiest way to confirm someone is legitimate is to do a simple validation all it takes is one picture We are here for you all and in these times better we stick together if any issues or concerns arise we actively encourage you to contact members of administration and we will do the best to help you or clarify where is needed Sorry I know is in wrong section just wanted make a point is all I will disable preview as to not offend anyone - SOOLE"

December 28, 2016:

"I love how comfortable he is to be masturbated and he has a very cute penis also. I am sure now that all

⁴ The user name is known to law enforcement, but is redacted for purposes of this affidavit.

kids in asia know at least one pedo haha I may need to make a trip because they all seem so willing."

20. HSI Boston and HSI Philadelphia began investigating several individuals who were active members of Website A identified on Network A as sharing or offering to share child pornography images/videos. Since that time, foreign law enforcement has arrested an individual ("herein referred to as FS1") who was producing child pornography images/videos and sharing them with individuals in Website A and Wickr.⁵ FS1 has been cooperating with law enforcement and has provided the following information to law enforcement:

a. "Soole" along with four other members including FS1 are members of a group on Wickr. "Soole" recently sent four images of children in a public location to members in the wicker group.

b. I have reviewed the images that "Soole" shared in the Wickr group and determined that some of the images were taken at what appeared to be a Cinemark movie theater in Los Angeles, California.

21. I learned from SA Evans that during the foreign law enforcement's review of FS1's digital devices, foreign law enforcement discovered a folder on FS1's computer. FS1 informed foreign law enforcement that the content of the folder was sent by the group members of Website A via Wickr and were taken specifically for FS1, as recent as February 2017.

⁵ Wickr is an application designed to make detection from law enforcement more difficult. In fact, Wickr allows users to set an automatic delete time, so that messages automatically self-destruct/erase.

a. In addition, foreign law enforcement discovered images/videos in a folder labeled "Soole" for FS1's computer. The images/videos contained images of children being exploited, some of those images were taken as recently as April 2017.

b. FS1 stated that he plays XBOX games with "Soole" and "Soole's" nickname on XBOX is "The War Titan."

22. On or about May 23, 2017, HSI Boston obtained a court order for subscriber information for the Xbox Live username "The War Titan" from May 23, 2016, to May 23, 2017. According to Microsoft, the gamer tag "The War Titan" was created on or about September 18, 2007, with a customer name listed as ARLAN HARRELL at the SUBJECT PREMISES. The email account associated with the XBOX Live account was listed as "wildacexxtitan@gmail.com." Furthermore, IP address 172.113.97.151 ("the SUSPECT IP ADDRESS") was utilized to access the XBOX Live account from approximately November 22, 2013, to approximately May 23, 2017.

C. WEBSITE A POSTS BY "SOOLE"

23. SA Evans provided me with the chat logs along with video and images retrieved from Website A. I have reviewed the images/videos associated with "Soole" in Website A. The following is a summary of some of "Soole's" chats:

a. On or about April 14, 2017, user "Soole" posted:

i. "Had a little fun with my boy this past week and after a little thought and discussion we decided to proceed with our next step in exploration. There is nothing more special then when your boy makes the choice to give himself to you. For those lucky enough to share a moment like this with

your special friend or friends remember to cherish it always..... And dont forget to share XD Hope you all like enjoy and be safe P.S 2 Picks one before one after all in the same file 1Prev:.. . ."

ii. In addition, "Soole" posted a hyperlink titled, "![Image] (http://pixs.ru/showimage/CummyHolem_4674129_25881125.jpg)," which contained an image file titled "CummyHolem_4674129_25881125.jpg." This file consists of approximately 16 images of video thumbnails depicting what appears to be a pre-pubescent minor, with semen on his butt and anal area. An adult male's hand is seen spreading the minor's butt cheeks apart and exposing the anus.

24. On or about April 22, 2017, user "Soole" posted "Looks like I left a few things out sorry !..." Attached to this post, were five image file hyperlinks. Three of the five hyperlinks are described as follows:

a. "![Image] (http://felixxxboni3mk4a.onion/img/uploads/170422/Felixxx_225413_rSF_3FS.jpg)"- this image depicts a naked pre-pubescent minor boy laying on his back on a brown blanket with his legs apart exposing his penis. On the minor's stomach is a white card with the writing "Soole xfritters."

b. "![Image] (http://felixxxboni3mk4a.onion/img/uploads/170422/Felixxx_225536_ouE_4FS.jpg)"- this image depicts what appears to be the same minor boy in the previous image lying on the same brown blanket with his legs raised, exposing his penis and anal area. Next to the child's anus is the same white card with the writing "Soole xFritters."

c. "[Image] (http://felixxxboni3mk4a.onion/img/uploads/170422/Felixxx_225630_LAV_5FS.jpg)" -depicts what appears to be a minor boy bent on his knees exposing his anus. Resting on the child's leg is the same white card with the writing "Soole xFritters."

25. On or about May 25, 2017, a DHS summons was served on Time Warner Cable/Charter Communications requesting subscriber information relating to the user of the SUSPECT IP ADDRESS, which was tied to "The War Titan" for May 7, 2017, and May 23, 2017. According to Charter Communications, the SUSPECT IP ADDRESS was assigned to Arlan Harrell at the SUBJECT PREMISES. According to Charter Communications, the internet service date is listed as January 20, 2016, and the internet service is listed as currently active.

26. On or about May 24, 2017, Intelligence Research Specialist ("IRS") Nancy Bravo and SA Emily Evans conducted a Consolidated Lead Evaluation and Reporting ("CLEAR") records check for the residents residing at the SUBJECT PREMISES. According to the CLEAR, the following individuals come back to the SUBJECT PREMISES: ARLAN HARRELL, Avery Harrell, Ashton Russ, Philip Harrell, and Richetta Harrell are currently associated with the SUBJECT PREMISES. Based on my training and experience, I know that CLEAR is a report generated by Thomson Reuters, which is a company that consolidates public records, including addresses, driver licenses, property deed transfers, and corporate information, as well as some property records.

27. On or about May 24, 2017, IRS Bravo conducted record checks in the California Department of Motor Vehicles ("DMV") records check for ARLAN, Avery, Philip, Richetta Harrell, and Ashton Russ. The DMV records for ARLAN, Avery, Philip, Richetta Harrell, and Ashton Russ lists the SUBJECT PREMISES as their address. In addition, the following vehicles with California license plates are also registered to the SUBJECT PREMISES: A 2013 Dodge XXXX6J1 (Phillip or Avery Harrell); 2003 Infinity XXXX996 (Ashton Russ); 2008 Ford XXXX438 (ARLAN HARRELL); 2011 Dodge XXXX524 and 2017 Kia XXXX287 (Philip Harrell); and 2010 Mercedes XXXX234 (Richetta Harrell or Arianne Russ).

28. On or about May 24, 2017, SA My Bach obtained information from the Department of Social Services State of California, the department which registers daycare businesses. SA Bach learned that the SUBJECT PREMISES is registered as 24/7 daycare facility since December 6, 2016. Richetta is listed as the registrant of the daycare.

29. On or about May 25, 2017, SA My Bach, Elaine Kwong, and Forrest Silberstein conducted surveillance at the SUBJECT PREMISES. SA Kwong observed the following vehicle XXX524 in the driveway of the SUBJECT PREMISES. Additionally, SA Kwong observed the vehicles with license numbers XXX287 and XXXX438 parked on the street in front of the residence. SAs observed a woman and man appearing to be Richetta and Philip exit the SUBJECT PREMISES and depart the residence in separate vehicles.

30. Subsequently SA Kwong used a wireless internet device to identify wireless Internet services that were being

broadcasted publicly near the SUBJECT PREMISES. SA Kwong identified approximately five different secured wireless access points and no unsecured wireless access points. One of the secured wireless points being broadcasted was "Harrell's Clan804." Based on my training and experience, I know that a secured wireless access point would require a password or key code in order to access the wireless Internet service.

D. IDENTIFICATION OF MINOR CHILDREN EXPLOITED BY "SOOLE" IN WICKR AND WEBSITE A

31. On or about May 25, 2017, SA Evans provided SA Asato and IRS Bravo images and videos that were likely produced and distributed by "Soole" in Website A and Wickr. IRS Bravo reviewed the images and videos provided by SA Evans and determined that some of the children in the sexually explicit images and videos appeared to be relatives of HARRELL based on her review of the Facebook profiles of HARRELL's immediate family members.

32. The folder labeled "Daisy 2017," which was recovered from FS1's digital devices, contains a series of approximately 21 images depicting what appears to be the same female toddler ("Minor Victim 1"). The series progresses from the toddler being clothed to close ups of the toddler's vaginal area. Placed next to the minor in majority of the photos is a white card written in black ink with the word "Soole". The following is a description of two of the images:

a. Image titled "SD15.jpg" depicts a close up of the vaginal area of a prepubescent child approximately one year old.

The word "SOOLE<3" is typed on a white sheet of paper and is displayed on the upper portion of the image. The female child appears to be a relative of Harrell and appears to be the same female child who is on the Facebook pages of Philip and Kayla Harrell.

b. Image titled "SD16.JPG" depicts a close up of the vaginal area of a prepubescent child approximately one year old. The hand of an adult male which is partially blacked out is spreading the vaginal area of the female child. The word "Soole<3" is typed in small letters and is displayed on the child's thigh.

33. Based on my training and experience and my investigation of "Soole/Fritters/Kronos," I know that producers of child pornography like to mark their images and / or videos by displaying some type of identifier to show ownership. For example in this investigation, I believe that "Soole/Fritters/Kronos" are the user names associated with HARRELL and these monikers are depicted in the images described above to show HARRELL created and owned these images.

34. In addition, on or about May 25, 2017, SA Evans provided me with a MP4 video titled "Pee on my bed" which she received from foreign law enforcement. SA Evans informed me that the video was also retrieved from the digital devices of FS1. The video is approximately 18 seconds long and depicts what appears to be a female toddler who appears to be Minor Victim 1. Minor Victim 1 is lying on her back exposing her chest and vagina. The video focuses in on the girl urinating and an adult

hand is seen wiping the girl's vagina with a white cloth. While the video is focused on the vaginal area, the adult hand spreads the vagina area of the girl. The face of Minor Victim 1 is visible during this video.

35. I have also reviewed other videos recovered from FS1's digital devices that investigators believe to be produced by "Soole," including a video that shows the grey shoes of the individual who appears to be taking the video. In another video, I observed black, white, and grey shorts that also appear to the clothing of the individual taking the video. Finally, throughout all of these images and videos, I observed bedroom items such as sheets, blankets, and pillows that could be used to identify the location of the production of the video, as well as children's items such as toys and clothing. I also watched a video that appears to have been produced in a bathroom, which shows a red bath mat.

36. After reviewing the "Pee on my bed" video, I compared the face of Minor Victim 1 with images obtained from the Facebook pages of HARRELL's parents, Richetta and Philip Harrell,⁶ which were publicly available. For example, I reviewed an image posted to Richetta Harrell's Facebook page that depicts Richetta and Philip Harrell with several minor children. One of the minor children appears to be Minor Victim 1. Additionally, I reviewed an image posted to Philip Harrell's Facebook page on April 30,

⁶ I was able to determine that Richetta and Philip Harrell were HARRELL's parents from government record checks and a publicly available website for the California Birth Index.

2017, that appears to be Minor Victim 1, with the caption, "Today I'm 2yrs old . . . HappyBirthday pawpaw love you."

37. In addition, record checks with a government database indicate that Harrell has been employed with a Cinemark movie theater since August 2016. As referenced above, "Soole" posted some images of children (not sexually explicit) on Wickr that appear to have been taken at the Cinemark movie theater located in Los Angeles, California.

38. Therefore, I believe that the individual utilizing user name "Soole/Fritter/Kronos" is HARRELL who resides at the SUBJECT PREMISES.

VIII. TRAINING AND EXPERIENCE REGARDING INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

39. Because of the structure of Website A, Network A, and Wickr, it is possible for users to view and distribute images/videos of child pornography to their own computers or digital devices. However, as set forth below in detail, I know from my training and experience, and the training and experience of other law enforcement officers experienced in investigating crimes involving the sexual exploitation of children with whom I have had discussions, that people who have a sexual interest in children, as demonstrated by their chats in Website A, often possess and maintain images of child pornography to satisfy their sexual interest in children.

40. As set forth above, there is probable cause to believe that an individual at the SUBJECT PREMISES utilized Website A and Wicker to view and distribute produced child pornography. Based

on my training and experience, and the training and experience of other law enforcement officers experienced in investigating crimes involving the sexual exploitation of children with whom I have had discussions, I have learned that individuals who view multiple images of child pornography, including on web-based bulletin boards, are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children 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 in other visual media; or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children often 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. Individuals who have a sexual interest in children or images of children almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etcetera, in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and/or videotapes for many years.

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

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

have been in contact and who share the same interests in child pornography.

f. Individuals who access hidden and embedded child pornography-related bulletin boards, and other forums such as newsgroups and IRC chatrooms, are typically more experienced child pornography collectors. These individuals likely would have gained knowledge about such forums through online communications with other individuals who have a sexual interest in children or images of children.

g. Individuals who have a sexual interest in children or images of children 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.

41. Child pornography received via computer is extremely mobile. Through computer technology, digital files are easily reproduced and transported. For example, with the click of a button, images and videos containing child pornography can be put onto thumb drives so small that they fit onto a keychain. Just as easily, these files can be copied onto floppy disks or compact disks, and/or stored on iPods, Blackberries, or cellular telephones. Because someone at the SUBJECT PREMISES likely collects and values child pornography, which is easily-stored and duplicated, there is probable cause to believe that evidence of a child pornography collection will be found in the SUBJECT PREMISES.

IX. AUTHORIZATION FOR NIGHT SERVICE AND NO-KNOCK ENTRY

42. This affidavit also seeks authorization for night service and no-knock entry in order to ensure officer and victim safety and prevent any destruction of the digital evidence.

43. Based on my training and experience, I know that individuals actively trading child pornography on highly secure online networks, such as Network A used for Website A, frequently discuss the use of encryption methods. I also know that many encryption methods can be employed incredibly rapidly. For instance, certain encryption software programs will encrypt an entire volume of a digital device with one key stroke. Once a piece of digital media is encrypted, it may be impossible for law enforcement to retrieve any evidence from it. I also know from my own experiences executing child exploitation search warrants that there are a number of rapid techniques a defendant can use to destroy evidence, including placing the digital devices in a bucket of acid, or destroying the devices with a dumbbell or a firearm.

44. Here, there are particular reasons to be concerned with the latter form of destruction. On May 25, 2017, HSI Intelligence Research Specialist Nancy Bravo advised me that she discovered approximately 22 firearms were registered to the occupants of the SUBJECT PREMISES based on a registered weapons check.

45. This also poses significant safety concerns during the execution of the search and arrest warrants. On May 25, 2017, I spoke with a member of the Homeland Security Special Response

Team, a highly trained tactical unit, who advised me that a nighttime, no-knock entry would allow his team to execute the warrants more safely, given the number of firearms likely located at the residence and given the potential that minor victim(s) could be residing there.

46. Accordingly, in order to preserve the evidence and ensure officer and victim safety during execution of the warrants, this affidavit seeks authorization for night service and no-knock entry.

X. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

47. 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 telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that data in digital form can be stored on a variety of digital devices and that during the

search of a premises it is not always possible to search digital devices for digital data for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. There are so many types of digital devices and software programs in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover "hidden," erased, compressed, encrypted, or password-protected data. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is essential to conducting a complete and accurate analysis of data stored on digital devices.

c. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage

space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 or more gigabytes are now commonplace. Consequently, just one device might contain the equivalent of 250 million pages of data, which, if printed out, would completely fill three 35' x 35' x 10' rooms to the ceiling. Further, a 500 gigabyte drive could contain as many as approximately 450 full run movies or 450,000 songs.

d. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, i.e., space on a hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space, for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed on the Internet are often automatically downloaded into a temporary directory or cache. The browser typically maintains a fixed

amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently downloaded or viewed content. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment. Recovery also can require substantial time.

e. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processing, picture, and movie files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital 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 contained on the digital devices are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive image as a whole. Digital data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently

used. Web browsers, e-mail programs, and chat programs often store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

f. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data on a digital device is not segregable from the digital device. Analysis of the digital device as a whole to demonstrate the absence of particular data requires specialized tools and a controlled laboratory environment, and can require substantial time.

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

XI. CONCLUSION

48. Based on the foregoing, I believe there is probable cause:

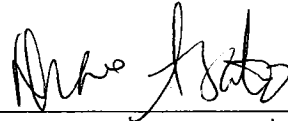
a. to find that HARRELL produced child pornography, in violation of 18 U.S.C. § 2251(a), from on or about July 21, 2016, and continuing to on or about April 22, 2017, in Los Angeles County, within the Central District of California, and elsewhere; and

b. to believe that evidence, fruits, and instrumentalities of violations 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography); 18 U.S.C. § 2252(a)(2) (distribution and receipt of child pornography); and 18 U.S.C. § 2251(a) (production of child pornography), as described above and in Attachment B of this affidavit, will be found in a search of the SUBJECT PREMISES, as further described above and in Attachment A of this affidavit.

XII. CERTIFICATION REGARDING REVIEW OF CHILD PORNOGRAPHY BY U.S. MAGISTRATE JUDGE

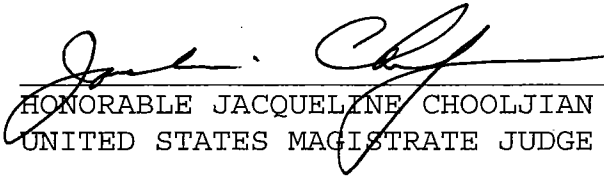
49. The image described in paragraph 32(b) was shown to the Honorable Jacqueline Chooljian, U.S. Magistrate Judge, on May 27, 2017, for her review. See United States v. Perkins, No. 15-50035 (9th Cir. Mar. 13, 2017) (warrant applications based on alleged child pornography under the 18 U.S.C. § 2256(2)(A)(v) standard – that is, including “the lascivious exhibition of the

genitals or pubic area" – should "provide copies of the images for the magistrate's independent review"). The image was then placed in a sealed envelope, signed by both the affiant and the Honorable Jacqueline Chooljian. The envelope containing this image will remain sealed and will be maintained in a secure location at HSI Long Beach offices.



Diane Asato, Special Agent
Homeland Security
Investigations

Subscribed to and sworn before me
this 27th day of May, 2017.⁷



HONORABLE JACQUELINE CHOOLJIAN
UNITED STATES MAGISTRATE JUDGE

⁷ This signature certifies review of the image described in paragraph 32(b).