UNITED STATES DISTRICT COURT

DISTRICT OF CONNECTICUT

AFFIDAVIT IN SUPPORT OF A COMPLAINT AND ARREST WARRANT

I, Michael J. Syrax, being duly sworn, depose and state as follows:

BACKGROUND OF AFFIANT

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since 2002. My experience as an FBI Special Agent has included the investigation of violent crimes, counterintelligence, counterterrorism, and weapons of mass destruction. Since 2018, I have been assigned to investigate violent crimes against children and have participated in multiple investigations involving child exploitation, trafficking of child pornography, and online enticement of minors. I received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer crimes, and various other criminal law procedures. I am a federal law enforcement officer who is engaged in enforcing federal criminal laws, and I am authorized by the Attorney General to request search and arrest warrants.

2. I am currently investigating an individual named ROBERT ECCLESTON, who has utilized the mobile application Kik, which is described below, using profile names "My Name" and "hartfordctguy," to commit violations of 18 U.S.C. § 2252A(a)(2) (distribution of child pornography) (the "TARGET OFFENSE").

3. This affidavit is being submitted in support of a criminal complaint and an arrest warrant authorizing the arrest of ROBERT ECCLESTON, who is believed to reside in Canton, Connecticut, at an address known to me, for violations of the TARGET OFFENSE. It is also being submitted in support of a search warrant for an Apple iPhone X bearing serial number F17VQCX0JCL9, associated with phone number (860) 202-4565, and belonging to

ECCLESTON (hereafter, the "TARGET DEVICE"), which is further described in Attachment A, for evidence, fruits, and instrumentalities of the crimes of distribution of child pornography and possession of child pornography, as further described in Attachment B.

4. The statements contained in this affidavit are based in part on information provided by other members of local, state, and federal law enforcement and my own investigation, including personal observations, documents, and other investigative materials that I have reviewed, as well as on my training and experience as a Special Agent with the FBI. Since this affidavit is being submitted for the limited purpose of obtaining a criminal complaint, an arrest warrant, and a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that ECCLESTON committed the TARGET OFFENSE and that evidence of ECCLESTON's commission of the TARGET OFFENSE and of possession of child pornography will be found on the TARGET DEVICE.

RELEVANT STATUTES

5. Title 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly distributing any child pornography, as defined in 18 U.S.C. § 2256(8), when such child pornography was mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

6. The following definitions apply to this Affidavit:

a. "OCE" is an Online Covert Employee who is an individual certified and trained by the FBI to engage in online undercover investigations using a false persona.

b. "Minor," as used herein, is defined by 18 U.S.C. § 2256(1) to mean any person under the age of eighteen years.

c. "Child Pornography" is defined by 18 U.S.C. § 2256(8) to mean any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Sexually explicit conduct" means actual or simulated (i) sexual intercourse, including genital/genital, oral/genital, anal/genital, or oral/anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person. 18 U.S.C. § 2256(2)(A).

e. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. Traditionally, IP addresses were either dynamic, meaning an Internet service provider ("ISP") assigns a different unique number to a computer every time it accesses the Internet, or static, meaning an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. Generally, the static IP addresses were assigned by those companies who offered "broadband" Internet service, such as through cable or digital subscriber line ("DSL"), whereas "dial up" companies would assign their users dynamic addresses. Now, however, as a greater number of American Internet users choose broadband Internet service, many of these users are being assigned what may be colloquially referred to as a "sticky dynamic IP address" or a "sticky IP." A sticky IP is a dynamically assigned IP address that does not change often. The address leases are usually set to long periods and simply renewed upon expiration.

BACKGROUND ON KIK

7. Kik is a free smartphone messenger application that, according to its Law Enforcement Guide, "lets users connect with their friends and the world around them through chat." Kik is owned and operated by Media Labs, Inc., a company headquartered in Santa Monica, California. The Law Enforcement Guide states that users can "send text, pictures,

videos and more – all within the app."[1] To use the Kik application, a user downloads the application to a mobile phone, computer, or other digital device via a service such as iOS App Store or the Google Play Store. *Id.* Once the Kik application is downloaded and installed, the user creates an account and a unique username that cannot be changed. Once the user has created an account, the user is able to locate others via a search feature.

8. Kik allows users to communicate via group or direct messages. Kik users can share, upload, and receive messages, images, and videos to specific users or groups. Kik users create display names and usernames when they register an account. Users can change their display name at will, but the username remains the same for the life of the account. Kik does not validate user information at the time an account is created.

9. Based on my training and experience using Kik in an undercover capacity, I know that Kik users are 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 items, such as photos or videos, to the group as a whole or to any other user. These groups are frequently created with a group name containing a hashtag (#) that is easily identifiable or searchable by keyword.

[1] Available at https://lawenforcement.kik.com/hc/en-us/articles/360039841472-Law-Enforcement-Guide (last accessed December 7, 2020).

PROBABLE CAUSE

A. FBI Field Office "A" Investigation

10. On or about October 15, 2020, an FBI OCE working in an FBI Field Office outside of Connecticut (Field Office "A")[2] was a member of two Kik user groups, Kik Public Group 1 and Kik Public Group 2, and observed an individual utilizing a Kik account with the display name "My Name" and a username "hartfordctguy" in both of the groups. The FBI OCE was aware the groups catered to individuals who have a sexual interest in children. Kik user "hartfordctguy" joined the group on August 15, 2020, at approximately 6:35 AM Eastern Time.

11. Between August 16, 2020, and September 15,2020, the individual using the Kik account "hartfordctguy" posted images and videos believed to be child pornography in both groups. The individual also posted images and videos of pornography depicting adults and others who appear to be minors but whose age is difficult to determine. Descriptions of some of the child pornography images are below. Only thumbnails of the images and videos were retrievable due to technical issues.

Item #[3]	Date & Time	File name ending in	Description
1	08/16/2020 7:41:32 AM ET	b2376fc7c0ef	A very close-up image of what appears to be an infant or toddler's vagina.
2	08/17/2020 7:52:43 AM ET	c1e326c445cd	An image of a young female, who appears to be a minor, who is nude from the waist down with her legs spread open exposing her vagina.
3	08/18/2020 6:23 AM ET	4341cf64dffc	An image of a video known to the writer to be a video of a young female, likely less than 12 years old who is

[2] In order to preserve ongoing investigations being conducted by FBI Field Offices, those offices' locations and the Kik groups they are investigating have been anonymized. The true office locations and Kik group names are known to me.

[3] The column "Item #" is used below for reference within this affidavit only and has no correlation to the data for the actual image.

			nude from the waist down. The child has her legs spread and a dog is licking the child's vagina.
4	08/18/2020 4:33:53 PM ET	5b12ee53e8a8	One image of a nude prepubescent female lying supine with her legs spread open. Her vagina is clearly visible in the image. Another person who is off camera is holding a white device that is pressed against the child's vagina.
5	08/28/2020 6:01:33 PM ET	03aac5ece9d0	An image of a shirtless female who appears to be less than 12 years old in front of an erect penis. The female's face is at the same level as the penis and her right hand is grasping the penis.
6	09/02/2020 9:00:25 AM ET	0d494515e27d	One image of a nude female who appears to be under 18 years old lying on the floor with her legs spread exposing her vagina. The female is touching her vagina with her right hand.
7	09/03/2020 7:56:11 PM ET	dfae5aec85db5	One image of a young female, who appears to be under 18 years old, sitting in front of a nude male whose penis is erect. The female has her left hand on the penis and her mouth on the top of the penis.
8	09/10/2020 4:32:32 PM ET	090212d3fa18	One image of a nude prepubescent female who appears to be less than 12 years old. The child is sitting on the floor with her legs spread open exposing her vagina.
9	09/11/2020 4:56:17 PM ET	6d0ad52dd084	One image of a nude male lying on a couch. A nude female whose body type appears to be a child is lying on top of the male. They are kissing and the female's left hand is touching her buttocks.
10	09/11/2020 5:03:08 PM ET	1f05d49b06a7	One image of a nude prepubescent female, likely less than 12 years old, sitting on the floor with her legs spread open exposing her vagina.

11	09/15/2020 6:44:23 AM ET	db403570076f	One image of a nude prepubescent female, likely less than 12 years old, exposing her breasts and vagina.

12. While chatting in the group, Kik user "hartfordctguy" asked another member who purported to be an 11-year-old female if she wanted to "cum to my house." In addition, "hartfordctguy" asked the purported 11-year-old female to private message him pictures of her "cunny." The affiant believes "cunny" to be a slang reference for vagina. The user who purported to be an 11-year-old female was not an FBI OCE. I am unaware whether the user was actually an 11-year-old female.

13. On October 5, 2020, MediaLab, Inc., responded to an administrative subpoena issued by the FBI requesting subscriber information and IP logs for "hartfordctguy." The subpoena returns contained IP address information dated September 7 through 16, 2020. Kik only provides the last 30 days of IP addresses for an account. The returns contained the following relevant account information:

- First Name: My
- Last Name: Name
- Email: bob.eccleston@sbcglobal.net
- Username: hartfordctguy
- Device: iPhone
- IP Address: 32.208.209.172
- Registration Date: 11/09/2019

14. The report showed approximately 2,479 connections to Kik from "hartfordctguy" between September 7 and 16, 2020. Of those connections 2,392 or 96%, came from IP address 32.208.209.172.

15. The FBI queried the IP address 32.208.209.172 through the American Registry for Internet Numbers ("ARIN"). The query revealed the IP address is registered to Frontier Communications. On October 13, 2020, the FBI issued an administrative subpoena to NorthWest

Fiber LLC on behalf of Frontier Communications. According to the subpoena response, during the time the individual with Kik username "hartfordctguy" utilized the IP address, it was assigned as follows:

- Subscriber Name: Susan Eccleston
- Address: [redacted] Canton, Connecticut 06019
- Phone Number: [redacted]
- E-mail: [redacted]

16. The FBI reviewed open-source information for Susan Eccleston and found Robert Eccleston is married to Susan Eccleston. Open-source searches indicate Robert Eccleston is employed as a Victim Services Advocate at Hartford Superior Court, Hartford, Connecticut.

17. As of November 30, 2020, according to records provided by Kik, the username "hartfordctguy" did not have an active account on Kik. The FBI submitted an administrative subpoena to Kik in an effort to determine if any Kik accounts were actively using IP address 32.208.209.172, known to be ECCLESTON's residence. Kik responded to the FBI that they did not have the ability to query their system for accounts associated with a particular IP address.

B. FBI Field Office "B" Investigation

18. Unrelated to the FBI Field Office "A" investigation, an FBI OCE in FBI Field Office "B," which is outside of Connecticut, also became aware of Kik user "hartfordctguy." During their observation of "hartfordctguy," OCEs observed him post child pornography to a Kik chat group ("Kik Public Group 3," the identity of which is known to me) that was focused on child pornography.

19. A review of the information collected by FBI Field Office "B" revealed "hartfordctguy" was an "administrator" for Kik Public Group 3. This meant "hartfordctguy" had the ability to vet and validate new members to the group. Through my experience as an OCE on various social media platforms including Kik, I know one of the methods to vet new members is

to request that they distribute child pornography, either to the group or through direct message to the group administrator.

20. Information collected by FBI Field Office "B" showed an interaction in September 2020 wherein "hartfordctguy," in what appears to be his capacity as an administrator for Kik Public Group 3, texts another member "send me 3 taboo vids to stay." Based on my training and experience as an OCE, I know that the word "taboo" is generally understood, in groups that cater to individuals who have a sexual interest in children, to mean child pornography, and that "vids" means "videos." Thus, I believe that "hartfordctguy" asked another member of the group to send him three videos of child pornography in order to remain a member of the group. The next post by "hartfordctguy" on or about September 16, 2020,[4] was an image of a completely nude child who appeared to be less than 15 years old. The child's vagina was visible in the image. The image had a mark indicating it was from LS Magazine, which was a Ukrainian child pornography magazine that operated as a modeling agency.[5] The very next post, on or about September 16, 2020, indicated "hartfordctguy" removed a member from Kik Public Group 3.

21. The OCE also described three videos posted by"hartfordctguy" in Kik Public Group 3:

Item #	Date & Time	Description
12	08/22/2020 5:54 AM CST	A video of a nude prepubescent female approximately 4 to 6 years old who was lying supine. An adult female wearing a prosthetic penis penetrated the child's anus.

[4] Due to the limitations of the Kik application interface and the format of the evidence provided to FBI New Haven, a precise date cannot be provided. Specifically, the Kik interface does not display the date and time for every post. The approximate date was established by using the date "hartfordctguy" created the account and adding the number of days on Kik displayed on the "hartfordctguy" profile page.

[5] The photographs published by LS Magazine included child pornography and child erotica.

13	09/15/2020 6:51 PM CST	A video of a prepubescent female approximately 6 to 9 years old wearing white and pink underpants performing oral sex on a nude male. The male then engages in sexual intercourse with the female.
14	09/15/2020 6:51 PM CST	A close-up video of what appears to be a prepubescent male who appears to be approximately 7-10 years old wearing red and white striped underwear. The male engages in vaginal intercourse with an adult female.
15	08/17/2020[4] 9:38 AM CST	A video of a young female less than 12 years old who appears to be asleep. The child's vagina is exposed. A male ejaculates on the pubic area of the child and a finger smears the ejaculate onto the labia of the child and then onto the child's mouth.

22. I reviewed digital evidence of the other images and videos posted in August and September 2020 by "hartfordctguy" to Kik Public Group 3. Based on my training and experience, a total of eleven videos, including the four described above in Items 12-15, and two still images, constitute child pornography. Additionally, Item 15 above appears to be the full video associated with the thumbnail described in Item 1 in paragraph 11 above. There were also three other videos provided by FBI Field Office B that appear to be the full child pornography videos associated with thumbnail images provided by FBI Field Office A (these thumbnail images are not listed in the table in paragraph 11).

23. On September 21, 2020, MediaLab, Inc., responded to an administrative subpoena issued by FBI Field Office "B" requesting subscriber information and IP logs for "hartfordctguy." The subpoena returns contained IP address information dated August 22, 2020, through September 16, 2020. The returns contained the following relevant information:

- First Name: My
- Last Name: Name
- Email: bob.eccleston@sbcglobal.net
- Username: hartfordctguy
- Device: iPhone
- Date of Birth: [redacted]1964

- Account Registration: 11/09/2019

20. The date of birth provided by Kik associated with "hartfordctguy" is Robert ECCLESTON's date of birth. In addition, the report showed approximately 7,037 connections to Kik from "hartfordctguy" between August 22, 2020, and September 16, 2020. Of those connections 6,732, or 96%, came from IP address 32.208.209.172, the same IP address referenced above that is assigned to Susan Eccleston at [redacted] in Canton, Connecticut.

C. Kik Referral to Royal Canadian Mounted Police and United States Homeland Security Investigations

21. On December 1, 2020, the FBI requested the National Center for Missing and Exploited Children (NCMEC) query their system for any references to IP address 32.208.209.172. NCMEC informed the FBI of matches related to a lead sent to the Department of Homeland Security, Homeland Security Investigations ("HSI"), in addition to the FBI Field Office "A" investigation noted above. Kik was previously headquartered in Canada, so leads generated during the time it was headquartered there were handled through the Royal Canadian Mounted Police ("RCMP") and referred to HSI. The FBI contacted HSI and learned HSI had received a tip from the Royal Canadian Mounted Police (RCMP) regarding Kik username "mowglihartford" in or about July 22, 2019. The report was provided to the RCMP by Kik based on their internal hash value matching system, which alerts Kik to possible child exploitation images based on a unique number assigned to the image. Upon review of the image, HSI agents determined that the image provided by Kik was child erotica and not child pornography. As a result, no further investigation was conducted by HSI. I reviewed the image and agree the image is not child pornography.

22. According to documents provided to HSI by RCMP and forwarded to the FBI, the Kik user "mowglihartford" uploaded the child erotica image during a chat session on July 20,

2019, at 12:22:35 UTC from IP address 32.208.209.172. This is the same IP address noted above that resolves to the Eccleston residence and used by Kik user "hartfordctguy."

23. Subscriber data provided by Kik to HSI and forwarded to the FBI revealed the following relevant account information:

- Username: mowglihartford
- First Name: Mowgli
- Last Name: Hartford
- Email: deletedbykik.27110.mowglihartford@gmail.com[6] (deactivated_unconfirmed)
- Username: mowglihartford

24. Kik provided records of IP connections with the "mowglihartford" user dated June 20, 2019, through July 20, 2019. There were approximately 1,872 connections to Kik by user "mowglihartford." Of those, approximately 1,619, approximately 86%, were from IP address 32.208.209.172, the same IP address noted above that resolves to the Eccleston residence and used by Kik user "hartfordctguy."

25. The FBI served Google, Inc with a subpoena for subscriber information regarding mowglihartford@gmail.com. The account was created on June 3, 2019, from IP address 198.177.8.109. The subscriber name provided to Google was "mowgli mowgli." There were no IP logs or recovery email addresses associated with this email account.

26. The FBI queried ARIN for 198.177.8.109 to determine the ISP for the address. ARIN results indicated the IP address 198.177.8.109, which was used to create the mowglihartford@gmail.com account, is registered to the State of Connecticut Judicial Branch,

[6] Based on my training and experience, I know that the "deleted by kik" reference in the email address means the account was deleted by Kik. I am aware companies, like Kik, will delete user accounts for violating the company's terms of service. The email account associated with the mowglihartford Kik username was likely mowglihartford@gmail.com without any of the other text noted above.

99 East River Drive, 6th Floor, East Hartford, Connecticut. A search of the internet for 99 East River Drive, East Hartford, Connecticut revealed it is the address for the State of Connecticut Judicial Branch Information Technology Unit. As noted elsewhere in this affidavit, ECCLESTON is employed as a Victim Advocate for the Hartford Superior Court.

D. Robert Eccleston Uses Mowgli as a Pseudonym

27. The FBI conducted an open-source search for Robert ECCLESTON and found posts attributed to Robert ECCLESTON on a publicly-available "Facebook page called "Acoustic Awakening," which appears to be related to a musical hobby of ECCLESTON's. Images of the person on the Facebook page appear to be identical to the photo contained in the Connecticut driver's license for Robert ECCLESTON. On the "Acoustic Awakening" Facebook page, Robert ECCLESTON made several references to "Mowgli" during a trip to Greece in 2018 for an event called "Hang Out Naxos 2018." Based on the context of the posts, "Mowgli" is likely a pseudonym for Eccleston or perhaps the name of his handpan, which is a drum-like instrument. A search of the internet revealed there is an event held in Naxos, Greece for music featuring handpans, an instrument Robert ECCLESTON plays.

E. Information about the TARGET DEVICE

28. The email address bob.eccleston@sbcglobal.net was used in the subscriber information for Kik account "hartfordctguy." This same email address is used for other accounts linked to Robert Eccleston.

29. As noted above, the FBI located a Facebook account for ECCLESTON's music hobby that included an email address of acousticawakening@gmail.com. Google provided that this email address is registered to Bob Eccleston and was created on December 7, 2012, from IP address 198.177.8.136. The recovery email address is bob.eccleston@sbcglobal.net. The

recovery SMS telephone number is 860-202-4565, the phone number associated with the TARGET DEVICE. There was no IP address log record information associated with the account. The "Terms of Service" IP for the creation of the account is registered to the State of Connecticut Judicial Branch.

30. The FBI served an order under 18 U.S.C. § 2703(d) to Apple for accounts related to ECCLESTON. Apple provided results for an account with the email address bob.eccleston@sbcglobal.net, telephone number 860-202-4565 (the phone number associated with the TARGET DEVICE), and address of [redacted] Canton, Connecticut. The Apple records also provided that the TARGET DEVICE bears serial number F17VQCX0JCL9 and an International Mobile Equipment Identifier ("IMEI") of 359407086763210. Based on my training and experience reviewing records from Apple, I know that the last digit "0" is a check digit so the actual device number ends in 1.

31. The service provider for telephone number 860-202-4565 is Cingular Wireless/AT&T. The FBI served an administrative subpoena on AT&T. AT&T responded with the following information: The subscriber for the telephone number is Susan M. Eccleston of [redacted] Canton, Connecticut. The telephone number is listed as active from 07/21/2007-Current. The username is Bob Eccleston of [redacted] Canton, Connecticut. The service start date was 07/21/2007. The contact home email address is listed as bob.eccleston@sbcglobal.net.

32. AT&T also provided data related to the cellular device information for telephone number 860-202-4565. The cellular telephone is described as an Apple iPhone X with an IMEI of 35940708676321 (the TARGET DEVICE).

33. Based on my training, experience, and research, I know that the TARGET DEVICE has capabilities that allow it to serve as a wireless telephone, a digital camera, a portable media player, and a GPS navigation device. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

34. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

35. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the TARGET DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the TARGET DEVICE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium 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).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw

conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

36. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant. I request that the warrant be deemed executed once the contents of the TARGET DEVICE have been extracted through the computer-assisted medium and that further analysis of the TARGET DEVICE be permitted at any time thereafter.

CONCLUSION

37. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe, and I do believe, that between August 16 and September 15, 2020, in the District of Connecticut and elsewhere, Robert ECCLESTON committed violations of 18 U.S.C. § 2252A(a)(2) (distribution of child pornography). Therefore, I request authorization for a criminal complaint and arrest warrant for ECCLESTON for the violation listed above.

38. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe, and I do believe, that the TARGET DEVICE will contain evidence, fruits, and instrumentalities of ECCLESTON's distribution of child pornography and possession of child pornography. Accordingly, I respectfully request that a search warrant issue for the TARGET DEVICE.

MICHAEL SYRAX
Digitally signed by MICHAEL SYRAX
Date: 2020.12.10 14:27:39 -05'00'

MICHAEL J. SYRAX
Special Agent
Federal Bureau of Investigation

Subscribed and sworn before me by telephone this 10th day of December, 2020.

Sarah A. L. Merriam, U.S.M.J.
Digitally signed by Sarah A. L. Merriam, U.S.M.J.
Date: 2020.12.10 18:35:47 -05'00'

HON. SARAH A. L. MERRIAM
UNITED STATES MAGISTRATE JUDGE

Attachment A
Property to be Searched

The property to be searched is an Apple iPhone X cellular telephone bearing serial number F17VQCX0JCL9 and an International Mobile Equipment Identifier ("IMEI") of 35940708676321 (the "TARGET DEVICE"). The TARGET DEVICE is believed to be associated with phone number (860) 202-4565 and is believed to be used by Robert ECCLESTON.

ATTACHMENT B
Items to Be Seized

All records on the TARGET DEVICE that relate to violations of 18 U.S.C. § 2252A(a)(2) (concerning distribution of child pornography) and 18 U.S.C. § 2252A(a)(5)(B) (concerning possession of child pornography) between the dates of July 19, 2019, and present, involving Robert ECCLESTON, including:

1. Records in any form, including group or private messages, with any person through Kik concerning the sexual exploitation of minors;

2. Records and information relating to images, videos, or other media of suspected child pornography, minors engaged in sexually explicit conduct, or child erotica;

3. Communications with, involving, or concerning any Online Covert Employees of the FBI, whose identities are known to the Affiant;

4. Records, contacts, and communications, including private messages, with any member of Kik Public Groups 1, 2, and 3, the true names of which are known to the Affiant.

5. Records and information relating to the existence or former existence of sites on the Internet or publications, including LS Magazine, that contain child pornography or that cater to those with an interest in child pornography;

6. Records and information relating to membership in online groups, clubs, or services that provide or make accessible child pornography to members; and

7. Evidence indicating the user of the "mowglihartford" and "hartfordctguy" Kik accounts and the email accounts bob.eccleston@sbcglobalnet, mowglihartford@gmail.com, and acousticawakening@gmail.com.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review. The warrant shall be deemed executed once the contents of the TARGET DEVICE have been extracted through the computer-assisted medium and further analysis of the TARGET DEVICE is permitted at any time thereafter.