

FILED IN OPEN COURT

1/17/2020

CLERK, U. S. DISTRICT COURT  
MIDDLE DISTRICT OF FLORIDA  
JACKSONVILLE, FLORIDA

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

United States of America  
v.  
REECE CHRISTOPHER DEPEW

Case No.

3:20-mj- 1028-JRK

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of June 21, 2019 in the county of Duval in the  
Middle District of Florida, the defendant(s) violated:

Code Section

18 U.S.C. § 2252(a)(2)

Offense Description

Knowing distribution of child pornography over the internet

This criminal complaint is based on these facts:

See attached.

Continued on the attached sheet.

Complainant's signature

Daniel Moxley, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 1-17-20

Judge's signature

James R. Klindt, U.S. Magistrate Judge

Printed name and title

City and state: Jacksonville, Florida

AFFIDAVIT

I, Daniel Moxley, being duly sworn, state as follows:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since July 2017. I am currently assigned to the Jacksonville, Florida Division of the FBI, where I conduct a variety of investigations, including those involving the sexual exploitation of children. Prior to this assignment, I was employed as an Intelligence Analyst and Management and Program Analyst for the FBI for approximately 7 years. I have Bachelor's Degrees in Economics and Political Science. I have received law enforcement training from the FBI Academy at Quantico, Virginia. A substantial portion of my duties are dedicated to investigating cases involving crimes against children under the auspices of the FBI's "Innocent Images" National Initiative. Since becoming a Special Agent, I have worked with experienced Special Agents who also investigate child exploitation offenses. In the performance of my duties, I have investigated and assisted in the investigation of matters involving the solicitation for, possession, collection, distribution, production, receipt, and transportation of depictions of child pornography. I have been involved in searches of residences pertaining to the possession, distribution, collection, production, and/or transportation of child pornography through the execution of search warrants.

2. I have investigated and assisted in the investigation of criminal matters involving the sexual exploitation of children that constituted violations of 18 U.S.C.

JMK

§§ 2251, 2252, and 2422. As a federal agent, I am authorized to investigate and assist in the prosecution of violations of laws of the United States, and to execute search warrants and arrest warrants issued by federal and state courts.

3. The statements contained in this affidavit are based on my personal knowledge, as well as on information provided to me by experienced Special Agents and other law enforcement officers and personnel. This affidavit is being submitted for the limited purpose of establishing probable cause for the filing of a criminal complaint, and I have not included each and every fact known to me concerning this investigation. I have set forth the facts that I believe are necessary to establish probable cause to believe that REECE CHRISTOPHER DEPEW has committed a violation of 18 U.S.C. § 2252(a)(2), that is, knowing distribution of child pornography over the internet.

4. I make this affidavit in support of a criminal complaint against REECE CHRISTOPHER DEPEW, that is, on or about June 21, 2019, in the Middle District of Florida and elsewhere, REECE CHRISTOPHER DEPEW did knowingly distribute visual depictions, that is, using any means and facility of interstate and foreign commerce by any means, that is, by computer via the internet, when the production of the visual depictions involved the use of minors engaging in sexually explicit conduct, and the visual depictions were of such conduct, in violation of 18 U.S.C. § 2252(a)(2).

5. On January 16, 2020, I applied for and obtained a federal search warrant for the residence located at 10870 John Randolph Drive, Jacksonville, Florida 32257, believed to be occupied by REECE CHRISTOPHER DEPEW and others. I was the affiant for the affidavit in support of the application for this search warrant, and I am familiar with the facts contained therein. A certified copy of the application and affidavit for this search warrant is attached as Exhibit A, and the facts and information contained therein is hereby incorporated by reference herein. This warrant authorized the search of this residence for fruits, evidence, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and/or 2252A, that is, transportation, receipt, distribution, possession, and access with intent to view child pornography. This search warrant was issued by United States Magistrate Judge James R. Klindt in Case No. 3:20-mj-1027-JRK.

6. On January 17, 2020, at approximately 6:50 a.m., I, together with other FBI agents and law enforcement personnel, executed this search warrant at the residence located at 10870 John Randolph Drive, Jacksonville, Florida 32257.

7. REESE CHRISTOPHER DEPEW was located inside the residence, and was asked to step outside while the residence was cleared for officer safety. I approached him for a possible interview. DEPEW agreed to talk to me and FBI SA Jonathan MacDonald inside SA MacDonald's FBI government vehicle that was parked outside the residence.

8. I introduced myself as a Special Agent and presented my badge and credentials. I informed DEPEW that he was not under arrest and asked him he would like to sit in the front passenger seat of Special Agent MacDonald's vehicle to speak to me, to which he agreed. I sat in the driver seat of the vehicle and SA MacDonald sat in the back seat. I again told DEPEW that he was not under arrest and was free to exit the vehicle at any time. I also told DEPEW that he did not have to speak to me if he did not want to and did not have to answer all of the questions I asked him. I told DEPEW that a search warrant was being executed at his residence. DEPEW again agreed to talk to us and provided, in substance, in summary, and among other things, the following information:

(a) DEPEW has lived at the current residence with his mother, father and other family members since April 2019. DEPEW graduated from high school and can read, write, and understand English.

(b) DEPEW uses the Internet for social media, e-mail, and online gaming. DEPEW uses social media sites such as, Facebook, Twitter, Instagram, and Snapchat. DEPEW uses social media to direct message about "what is going on with my life." DEPEW plays online gaming with other individuals he knows and some he doesn't know. DEPEW uses the private chat feature while playing online games.

(c) DEPEW is very knowledgeable about computers and knows how they operate. DEPEW mostly uses his laptop computer in his bedroom to access the Internet and social media. In the past, DEPEW has used private messaging applications, such as KiK Messenger, to talk with others about sex who are over 18 years old. DEPEW stated the dark web has “creepy stuff you can’t imagine” including “CP,” which he clarified meant child pornography. DEPEW added that he “reports” every time he sees child pornography on social media. DEPEW stated that he has not used a cellular phone for the past two years.

(d) In addition to other social media applications, DEPEW stated he has used MeWe since 2018. DEPEW uses MeWe to communicate with others in the private chat feature. DEPEW admitted using MeWe account “Android 18” and registered the account with e-mail address “lolilover013198@gmail.com.”

(e) DEPEW admitted to using MeWe account “Android 18” to view and distribute child pornography with others over the Internet. DEPEW was shown several images of child pornography and admitted to distributing them to another MeWe user in June 2019, via the private chat feature. DEPEW stated he distributed at least 10 images of child pornography during a private chat session. DEPEW stated he downloaded the images from a website on the Internet, but could not recall the name of the website.

JRS

(f) I showed DEPEW the image titled "Screen Shot 2019-06-26 at 11.59.30 AM.png" that is described in the affidavit in support of the search warrant for his residence (see Exhibit A), and he admitted downloading, masturbating to this image in private, and then distributing it through the MeWe application. This is a color image of a female infant lying on her back. The infant's shirt is raised above her stomach and she is not wearing any pants or a diaper, fully exposing the infant's vagina, making it the focal point of the image. An adult penis is pressed against the infant's vagina and the tip of the adult's penis is slightly penetrating the infant's vaginal opening.

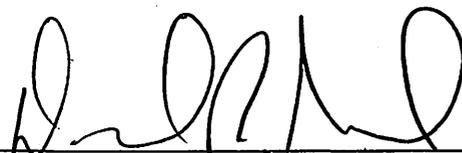
(g) Next, I showed DEPEW the image titled "Screen Shot 2019-06-26 at 11.59.16 AM.png" that is described in the affidavit in support of the search warrant for his residence (see Exhibit A), and he admitted to downloading, masturbating to the image in private, and then distributing it through the MeWe application. This is a color image of a prepubescent female child, based on her child-sized torso and lack of any pubic hair, lying flat on her back. The child's shirt and jacket is pulled up over her abdomen and she is not wearing any pants or underwear, fully exposing the child's vagina, making it the focal point of the image. There is a white fluid-like substance, which appears to be semen, present on the child's vaginal area and waist.

(h) Although DEPEW stated he did not know any of the children depicted in the images that he distributed, he stated he knew child pornography was “illegal” and “wrong.” DEPEW stated his involvement with child pornography has gone on for years, and that he has “tried to stop,” and “can’t control” himself.

9. After the conclusion of the interview of DEPEW, I contacted Assistant United States Attorney D. Rodney Brown, who authorized me to arrest DEPEW for knowing distribution of child pornography. Shortly thereafter, I placed DEPEW under arrest.

10. Based upon the foregoing facts, I have probable cause to believe that on or about June 21, 2019, in the Middle District of Florida and elsewhere, defendant, REECE CHRISTOPHER DEPEW, did knowingly distribute visual depictions using any means and facility of interstate and foreign commerce by any means, that is, by computer via the internet, when the production of the visual depictions involved the

use of minors engaging in sexually explicit conduct, and the visual depictions were of such conduct, in violation of 18 U.S.C. § 2252(a)(2).

  
\_\_\_\_\_  
DANIEL MOXLEY, Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me this 17<sup>th</sup> day of January, 2020, at Jacksonville, Florida.

  
\_\_\_\_\_  
JAMES R. KLINDT  
United States Magistrate Judge

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

COPY

for the Middle District of Florida

In the Matter of the Search of (Briefly describe the property to be searched or identify the person by name and address)

residence located at 10870 John Randolph Drive, Jacksonville, Florida 32257 more fully described in Attachment A

Case No. 3:20-mj- 1027-JRK

APPLICATION FOR A SEARCH WARRANT

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

residence located at 10870 John Randolph Drive, Jacksonville, Florida 32257 more fully described in Attachment A located in the Middle District of Florida, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

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

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

The search is related to a violation of:

Table with 2 columns: Code Section (18 U.S.C. §§ 2252(a) and 2252A) and Offense Description (Distribution, receipt, transportation, possession of and access with intent to view child pornography).

The application is based on these facts:

See attached affidavit

- [x] Continued on the attached sheet. [ ] Delayed notice of \_\_\_ days (give exact ending date if more than 30 days: \_\_\_ ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Handwritten signature of Daniel Moxley

Applicant's signature

Daniel Moxley, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 1-16-20

Handwritten signature of James R. Klindt

Judge's signature

James R. Klindt, United States Magistrate Judge

Printed name and title

City and state: Jacksonville, Florida

I CERTIFY THE FOREGOING TO BE A TRUE AND CORRECT COPY OF THE ORIGINAL CLERK OF COURT UNITED STATES DISTRICT COURT MIDDLE DISTRICT OF FLORIDA BY: [Signature] DEPUTY CLERK

**ATTACHMENT A**

**PREMISES TO BE SEARCHED**

The premises to be searched is a single family residence located at 10870 John Randolph Dr., Jacksonville, Florida 32257, and within a community referred to as "Carter Hall." John Randolph Drive is the first street on the left of the main entrance to the Carter Hall community, and this main entrance is located on Marilyn Anne Drive just off Clydesdale Drive West. The residence located on the east side of John Randolph Drive and is the second house south of the intersection with Marilyn Anne Drive. The residence is a single story, tan-colored building with white accent trim, and a three-car garage. There is a stone archway leading up to the front door of the residence. The front door appears to be constructed of wood and glass. The handle on the front door appears to be made of brass and is on the left side of the door, which appears to be inward opening. On the exterior of the residence, there is a sign that reads "10870" affixed over the center of the garage. The rear of the residence faces east toward Clydesdale Drive and there is no fence surrounding the property. There is a screened-in patio at the rear of the residence with a glass sliding door that leads into the interior of the residence. There are green bushes and other vegetation around the perimeter of the residence.

*JRS*

**ATTACHMENT B**

**DESCRIPTION OF ITEMS TO BE SEARCHED AND SEIZED**

1. Any and all computer(s), computer hardware, computer software, electronic storage media (including any and all disk drives, compact disks, flash drives, cellular telephones, "smart" phones such as an Apple iPhone, electronic tablets such as an Apple iPad, digital cameras and/or memory cards, or any other device capable of electronic storage of data and/or images), computer-related documentation, computer passwords and data-security devices, videotapes, video-recording devices, video-recording players, and video display monitors that are or may be used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography or child erotica.

2. Any and all computer software, including programs to run operating systems, applications, such as word processing, graphics, and communications programs peer to peer software, that may be or are used to: visually depict child pornography (any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2) or child erotica, display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess or receive child pornography or child erotica.

*JFK*

3. Any and all notes, documents, records, or correspondence, in any format and medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

5. Any and all diaries or address books containing names or lists of names and addresses of individuals who have been contacted by use of the computer(s) or by other means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means (including the United States Mail or computer) any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

7. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

8. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

9. Any and all notes, documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an internet service provider.

11. Any and all records, documents, invoices and materials, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

12. Any and all cameras, film, videotapes or other photographic equipment capable of being used to produce, manufacture, store and/or conceal visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

13. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means (including the United States Mail or computer) any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

14. Any and all documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and

electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

15. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

16. Any and all documents, records, or correspondence, in any format or medium (including envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files), pertaining to the identity of any and all owners and/or users of any computers, computer media and any electronic storage devices discovered in the premises and capable of being used to produce, manufacture, store and/or conceal visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

17. Any documents, records, programs or applications relating to the existence of wiping, data elimination, and/or counter-forensic programs (and associated data) that are designed to delete data from the subject computers and computer media.

**AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT**

I, Daniel Moxley, being duly sworn, hereby state as follows:

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since July 2017. I am currently assigned to the Jacksonville, Florida Division of the FBI, where I conduct a variety of investigations, including those involving the sexual exploitation of children. Prior to this assignment, I was employed as an Intelligence Analyst and Management and Program Analyst for the FBI for approximately 7 years. I have Bachelor's Degrees in Economics and Political Science. I have received law enforcement training from the FBI Academy at Quantico, Virginia. A substantial portion of my duties are dedicated to investigating cases involving crimes against children under the auspices of the FBI's "Innocent Images" National Initiative. Since becoming a Special Agent, I have worked with experienced Special Agents who also investigate child exploitation offenses. In the performance of my duties, I have investigated and assisted in the investigation of matters involving the solicitation for, possession, collection, distribution, production, receipt, and transportation of depictions of child pornography. I have been involved in searches of residences pertaining to the possession, distribution, collection, production, and/or transportation of child pornography through the execution of search warrants.

2. I have investigated and assisted in the investigation of criminal matters involving the sexual exploitation of children that constituted violations of 18 U.S.C. §§ 2251, 2252, and 2422. As a federal agent, I am authorized to investigate and

JMK

assist in the prosecution of violations of laws of the United States, and to execute search warrants and arrest warrants issued by federal and state courts.

3. The statements contained in this affidavit are based on information I obtained from my own personal observations, my personal knowledge, training, and experience, and from information directly provided to me by other law enforcement officers and personnel. This affidavit is being submitted for the limited purpose of establishing probable cause and securing a search warrant, and 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 contraband, fruits, instrumentalities, other items illegally possessed and evidence of violations of Title 18, United States Code, Sections 2252 and/or 2252A, are present in the location to be searched.

4. I am requesting authority to search the residence specifically identified in Attachment A, which includes the physical structure, as well as any computer and computer media and electronic storage devices located therein. I also request to seize any and all items listed in Attachment B as instrumentalities, fruits, and/or evidence of criminal activity specified herein.

**STATUTORY AUTHORITY**

5. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors. Based upon my training and experience, as well as

*JLK*

conversations with other experienced law enforcement officers, computer forensic examiners, and federal prosecutors, I know the following:

a. 18 U.S.C. § 2252(a) in pertinent part prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing or accessing with intent to view any visual depiction of minors engaging in sexually explicit conduct using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mails.

b. 18 U.S.C. § 2252A(a) in pertinent part prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any child pornography, as defined in 18 U.S.C. § 2256(8), using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer.

c. 18 U.S.C. § 2252(a)(1) prohibits a person from knowingly transporting or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mails, any visual depiction of minors engaging in sexually explicit conduct.

Under 18 U.S.C. § 2252(a)(2), it is a federal crime for any person to knowingly receive or distribute, by any means including by computer, any visual depiction of minors engaging in sexually explicit conduct using any means or facility of interstate or foreign commerce or that has been mailed or shipped or transported in or affecting interstate or foreign commerce. That section also makes it a federal crime for any

JJK

person to knowingly reproduce any visual depiction of minors engaging in sexually explicit conduct for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails. Under 18 U.S.C. § 2252(a)(4), it is also a crime for a person to knowingly possess or knowingly access with intent to view, one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been mailed, or have been shipped or transported using any means or facility of interstate or foreign commerce or in and affecting interstate or foreign commerce, or which were produced using materials which have been mailed or so shipped or transported, by any means including by computer.

d. 18 U.S.C. § 2252A(a)(1) prohibits a person from knowingly mailing, transporting, or shipping using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography. 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly receiving or distributing any child pornography that has been mailed or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer. 18 U.S.C. § 2252A(a)(3) prohibits a person from knowingly reproducing child pornography for distribution through the mails or in or affecting interstate or foreign commerce by any means, including by computer. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any book, magazine, periodical, film, videotape, computer disk,

JRK

or other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer.

### DEFINITIONS

6. The following definitions apply to this Affidavit:

a. "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, in and of themselves, illegal or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child pornography," as used herein, includes the definitions in 18 U.S.C. §§ 2256(8) and 2256(9) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct). See 18 U.S.C. §§ 2252 and 2256(2).

c. "Visual depictions" include undeveloped film and videotape, data stored on computer disk or by electronic means which is capable of conversion

into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in permanent format. See 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person. See 18 U.S.C. § 2256(2).

e. "Computer," as used herein, 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, arithmetic or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict

access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), personal digital assistants (PDAs), multimedia cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

i. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware,

software, or other programming code. A password (a string of alpha numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Digitally coded data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "boobytrap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet and is associated with a physical address. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) may assign a unique and different number to a computer at different times that it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

k. "Wireless telephone" (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of

capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device. Many wireless telephones are minicomputers or “smart phones” with immense storage capacity and connectivity capability.

l. A “digital camera” is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

m. A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives.

This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

### COMPUTERS AND CHILD PORNOGRAPHY

7. Based upon my training and experience, as well as conversations with other experienced law enforcement officers and computer forensic examiners, I know that computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. In the past, child pornography was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and significant skill to develop and reproduce the images. There were definable costs involved with the production of pornographic images, and to distribute these images on any scale required significant resources and significant risks. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public and/or law enforcement. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

8. The development of computers has radically changed the way that child pornographers manufacture, obtain, distribute and store their contraband. Computers basically serve five functions in connection with child pornography: access, production, communication, distribution, and storage.

9. Child pornographers can now convert paper photographs taken with a

traditional camera (using ordinary film) into a computer readable format with a device known as a scanner. Moreover, with the advent, proliferation and widespread use of digital cameras, images and videos can now be transferred directly from a digital camera onto a computer using a connection known as a USB cable or other device. Digital cameras, as well as "smart" phones such as the Apple iPhone, have the capacity to store images and videos indefinitely, and memory storage cards used in these cameras are capable of holding hundreds of images and videos. 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, that is, the hard disk drive used in home computers has grown tremendously within the last several years. These hard disk drives can store hundreds of thousands of images at very high resolution.

11. The World Wide Web of the Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

12. Collectors and distributors of child pornography frequently use online resources to retrieve and store child pornography, including services offered by Internet portals such as Yahoo!, Hotmail, and Google, among others. The online services allow a user to set up an account with a remote computing service that

provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

13. As is the case with most digital technology, communication by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or saving particular website locations in, for example, "bookmarked" files. Digital information, images and videos can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). Often, a computer will automatically save transcripts or logs of electronic communications between its user and other users that have occurred over the Internet. These logs are commonly referred to as "chat logs." Some programs allow computer users to trade images while simultaneously engaging in electronic communications with each other. This is often referred to as "chatting," or "instant messaging." Based upon my training and experience, as well as conversations with other law enforcement officers and computer forensic examiners, I know that these electronic "chat logs" often have great evidentiary value in child pornography investigations, as they can record communication in transcript form, often show the date and time of such communication, and also may show the dates and times when images of child

pornography were traded over the Internet. In addition to electronic communications, a computer user's internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained on a computer for long periods of time until overwritten by other data.

#### SEARCH AND SEIZURE OF COMPUTER SYSTEMS

14. Based upon my training and experience, as well as conversations with other experienced law enforcement officers, I know that searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (e.g., hard drives, compact disks ("CDs"), diskettes, tapes, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on

the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system, which includes the use of data search protocols, is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis. Based on my training and experience, as well as conversations with other law enforcement officers and computer forensic examiners, I know that computer forensic techniques can often recover files, including images and videos of child pornography, that have long been "deleted" from computer media by a computer user.

#### **CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS**

15. Based on my experience, training, and conversations with other experienced agents who investigate cases involving the sexual exploitation of children, I know that certain common characteristics are often present in individuals

who collect child pornography. I have observed and/or learned about the reliability of these commonalities and conclusions involving individuals who collect, produce and trade images of child pornography. Based upon my training and experience, and conversations with other experienced agents who investigate cases involving the sexual exploitation of children, I know that the following traits and characteristics are often present in individuals who collect child pornography:

a. Many individuals who traffic in and trade images of child pornography also collect child pornography. Many individuals who collect child pornography have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by sexually explicit depictions of children.

b. Many individuals who collect child pornography also collect other sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. Many of these individuals also collect child erotica, which may consist of images or text that do not meet the legal definition of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.

c. Many individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. This contact also helps these individuals to

rationalize and validate their deviant sexual interest in children and associated behavior. The different Internet based vehicles used by such individuals to communicate with each other include, but are not limited to, Peer-to-Peer (P2P), email, email groups, bulletin boards, Internet Relay Chat Rooms (IRC), newsgroups, instant messaging, and other similar vehicles.

d. Some individuals who collect child pornography maintain books, magazines, newspapers and other writings (which may be written by the collector), in hard copy or digital medium, on the subject of sexual activities with children as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals often do not destroy these materials because of the psychological support that they provide.

e. Some individuals who collect child pornography often collect, read, copy or maintain names, addresses (including email addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange, or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

f. Many individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect them from discovery, theft, or damage. These individuals view their

sexually explicit materials as prized and valuable materials, even as commodities to be traded with other like-minded individuals over the Internet. As such, they tend to maintain or "hoard" their visual depictions of child pornography for long periods of time in the privacy and security of their homes or other secure locations. These individuals may protect their illicit materials by passwords, encryption, and other security measures; save it on movable media such as 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 send it to third party image storage sites via the Internet. Based on my training and experience, as well as my conversations with other experienced law enforcement officers who conduct child exploitation investigations, I know that individuals who possess, receive, and/or distribute child pornography by computer devices using the Internet often maintain and/or possess the items listed in Attachment B.

16. As stated in substance above and based upon my training and experience, as well as my conversations with other experienced law enforcement officers, I know that individuals who collect and trade child pornography often do not willfully dispose of their child pornography collections, even after contact with law enforcement officials.

17. Based on my training and experience, I also know that, with the development of faster Internet download speed and the growth of file-sharing networks and other platforms through which individuals may trade child pornography, some individuals also have been found to download, view, and then

delete child pornography on their computers or digital devices on a cyclical and repetitive basis. However, as referenced above, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices using forensic tools. Furthermore, even in instances in which an individual engages in a cycle of downloading, viewing, and deleting images, a selection of favorite images involving a particular child or act is often maintained on the device.

18. Based on my training and experience, I know that within the last several years, individuals who have a sexual interest in minor children have used the internet and internet-enabled devices with increasing frequency to make contact with and attempt to establish relationships with potential child victims. These individuals may perceive that the internet provides some degree of anonymity and safety from prosecution. Because more and more children are using the internet and internet enabled devices, these individuals potentially expose more and more child victims to online sexual exploitation. These individuals may contact potential child victims through social networking websites or applications ("apps") such as Facebook and Twitter, or may engage in online conversations with children through text messaging and email. During these online conversations, photographic images and links to internet websites can be easily exchanged between the individual and the targeted child. Based on my training and experience, I know that when such an individual uses text messaging, email, or other websites to have online contact with children, the Internet-enabled device used, whether it is a computer, a cellular telephone, a

*JMM*

“smart” phone such as an “iPhone,” or a tablet such as an “iPad,” often saves and maintains evidence of such contacts. This evidence can often be extracted and examined by a trained forensic examiner.

### MEWE APPLICATION INFORMATION

19. The following information has been provided to me by other experienced law enforcement officers and also comes from online research that I have conducted, as well as from my training and experience. MeWe is an online social networking application (“app”) allowing individual and group chatting capabilities, as well as online cloud storage of files, including image and video files. It is available in versions for iOS and Android devices, as well as versions for Macintosh (Apple) and Windows desktop versions. MeWe officially launched in 2016 and may be found on the Internet at [www.mewe.com](http://www.mewe.com). This website advertises the MeWe app as “inspired by trust, control, and love for social media users” and “Engineered with privacy-by-design.” MeWe is a social network which “emphasizes social sharing where people can be their true, authentic selves.” The service provides newsfeeds, private and group online chatting, private and open groups, following pages, disappearing content, a camera with GIF creation, next-gen voice messaging, secret encrypted chats, a personal social cloud, custom group profiles, and 2,800 emojis. Users can post text and images to what the app refers to as their “Home Feed.” MeWe is free for members with the option to purchase additional upgrades to include extra storage, live voice and video calling, custom emojis and stickers, MeWe pages, and overlays. The personal cloud provided to users is called “My

Cloud," which can be used to organize content and provide the user with an interactive dashboard to control everything the user has posted or shared, making it easy to delete or re-share materials.

20. Based on my training and experience, as well as conversations with other more experienced law enforcement officers, I have learned that the MeWe app platform may be used for illegal activity, including the trading and solicitation of child pornography, because of the high degree of anonymity that is afforded to users during the use of the MeWe application.

**FACTS ESTABLISHING PROBABLE CAUSE**

21. I make this affidavit in support of a search warrant for the Subject Location that I believe to be currently occupied by DIANA LYNN DEPEW, RAY CLIFTON DEPEW JR., REECE CHRISTOPHER DEPEW, PATRICIA MOUNGER DEPEW, and a minor female. This affidavit is based upon information provided to me both verbally and in written documentation from other law enforcement officers and personnel, as well as through investigation that I personally conducted as set forth herein. I have personally observed the residence, and it appears as set forth in Attachment A.

22. The FBI is investigating the individuals residing at 10870 John Randolph Dr., Jacksonville, Florida 32257 as potential suspects for using one or more computers, smart phones, and computer media at this residence to commit violations of Title 18, United States Code, Sections 2252 and 2252A, which prohibit the transportation, receipt, distribution, possession, and access with intent to view

child pornography, that is, visual depictions of minors engaging in sexually explicit conduct as defined in Title 18, United States Code, Section 2256.

23. On October 30, 2019, I reviewed an investigative lead based on CyberTip report 51222603 (C.T. 51222603) that was submitted to the National Center for Missing and Exploited Children (NCMEC). Based on my training and experience, I know that NCMEC receives Cyber Tips from individuals and business entities regarding the possible sexual exploitation of children. I reviewed C.T. 51222603 and learned, among other things, the following:

- a. On June 26, 2019, Mary Strong, a MeWe representative, submitted C.T. 51222603 to NCMEC regarding the MeWe user, "Android 18", uploading 13 images of child pornography on June 21, 2019. Based on the file names of the images sent to NCMEC, Strong took screen captures of the images uploaded by "Android 18" and attached them to C.T. 51222603. According to the information submitted by Strong, MeWe user "Android 18" signed up for the account using e-mail account "lolilover013198@gmail.com."
- b. NCMEC staff reviewed the 13 child pornography images uploaded by the user "Android 18" and confirmed that two of those images have been previously viewed and categorized by NCMEC as "apparent child pornography."
- c. On August 14, 2019, an administrative subpoena and two year non-disclosure agreement was served to Sgrouples, Inc., d/b/a MeWe, to

provide information pertaining to the MeWe user "Android 18." On August 16, 2019, results of the subpoena listed the account name as "Android 18", the e-mail address as "lolilover013198@gmail.com," the registration date as June 21, 2019, and the last login date as June 26, 2019.

- d. On August 14, 2019, an administrative subpoena and two year non-disclosure order was served to Google, Inc., pertaining to the email address "lolilover013198@gmail.com." On August 16, 2019, results of the subpoena listed the account registration date as June 21, 2019. The IP address used to register and access the account was 2601:341:200:d0d:45b3:79aa:91e5:e584. The name listed on the account was "Android 18."
- e. On August 27, 2019, an administrative subpoena was served to Comcast requesting identifying information for the subscriber of IP address 2601:341:200:d0d:45b3:79aa:91e5:e584 on June 21, 2019. Comcast responded on the same day and listed the subscriber of the account that used IP address 2601:341:200:d0d:45b3:79aa:91e5:e584 on June 21, 2019 as "Diana Depew," with a service address as 10870 John Randolph Dr., Jacksonville, Florida 32257. The telephone number listed on the account was 678-910-3290 and start of service date was May 2, 2019.

24. On October 30, 2019, I reviewed the 13 child pornography images uploaded to MeWe by “Android 18,” and I observed at least one prepubescent child engaged in sexually explicit conduct in each of the 13 images. At least one of the images involved infants and/or toddlers engaged in sexually explicit conduct. Since the child pornography provided to NCMEC were screen captures, the original file titles and MD5 hashes of child pornography were not captured. Descriptions of some of the images of child pornography uploaded by the user “Android 18” and captured by MeWe that I observed are as follows:

TITLE: “Screen Shot 2019-06-26 at 11.59.30 AM.png”

MD5 HASH: 598cfb95b80b4075b83fe9c27032aed3

DESCRIPTION: A color image of a female infant lying on her back.

The infant’s shirt is raised above her stomach and she is not wearing any pants or a diaper, fully exposing the infant’s vagina, making it the focal point of the image. An adult penis is pressed against the infant’s vagina and the tip of the adult’s penis is slightly penetrating the infant’s vaginal opening. Based on my training and experience, I have probable cause to believe that this image depicts a prepubescent minor engaged in sexually explicit conduct, that is, the genital-genital sexual intercourse, and therefore constitutes child pornography pursuant to Title 18, United States Code, Section 2256.

TITLE: “Screen Shot 2019-06-26 at 11.59.16 AM.png”

MD5 HASH: 489f61f317dfe9283fcc86212a0ea216

**DESCRIPTION:** A color image of a prepubescent female child, based on her child-sized torso and lack of any pubic hair, lying flat on her back. The child's shirt and jacket is pulled up over her abdomen and she is not wearing any pants or underwear, fully exposing the child's vagina, making it the focal point of the image. There is a white fluid-like substance, which appears to be semen, present on the child's vaginal area and waist. Based on my training and experience, I have probable cause to believe that the image depicts a prepubescent minor engaged in sexually explicit conduct, that is, the lascivious exhibition of her genitalia, and therefore constitutes child pornography pursuant to Title 18, United States Code, Section 2256.

**TITLE:** "Screen Shot 2019-06-26 at 11.59.42 AM.png"

**MD5 HASH:** 9a8e35a1ef4a41b05666731e97537815

**DESCRIPTION:** A color image of a prepubescent female, based on her small size and child-like facial features, with blonde hair and wearing a white shirt. There appears to be a tan-colored couch or chair in the background. The child is facing an adult male who is placing his penis in the child's mouth. The adult male is using his left hand to hold his penis into the child's mouth. The adult male has a tattoo on his forearm. Based on my training and experience, I have probable cause to believe that this image depicts a prepubescent minor engaged in sexually explicit conduct, that is, oral-genital

*Handwritten signature*

sexual intercourse, and therefore constitutes child pornography pursuant to Title 18, United States Code, Section 2256.

25. On October 31, 2019, I spoke to Mary Strong, MeWe representative, regarding her submission of C.T. 51222603 to NCMEC. Strong acknowledged she submitted C.T. 51222603 and confirmed MeWe user "Android 18" uploaded 13 images of child pornography to the application on June 21, 2019. Strong also told me that the user "Android 18" uploaded the 13 images of child pornography to his/her MeWe timeline or posted them in a public chat room within the application, and that this allowed other MeWe users to view the child pornography images "Android 18" uploaded.

26. On November 1, 2019, Staff Operations Specialist (SOS) Megan Hammerling conducted a Florida DMV records check for the residents of 10870 John Randolph Dr., Jacksonville, Florida 32257, and identified Ray Clifton Depew Jr., Diana Lynn Depew, Patricia Mounger Depew, as occupants of the residence.

27. On November 1, 2019, SOS Hammerling conducted a utilities check which identified "Ray C Depew" as the utilities customer listed at 10870 John Randolph Dr., Jacksonville, Florida 32257.

28. On December 31, 2019, SOS Hammerling conducted open source social media checks and identified Ryan Depew, Reece Depew, and a minor female, as potential children of Ray Depew Jr.

29. On December 31, 2019, SOS Hammerling conducted a Florida DMV records check for Reece Depew, which listed his residence as 8150 Point Meadows

Drive, Apartment 301, Jacksonville, Florida 32256. Reece Depew's date of birth was listed as January 31, 1998.

30. On January 9, 2020, personnel with the FBI Atlanta office conducted a DMV records check and have advised that they have identified Ryan Depew's residence as 1000 Lakeside Drive, apartment 367, Athens, Georgia 30605.

31. On January 9, 2020, I conducted visual surveillance at the residence located at 10870 John Randolph Dr., Jacksonville, Florida 32257. I observed a white Chevrolet pickup truck, bearing Florida license plate ZT84X, in the driveway of the residence, and a white Toyota Camry exit the garage and depart the residence. I also observed an adult male, matching the physical description of Reece Depew, exit the residence through the garage door to place the trash receptacle and other lawn debris on the curb of the residence.

32. On January 15, 2020, I spoke to Mary Strong, MeWe representative, who confirmed the images of child pornography that she submitted to NCMEC on June 26, 2019, as referred to above, were screen captures of the original images uploaded by the user "Android 18".

33. On January 15, 2020, I spoke to Jason Wiley, MeWe representative, and learned that the user "Android 18" did not create the MeWe account using a mobile device. Wiley explained to me that MeWe is able to identify and provide the type of device used to create an account only if it was created using that mobile device. Wiley told me that he was currently reviewing the account information for

the user "Android 18", and Wiley confirmed the account creation device type was unavailable.

**CONCLUSION**

34. Based on the foregoing, I have probable cause to believe that one or more individuals has used and is using one or more computer devices, smart phones, and/or electronic storage media located in the residence located at 10870 John Randolph Drive, Jacksonville, Florida 32257, more fully described in Attachment A to this affidavit to, among other things, receive, distribute, and possess child pornography. Therefore, I have probable cause to believe that one or more individuals, using the residence described above has violated 18 U.S.C. §§ 2252 and/or 2252A. Additionally, I have probable cause to believe that fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, including at least one computer device and/or other electronic storage media containing images and/or video depicting child pornography, and the items more fully described in Attachment B to this affidavit (which is incorporated by reference herein), will be located in this residence.



DANIEL MOXLEY, Special Agent  
Federal Bureau of Investigation

Sworn and subscribed before me this 16<sup>th</sup> day of January, 2020.



JAMES R KLINDT  
United States Magistrate Judge