

JAM

10:49 am, May 24 2021

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MARYLAND**

AT BALTIMORE  
CLERK, U.S. DISTRICT COURT  
DISTRICT OF MARYLAND  
BY \_\_\_\_\_ Deputy

**IN THE MATTER OF THE  
APPLICATION FOR A SEARCH  
WARRANT FOR THE ITEMS  
DESCRIBED IN ATTACHMENT A:**

\*  
\*  
\*  
\*  
\*  
\*  
\*  
\*

**CASE NO.** 21-1367 BPG

**Currently secured at FBI, 185 Admiral  
Cochrane Drive, Suite 101, Annapolis,  
Maryland 21401**

\*\*\*\*\*

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

I, Linh Phung, a Special Agent (SA) with the Federal Bureau of Investigation (FBI), United States Department of Justice, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION**

1. I am a law enforcement officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in 18 U.S.C. § 2516. I am a Special Agent with the FBI and have been since May 2006. I am currently assigned to the Violent Crimes Against Children Task Force in the Baltimore Division of the FBI and have been assigned investigations concerning child human trafficking, child pornography, and the sexual exploitation of children. During my employment with the FBI, I have gained experience through training in seminars, classes, and daily work related to conducting these types of investigations. In addition, I have also received training regarding the use of the internet and digital communications as they pertain to federal investigations. I have participated in the execution of numerous search warrants, most of which have involved child exploitation offenses. Many of the search warrants resulted in the seizure of computers, cell phones and/or "smart phones," magnetic storage media for

computers, other electronic media, and other items evidencing violations of federal laws, including 18 U.S.C. § 2252, certain activities relating to material involving the sexual exploitation of minors. I have also participated in the execution of numerous search warrants for online accounts related to child exploitation and/or child pornography. In the course of my employment with the FBI, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media and within online accounts.

2. This affidavit is made in support of an application for a warrant to search the following devices:

- a. LG Rebel smartphone (**TARGET DEVICE 1**), belonging to Paul Philip, confiscated by U.S. Probation on April 8, 2021; and
- b. Onn Android tablet, serial number TKKG7A0784L4 (**TARGET DEVICE 2**), confiscated by U.S. Probation on April 13, 2021.

which are more fully described in Attachment A and collectively, the “**TARGET DEVICES**”.

3. The **TARGET DEVICES** are to be searched for evidence of crimes related to the distribution, receipt, and/or possession of child pornography, in violation of 18 U.S.C. § 2252(a)(2), (4), as well as 18 U.S.C. § 2252A(a)(2), (5), (the “**TARGET OFFENSES**”). There is probable cause to search the **TARGET DEVICES** for evidence of the **TARGET OFFENSES** as described in Attachment B.

4. The statements in this affidavit are based in part on information and reports provided by the U.S. Probation Office and my experience and background as a Special Agent of the FBI. Since this affidavit is being submitted for the limited purpose of securing 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 evidence, fruits, and instrumentalities of the **TARGET OFFENSES** are located in the **TARGET**

**DEVICES.** Unless otherwise indicated, all written and oral statements referred to herein are set forth in substance and in part, rather than verbatim.

**STATEMENT OF PROBABLE CAUSE**

5. On or about April 29, 2015, Paul Anthony Philip was sentenced to 48 months federal imprisonment in the District of Maryland by United States District Judge Catherine C. Blake for one count of possession of child pornography, 18 U.S.C. § 2252A(a)(5)(B). Judge Blake ordered that Philip shall be on supervised release upon release from imprisonment for a term of 180 months. One condition of Philip's supervision included that "the defendant is not to use computer systems, Internet-capable devices and/or similar electronic devices at any location (including employment or educational program) without the prior written approval of the U.S. Probation and Pretrial Services Officer. The defendant shall cooperate with the U.S. Probation and Pretrial Services Office monitoring of compliance with this condition. Cooperation shall include, but not limited to, participating in a Computer & Internet Monitoring Program, identifying computer systems, Internet-capable devices and/or similar electronic devices the defendant has access to, allowing the installation of monitoring software/hardware at the defendant's expense, and permitting random, unannounced examinations of computer systems, Internet-capable devices and similar electronic devices under the defendant's control."

6. On or about January 8, 2019, Philip was released from federal custody and on or about January 10, 2019, Philip signed a form acknowledging that he understood that upon a finding of violation of supervised release that the Court may (1) revoke supervision, (2) extend the term of supervision and/or (3) modify the conditions of supervision.

7. On or about August 30, 2019, Philip signed a monitoring agreement with U.S. Probation where he agreed to "waive any expectations of privacy from the supervising

probation/parole officer, his or designee, and RemoteCOM.” The agreement also included that Philip “shall not view, subscribe to, download, or transmit any content in any medium, including but not limited to text, images, movies, or multi-media files, in violation of state or federal laws or in violation of his conditions of supervised release.”

8. On or about September 6, 2019, TARGET DEVICE 1 was approved for Philip’s use by U.S. Probation and the monitoring software, RemoteCOM, was installed on TARGET DEVICE 1. U.S Probation changed the monitoring contracted vendor and on or about November 23, 2020, the new monitoring software was installed on TARGET 1.

9. On or about April 1, 2021 and April 5, 2021, Philip failed to report for sex offender treatment, per the conditions of his supervised release. On or about January 19, 2021; March 4, 2021; and April 8, 2021, Philip failed to attend the mental health and substance abuse therapy sessions, per the conditions of his supervised release.

10. On or about April 8, 2021 at 8:30 AM, Philip was scheduled to meet with Senior U.S. Probation Officer (USPO) Jessica Turro in the U.S. Probation office located in Baltimore, to discuss his noncompliance of his supervised release conditions. Philip communicated with USPO Turro and advised of her of his estimated time of arrival, but Philip never showed up for his meeting. USPO Turro attempted to contact Philip several times but received no response from Philip. USPO Turro contacted Philip’s father for his assistance. Philip’s father was unable to contact Philip, however, Philip’s father checked his bank records and it posted that Philip paid for parking in downtown Baltimore and a transaction was posted for Mick O’Shea’s in Baltimore on April 8, 2021.

11. On or about April 8, 2021, USPO Turro conducted a home visit at Philip’s residence, 8019 Outing Avenue, Pasadena, Maryland 21122, which is a sober house. The house

manager provided that Philip was not home and that Philip was noncompliant with the sober house rules. The house manager also advised that he observed Philip utilizing his tablet and smartphone often. USPO Turro requested to see Philip's bedroom. After visually inspecting Philip's belongings in plain view, USPO Turro began to exit out of Philip's bedroom. The house manager removed the pillows from Philip's bed and observed TARGET DEVICE 2 on the bed, which was not authorized by U.S. Probation. TARGET DEVICE 2 was confiscated by USPO Turro and currently in the custody of U.S. Probation.

12. On or about April 12, 2021, USPO Turro spoke with Philip and he was asked if there was any child pornography on TARGET DEVICE 2 and Philip declined to answer any questions from USPO Turro regarding TARGET DEVICE 2. On or about April 12, 2021, U.S. Probation referred the investigation to the United States Attorney's Office, Baltimore, Maryland, and the FBI.

13. On or about April 13, 2021, USPO Turro confiscated TARGET DEVICE 1 from Philip, which was in Philip's pocket. Philip also provided the passcodes for TARGET DEVICE 1 and TARGET DEVICE 2, which were "1983" and "0623", respectively. Philip admitted to viewing images of minors that were not pornographic in nature.

14. On or about April 26, 2021, a federal search warrant was issued by the Honorable Thomas M. DiGirolamo, U.S. Magistrate Judge, District of Maryland, to search the **TARGET DEVICES** for evidence of crimes related to failure to register as a sex offender and the willful and knowing disobedience and contempt of court.<sup>1</sup>

---

<sup>1</sup> Attachment B to the April 26, 2021 warrant authorized the seizure of child pornography and child erotica, which were specifically prohibited by the terms of Philip's supervised release. Thus an additional warrant seeking evidence of child pornography offenses may not be necessary. Nevertheless, I am applying for a new warrant out of an abundance of caution, and on the advice of the United States Attorney's Office.

15. On or about April 29, 2021, pursuant to the search warrant issued April 26, 2021, your affiant conducted a data extraction of TARGET DEVICE 2 utilizing a forensic software. Upon completion of the data extraction, your affiant selected the category title “images” on the forensic software and your affiant observed image files depicting child pornography. Your affiant immediately ceased the review of TARGET DEVICE 2 and contacted AUSA Zachary Myers. Your affiant observed the following files:

- a. “(( PTHC )) RED (3).jpg”<sup>2</sup> – This image depicts a nude prepubescent girl who appears to be in a bath tub with her legs spread apart exposing her vagina. The girl also appears to be sitting on top of another person’s legs.
- b. “004.jpg” – This image depicts what appears to be a close-up of a prepubescent girl’s vagina, with her underwear was pulled down to mid-thigh.
- c. “(( PTHC )) RED (88).jpg” – This image depicts a prepubescent girl who appears to be kneeling on her hands and knees with her underwear or shorts pulled down exposing her anus.

**SUMMARY CONCERNING CHILD PORNOGRAPHY, PERSONS WHO POSSESS  
AND COLLECT CHILD PORNOGRAPHY AND HOW USE OF COMPUTERS  
AND THE INTERNET RELATE TO THE POSSESSION OF CHILD  
PORNOGRAPHY**

16. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned individuals who utilize the internet to view and receive images of child pornography are often individuals who have a sexual interest in children and in images of children, and there are certain characteristics common to such individuals, including the following:

- a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.
- b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for

---

<sup>2</sup> Through my training and experience, I know “PTHC” to be an acronym for “Pre-Teen Hard-Core.” Individuals who traffic in child sexual abuse images often use this description to alert others that the images or videos contain visual depictions of preteen minors engaged in sexually explicit conduct.

their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

- c. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer, cell phone or tablet, and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, or in online stores, email accounts or other online communication accounts, to enable the individual to view the collection, which is highly valued by the individual.
- e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers, cell phones and in online storage, email accounts or other online communication accounts.
- f. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

17. Based on my investigative experience related to computer and internet related child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following:

- a. Computers, smartphones, and the internet are all methods used by child pornography collectors and those with an interest in sexual encounters with children to interact with and sexually exploit children.
- b. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e. "Instant Messaging"), easy access to the internet, and online file sharing and storage, electronic devices are the preferred method of distribution and receipt of child pornographic materials.
- c. The internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography as well as those

with an interest in sexual contact with children use online resources to retrieve and store child pornography and to communicate with children, including services offered by internet portals such as AOL Inc., Yahoo! And Google, Inc., Facebook, Dropbox, Instagram, and others. The online services allow a user to set up an account with a remote computing service that provides email services, file exchange services, messaging services, as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the internet, including (for example) a smart phone. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data.

- d. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know the individuals who collect child pornography are using email accounts, online storage accounts, and other online communication accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

18. Modern communications, including through smart phones and computers equipped with communications applications like Facebook Messenger, WhatsApp, and many others, allow near instantaneous contact through voice, text, video, and images. Individuals with a sexual interest in children, whether or not they are also interested in child pornography, make use of these modern communications systems to contact children, including for the purpose of initiating sexual encounters with children.

19. In addition, when devices connect to the internet, logs can be generated pertaining to internet connectivity, to include Internet Protocol Address, as well as location information. This information can be analyzed to determine how and where devices were used to access the internet which can be used to determine where and for how long a particular device was used at a particular location.


20. The search of electronic devices often requires recursive searching of the device and the repeated use of a variety of forensic tools to restore data—including data previously “deleted” by the user. The data does not actually disappear; rather, the data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. This affidavit and warrant specifically contemplate the repeated use of forensic tools to recover data from electronic devices.

### **CONCLUSION**


21. Based on the foregoing, I submit that there is probable cause to believe that the TARGET OFFENSES have been committed and there is probable cause to believe evidence of these crimes can be found stored at or on the **TARGET DEVICES**, further described in



Attachment A, which are incorporated herein by reference. Therefore, I respectfully request that the attached warrant be issued authorizing the search of the **TARGET DEVICES**, and to seize any items located pursuant to the search as described in Attachment B, also incorporated herein by reference.

  
\_\_\_\_\_  
Special Agent Linh Phung,  
Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 3rd day of May, 2021.

  
\_\_\_\_\_  
The Honorable Beth P. Gesner  
Chief United States Magistrate Judge

**ATTACHMENT A**

***Items to be Searched***

This warrant applies to information associated with the items listed below (collectively, the “TARGET DEVICES”):

- A. LG Rebel smartphone (**TARGET DEVICE 1**);
- B. Onn Android tablet, serial number TKKG7A0784L4 (**TARGET DEVICE 2**);

The TARGET DEVICES are currently in the custody of FBI Baltimore, at 185 Admiral Cochrane Drive, Suite 101, Annapolis, Maryland 21401.

## **ATTACHMENT B**

### **ITEMS TO BE SEIZED**

All records, documents, items, data and other information that may constitute fruits or instrumentalities of, or contain evidence related to, violations of Title 18, United States Code, 2252A(a)(2) and 2252A(a)(5)(B), including, but not limited to, the following that may be found in the locations described in Attachment A:

1. Any and all cellular telephones with cameras and/or Internet capability, web cameras, cameras, film, videotapes, video recording devices, video recording players or other photographic or video equipment.

2. Computer(s), computer hardware, software, related documentation, passwords, data security devices (as described below), videotapes, and or video recording devices, and data that may constitute instrumentalities of, or contain evidence related to, this crime. The following definitions apply to the terms as set out in this affidavit and attachment:

a. Computer hardware: Computer hardware 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. Hardware includes any data processing devices (including but not limited to central processing units, laptops, tablets, eReaders, notes, iPads, iPods, personal data assistants, cellular telephones; internal and peripheral storage devices such as external hard drives, thumb drives, SD cards, flash drives, USB storage devices, CDs and DVDs, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, 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).

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

c. Documentation: Computer-related documentation consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.

d. Passwords and Data Security Devices: Computer passwords and other data security devices are 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. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touches. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data

to make it inaccessible or unusable, as well as reverse the progress to restore it.

3. Any and all images, videos, notes, documents, records, or correspondence pertaining to minors engaged in sexually explicit conduct.

4. Any and all records, documents, invoices and materials that concern any online accounts including Snapchat, Facebook, Instagram, Skype, or any other account that allows chatting, email, or video chats over the Internet, including screen names and email accounts.

5. Any and all records, documents, invoices and materials that concern any accounts with Internet Service Providers.

6. Any and all diaries, notebooks, notes, pictures, chats, directions, maps, banking, travel, documents, and any other records reflecting personal contact and any other activities with minors.

7. Any and all notes, documents, records, or correspondence, including images or videos, that indicate a sexual interest in children or communications with children regarding sexual activity, including, but not limited to:

- a. Correspondence with children;
- b. Any and all visual depictions of minors;
- c. Internet browsing history;
- d. Books, logs, diaries and other documents.

8. Any and all records, documents, or correspondence relating to persuading, inducing, enticing, or coercing any minor to engage in any sexual activity in violation of the law.

9. Any and all records, documents, or correspondence relating to transmitting obscene materials to minors.

As used above, the terms “records, documents, messages, correspondence, data, and materials” includes records, documents, messages, correspondence, data, and materials, created, modified or stored in any form, including electronic or digital form, and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices.

For any computer, computer hard drive, or other physical object upon which computer data can be recorded, which includes cellular phones, tablets, iPods, and other electronic devices (hereinafter, “COMPUTER”) that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles,

email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment.

j. any and all clothing or bedding visible in records, documents, or correspondence relating to transmitting obscene materials to minors, including but not limited to black and green shorts or pants and a white or light-colored blanket.

11. With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a nonexclusive list, and the government may use other procedures that, like those listed below, to minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

- c. "scanning" storage areas to discover and possible recover recently deleted files;
- d. "scanning" storage areas for deliberately hidden files; or
- e. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

12. If after performing these procedures, the directories, files or storage areas do not reveal evidence of child pornography or other criminal activity, the further search of that particular directory, file or storage area, shall cease.

13. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.