United States District Court

SOUTHERN DISTRICT OF INDIANA

UNITED STATES OF AMERICA

V.

VINCENT GEVIRTZ

CRIMINAL COMPLAINT

CASE NUMBER: 1:16-mj-0487

I, the undersigned complainant being duly sworn state the following is true and correct to the best of my knowledge and belief. Between on or about April 7, 2016 and May 4, 2016, in Delaware County, in the Southern District of Indiana defendant did,

Count 1, 18 U.S.C. § 2251(d): Noticing or Advertising Child Pornography;

Counts 2 - 6, 18 U.S.C. § 2252(a)(2): Distribution, Receipt and Possession of Child Pornography;

Count 7, 18 U.S.C. § 2252(a)(4)(B) and (b)(2): Possession of Child Pornography,

I further state that I am a Special Agent, and that this complaint is based on the following facts:

See attached affidavit

Continued on the attached sheet and made a part hereof.

Michael Johnson, Special Agent, Department of Homeland Security

Sworn to before me, and subscribed in my presence

July 14, 2016
Date

at Indianapolis, Indiana

Tim A. Baker, U.S. Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

AFFIDAVIT

I, Special Agent Michael Johnson, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. **Affiant**: I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations ("HSI"). I am currently assigned to the Office of the Resident Agent in Charge, Indianapolis, Indiana (RAC/IP). I have been employed as a Special Agent with HSI since February of 2006. Before being appointed as a Special Agent with HSI, I was a Police Officer for the City of Indianapolis for approximately eleven years. The last four years, I was assigned to a federal task force. During my experience with both agencies, I have been involved in numerous investigations, including those involving production, advertising, distribution and possession of child pornography. I have had training through the Federal Law Enforcement Training Center, HSI, the Indiana State Police, Office of Juvenile Justice Prevention, the United States Attorney's Office, and Project Safe Childhood in investigating computer related crimes and child exploitation. Since being employed with HSI, I was temporarily assigned to HSI's Cyber Crimes Center (C3). During that assignment, I worked on active undercover cyber investigations as well as the cataloging of over 10,000 images and videos of child pornography. I have been involved in over one-hundred investigations pertaining to the sexual exploitation of children.

1. **Information Provided**: Because this affidavit is being submitted for the limited purpose of securing an arrest warrant and criminal complaint, 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 that **Vincent Gevirtz** (DOB: 1992)("**Gevirtz**") has violated the following statutes

a. Count 1, 18.U.S.C. § 2251(d)(Noticing Or Advertising Child Pornography Using Chat Applications);

b. Counts 2 through 6, 18.U.S.C. § 2252(a)(2)(Distribution and Receipt Of Child Pornography); and

c. Count 7, 18 U.S.C. § 2252(a)(4)(B) and (b)(2) (Possession Of Child Pornography).

2. **Requested action**: I make this affidavit in support of an application for a ~~search~~ ARREST warrant for the **Subject Premises** for evidence of violations of the below listed statutes.

3. **Relevant Crimes**: I have set forth the facts that I believe necessary to establish probable cause to believe that **Gervitz** has violated **18 U.S.C. §§ 2251(d), 18 U.S.C. § 2252(a)(2) and (b)(1), and 18 U.S.C. § 2252(a)(4)(B) and (b)(2)** .

4. **Noticing or Advertising Child Pornography**: The investigation also concerns alleged violations of **18 U.S.C. § 2251(d)** which generally prohibits a person from knowingly making, printing, or publishing, or causing to be made, printed, or published, any notice or advertisement seeking or

offering (A) to receive, exchange, buy, produce, display, distribute, or reproduce, any visual depiction, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct; or (B) participating in any act of sexually explicit conduct by or with any minor for the purpose of producing a visual depiction of such conduct, if such person (A) such person knows or has reason to know that such notice or advertisement will be 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 mailed; or (B) such notice or advertisement is 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 mailed.

5. **Distributing, Receiving and Possessing Visual Depictions**: This investigation concerns also alleged violations of **18 U.S.C. 2252 (a) and (b)**, which generally prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce. This includes the distribution, receipt, and possession of at least one visual depiction of a prepubescent minor or a minor less than 12 years of age, engaged in sexually explicit conduct.

6. **Definitions**:

a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the user who sent/received such a message, or by the Website Administrator.

b. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally

short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. "Virtual private network" also known as a (VPN) is a private network that extends across a public network or internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Individual Internet users can use some VPNs to secure their wireless transactions, to circumvent geo-restrictions and censorship, and/or to connect to proxy servers for the purpose of protecting personal identity and location. A VPN provides a secure connection from a remote computer to a server and/or network, using an existing infrastructure, i.e the Internet. Once connected to the VPN, the broadcasting IP address can appear to be that of the VPN server, rather than that of the remote computer thus hiding the true IP address.

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

a. "Child pornography," as defined in 18 U.S.C. § 2256(8), is 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.

b. "Cloud-based storage service," as used herein, refers to a publicly accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the

file. Access is free and readily available to anyone who has an Internet connection.

c. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. *See* 18 U.S.C. § 1030(e)(1).

d. "Computer hardware," as used herein, consists of all equipment that 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 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 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 physical keys and locks).

e. "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.

f. "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 what might be termed a 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 touched. 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 process to restore it.

g. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

h. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

i. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web

hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

j. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

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

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

m. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

n. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), 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 genitals or pubic area of any person.

o. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other 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 a permanent format.

e. Background on Child Pornography, Computers, the Internet, and Email: I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras and smartphones with

cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

c. 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. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic

communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) 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"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an

individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail 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. Even in cases where online storage is

used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

g. As is the case with most digital technology, communications 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 e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the 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). 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. Such information is often maintained indefinitely until overwritten by other data.

f. **Specifics of Search and Seizure of Computer Systems:** Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including

external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including, but not limited, to "cloud" storage. I also know that during the search of the premises, it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is

essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

g. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for contraband, evidence, fruits, or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords), so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). Further, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any

applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

h. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

i. **Investigation of Suspect User:** On May 4, 2016, HSI Special Agent Scott Sikes ("SA Sikes") was online acting in an undercover capacity. SA Sikes entered an internet relay chat (IRC) network using a particular moniker or "nick" (hereinafter referred to as "UC"). The actual moniker or "nick" is known to your affiant. SA Sikes was monitoring activity in IRC channel "#imgur", when he noticed a link posted to the room by a particular IRC user (**Suspect User)**, whose actual "nick" is known to your affiant but is referred to as "Suspect User" as the investigation into these internet activities is on-going. SA Sikes opened the link and discovered the contents to be an image of child pornography.

j. On May 4, 2016, "UC" initiated a direct, one-on-one chat session with **Suspect User**. "UC" searched the IRC channel for user information on **Suspect User**. The IRC search retrieved the IRC Address Book and provided the following information:

a. Nick: **Suspect User**

b. Name: kitty

c. Address: ~daddystoy@209.197.26.72

d. Channels: #imgur #0!!!!!!younggirlsex

k. "UC" and **Suspect User** then began a direct, one-on-one, chat session. During the chat, **Suspect User** posted the following three (3) links, making the associated files available for download by "UC:"

a. http://picpaste.com/I1zweTx1.jpg was posted by **Suspect User** directly to "UC." Upon opening the

link, "UC" discovered the file contained a photograph depicting an adult male penis penetrating the vagina of what appears to be a prepubescent female.

b. http://picpaste.com/Z9Sndoev.jpg was posted by **Suspect User** directly to "UC." Upon opening the link, "UC" discovered the file contained a photograph depicting an adult male penis penetrating the vagina of an unconscious prepubescent female.

c. http://en.file_upload.net/download_11547906/ky.mpg.html was posted by **Suspect User** directly to "UC." "UC" was unsuccessful downloading and installing the media player required to open and view the file.

l. During the chat session **Suspect User** described his interest in child exploitation material by telling "UC" "yea I luv the hardcore stuss :)". **Suspect User** directed "UC" to use encryption to save his photos by saying "if ur gonna save thm on ur pc make sure u encrypt them well"..."EncFS"..."when setting it up use the highest security form".

m. While communicating one-on-one with **Suspect User**, "UC" continued to monitor IRC channel #imgur for further postings by **Suspect User** containing links to photographs or videos. "UC" discovered seventeen total postings which contained links. Among the links posted by **Suspect User** were:

a. http://picpaste.com/ch2L6LAo.jpg (photograph depicting an adult male penis penetrating the vagina of a prepubescent female)

b. http://picpaste.com/ThHZaHVJ.jpg (photograph of an adult male ejaculating on the genitals of infant female)

c. http://picpaste.com/HHM1fvyp.jpg (photograph of an adult male penis penetrating the vagina of a prepubescent female)

d. http://picpaste.com/HBvxYFpe.jpg (photograph of an adult male ejaculating on the genitals and torso of an infant female)

e. https://sendvid.com/12dajo7f (video of an adult male penis penetrating the anus of a prepubescent male)

n. **Highwinds Network Group information:** On May 11, 2016, a Department of Homeland Security Summons for Records was served on Highwinds Network Group, Inc., requesting subscriber information for internet protocol (IP) address 209.197.26.72 for the dates and times recorded as timestamps of postings of links posted by **Suspect User** including the files described above.

o. On May 26, 2016, Highwinds Network Group, Inc. delivered a response to the summons served on May 11, 2016. Highwinds Network Group,

Inc. response stated that the IP address (209.197.26.72) "is for a VPN (Virtual Private Network) service. This service allows people to use the Internet securely (banking, public wifi spots, etc.). To protect customer data, we do not log any usage information. Therefore, we do not have any information regarding the referenced IP."

p. SA Sikes contacted Highwinds Network Group, Inc. regarding the above described response. Highwinds Network Group, Inc. suggested that HSI submit a second summons requesting subscriber information more detailed in nature.

q. On June 9, 2016, a Department of Homeland Security Summons for Records was served on Highwinds Network Group, Inc. requesting subscriber information and/or "any data associated with IRC traffic using IP 209.197.26.72, port 6667."

r. On June 21, 2016, Highwinds Network Group, Inc. delivered a response to the summons served on June 9, 2016. Highwinds Network Group, Inc. provided a report as well as subscriber information identifying user **Suspect User**. The following information was provided identifying IRC user **Suspect User**:

a. User connecting to the vpn server

b. User **Suspect User** connecting to undernet irc server(s)

c. User disconnecting from the vpn server

d. In each case the user is vingev@gmail.com

e.	Full Name	Vincent GEVIRTZ
f.	Email Address	vingev@gmail.com
g.	Username	vingev@gmail.com
h.	Reset Password	
i.	Account Status	Active
j.	Activated	Yes
k.	Current Subscription	1 Month
l.	EOB Date	04/07/2016

s. In addition to the information provided in Paragraph 20, Highwinds Network Group, Inc. provided additional information related to this user, including the IP address 50.178.206.161, as well as dates and times **Suspect User** connected to, and disconnected from, the IRC network. These dates and times coincided with the activity of **Suspect User** which is described above.

t. **Comcast Information**: On June 22, 2016, an online search for IP address 50.178.206.161 was conducted. IP address 50.178.206.161 was discovered to possibly be assigned to Comcast and geo-located to a physical address in Muncie, Indiana.

u. On June 24, 2016, a Department of Homeland Security Summons for Records was served on Comcast Cable Communications, LLC, requesting subscriber records for IP 50.178.206.161. The summons requested the

subscriber of IP 50.178.206.161 on dates and times reflected in the Highwinds Network Group, Inc. report.

v. On June 27, 2016, Comcast Cable Communications, LLC delivered a response to the summons served on June 24, 2016. The following subscriber information was included in the response:

a. Subscriber Name: JULIAN GEVIRTZ

b. Subscriber Address: 2005 N WINTHROP RD MUNCIE, IN 47304

w. A search for Vincent GEVIRTZ was conducted in a publicly available database. The search located Vincent GERVITZ (DOB: 1992) located at physical address 2005 North Winthrop Road, Muncie, Indiana 47304.

x. Indiana Bureau of Motor Vehicles (BMV) information related to Vincent GEVIRTZ indicated Vincent GEVIRTZ (DOB: 1992) resides at 2005 North Winthrop Road, Muncie, Indiana.

y. **Search Warrant and contact with Gevirtz**: On July 13, 2016, a Federal search warrant was served at the residence located at 2005 N Winthrop Road, Muncie, Indiana 47304. Upon serving the warrant, your affiant came into contact with GEVIRTZ.

z. I explained the investigation leading to the issuance of the search warrant in detail to GEVIRTZ. GEVIRTZ asked for time to consult with his parents, the owners of the residence, before agreeing to speak with Agents. After some time and consultation with his parents, GEVIRTZ agreed to speak with Agents.

aa. GEVIRTZ was advised of his rights both verbally and through an advice of rights form. GEVIRTZ waived his rights both verbally and by signing the advice of rights form.

bb. GEVIRTZ admitted to the above described behavior (the distribution and receipt of child pornography, as well as the posting of hyperlinks which would direct other users to locations where child pornography was stored) and to being the IRC **Suspect User**. GEVIRTZ provided encryption keys to your affiant, which allowed encrypted data on a Seagate external hard drive to be viewed.

cc. Within the folder structure of the encrypted partition of the hard drive were numerous files of child pornography including the following:

a. 1.jpg – This file depicts a pre-pubescent female child whose pants have been pulled down. The child's legs are pulled toward her head, exposing her genitals to the camera.

b. 12.jpg – An adult male putting his penis into the anus of a pre-pubescent child.

c. 4.jpg – In this image, a pre-pubescent female victim has her mouth on the penis of an adult male.

d. 77777.mp4 – This video depicts a pre-pubescent female victim performing oral sex on an adult male.

e. 9797.mp4 – This video depicts a female child victim performing oral sex on a male child victim.

dd. GEVIRTZ admitted to sharing child pornography for at least 7 years.

ee. GEVIRTZ is a member of a private video and image hosting site on the TOR network, commonly referred to as the "Darknet," which site is predominately known for child abuse material, including children being molested and children being tortured and engaged in bestiality.

ff. **Conclusion**: Based upon the contents of this Affidavit, I respectfully request that the Court issue an arrest warrant and criminal complaint for the offenses listed above.

Michael Johnson
Special Agent

Subscribed and sworn before me this 14th day of July, 2016.

Tim A. Baker
United States Magistrate Judge
Southern District of Indiana