AFFIDAVIT IN SUPPORT OF A
CRIMINAL COMPLAINT AND ARREST WARRANT

I, Darrell Franklin, a Special Agent (SA) with U.S. Immigration and Customs Enforcement (ICE) – Homeland Security Investigations (HSI), being duly sworn, depose and state as follows:

I am a Special Agent of HSI and have been so employed since February 2007. I have successfully completed the eleven-week Criminal Investigator Training Program at the Federal Law Enforcement Training Center; and the eleven-week Special Agent Basic Training course offered by ICE. As part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to persons traveling in interstate and foreign commerce to sexually exploit children, coercion and enticement, and the illegal production, distribution, receipt and possession of child pornography, in violation of Title 18, United States Code, Sections 2423, 2422, 2251, 2252, and 2252A. I have personally conducted and participated in numerous child exploitation and child pornography investigations, search warrants, interviews and computer forensic examinations. I have received training and instruction in the field of investigation of child pornography and have had the opportunity to participate in investigations relating to the sexual exploitation of children. I have successfully completed several basic and advanced child exploitation and child pornography investigation courses, including online undercover techniques, child sex tourism, undercover chat, peer to peer investigations, and data recovery and acquisition. Based on my training and experience, I have provided training and instruction to other law enforcement officers on how to conduct child exploitation and child pornography investigations. As part of my training and experience, I have reviewed images containing child pornography in a variety of formats (such as digital still images and video images) and media (such as storage devices, the Internet, and printed images).

This case involves an international investigation of a Tor network-based child pornography website called "The Website."[1] The Website server was physically located in South Korea.

This affidavit is submitted in support of a complaint charging Vincent Galarza (hereinafter "Galarza") with Conspiracy to Distribute Child Pornography, in violation of Title 18, United States Code, Sections 2252(a)(2) and (b)(1). This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The statements in this affidavit are based on my investigation of this matter as well as information conveyed to me by other law enforcement officers, including agents with the Internal Revenue Service – Criminal Investigation (IRS-CI), Cyber Crimes Unit.

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

DEFINITION OF TERMS

The Tor Network

Tor is a computer network which anonymizes Internet activity by routing a user's communications through a global network of relay computers (or proxies), thus effectively masking the internet-protocol ("IP") address of the user. An "IP address" is a unique numeric address (used by computers on the internet) that is assigned to properly direct internet traffic. A publically visible IP address can allow for the identification of the user and his/her location.
To access the Tor network, a user has to install freely available Tor software, which relays only the IP address of the last relay computer (the "exit node"), as opposed to the user's actual IP address. There is no practical method to trace a user's actual IP address back through those Tor relay computers.

The Tor network makes it possible for a user to operate a special type of website, called "hidden services," which uses a web address that is comprised of a series of 16 algorithm-generated characters (such as "asdlk8fs9dflku7f") followed by the suffix ".onion." Websites, including hidden services, have system administrator(s) (also called the "admin(s)") who are responsible for overseeing and operating these websites.

Bitcoin

Bitcoin ("BTC") is one type of virtual currency that is circulated over the Internet. BTC is not issued by any government, bank, or company but rather is controlled through computer software. Generally, BTC is sent and received using a BTC "address," which is like a bank account number and is represented by a case-sensitive string of numbers and letters. Each BTC address is controlled through the use of a unique private key, a cryptographic equivalent of a password. Users can operate multiple BTC addresses at any given time, with the possibility of using a unique BTC address for every transaction.

BTC fluctuates in value. Around March 5, 2018, one BTC was worth approximately $11,573.00. A typical user purchases BTC from a BTC virtual-currency exchange, which is a business that allows customers to trade virtual currencies for conventional money (*e.g.*, U.S. dollars, euros, etc.). Little to no personally identifiable information about the sender or recipient is transmitted in a BTC transaction itself. However, virtual currency exchanges are required by U.S. law to collect identifying information of their customers and verify their clients' identities.

To send BTC to another address, the sender transmits a transaction announcement, cryptographically signed with the sender's private key, across the BTC network. Once the sender's

transaction announcement is verified, the transaction is added to the blockchain. The blockchain is a decentralized, public ledger that logs every BTC transaction. In some instances, blockchain analysis can reveal whether multiple BTC addresses are controlled by the same individual or entity. For example, analyzing the data underlying BTC transactions allowed for the creation of large databases that grouped BTC transactions into "clusters." This analysis allowed for the identification of BTC addresses that were involved in transacting with the same addresses.

THE WEBSITE

"The Website" was a website dedicated to the advertisement and distribution of child pornography that operated as a hidden service on the Tor network until March of 2018 when it was seized by law enforcement. On or about September 28, 2017, February 8, 2018, and February 22, 2018, from a location in Washington, D.C. law enforcement agents accessed The Website and documented its content, which is described herein. The Website was used to host and distribute video files depicting child pornography that could be downloaded by site users. The Website was not intended to be used to upload pornography of adults, as evidenced on the upload page on The Website which clearly stated: "Do not upload adult porn."

On the video search page of The Website, there was a list of keyword search terms and the number of videos associated with the keyword. When law enforcement accessed the contents of The Website on or about February 8, 2018, it was determined that some of the top keyword search terms included "PTHC" (over 10,000 videos), "PEDO" (over 7,000 videos), "2yo%" (over 4,000 videos) and "4yo%" (over 4,000 videos).[2]

On or about February 8, 2018, The Website indicated on its download page details that its users had downloaded video files from The Website more than a million times. On or about March 5, 2018, The Website server had over 200,000 unique video files, which totaled approximately eight terabytes of data.

Any user could create a free account on The Website by creating a username and password. Only after the user registered an account could the user browse previews of videos available for download and post text to The Website. To download videos from the site, users used "points," which were allocated to users by The Website. A registered user could earn points from The Website in several ways: (1) uploading videos depicting child pornography; (2) referring new users to The Website; (3) paying for a "VIP" account, which lasted for six months, entitled a user to unlimited downloads, and was priced at 0.03 BTC (approximately $327.60 as of March 1, 2018);

[2] I am aware from my training and experience that "PTHC" stands for "preteen hardcore," PEDO is a reference to "pedophile," and the references to "2yo" and "4yo" represent ages of children.

or (4) paying for points incrementally (*i.e.*, .02 BTC for 230 points).[3] Points were not transferable to any other website or application. Once a customer sent BTC to The Website, the BTC could not be refunded or redirected. The points obtained by the payment of BTC could only be used for downloading videos.

Certain persons joined the conspiracy to distribute child pornography by uploading videos to The Website. Those co-conspirators who uploaded videos of child pornography to The Website for "points" also earned additional "points" each time a customer of the site downloaded that particular video from The Website. Thus, the co-conspirators had a shared goal as part of the conspiracy – increasing the number of unique videos on The Website to drive additional traffic to it, which in turn led to greater downloads and more points for the co-conspirators. When uploading videos, the co-conspirators would use explicit file names highlighting the content as showing the sexual exploitation of minors and would add tags that customers could search for, such as PTHC, 2yo, etc. In order to prevent duplicate videos from being uploaded, The Website operated a digital hash-value check of videos the co-conspirators uploaded in order to compare the video to other videos previously uploaded to the site. The Website did not allow a co-conspirator to upload a video whose hash value matched something previously uploaded to the site.

During the course of the investigation, law enforcement agents in Washington, D.C. accessed The Website on multiple occasions, including on or about September 28, 2017, February 8, 2018, and February 22, 2018, observed its functionality by browsing the listings on The Website, and conducted undercover purchases by downloading child pornography video files from The Website. These downloaded child pornography video files included pre-pubescent children, infants, and toddlers engaged in sexually explicit conduct. Each video available for download from The Website had a title, a description (if added by the co-conspirator), "tags" with further descriptions of the video enabling a user to more easily locate a particular category of video using The Website's search function, and a preview thumbnail image that contained approximately sixteen unique still images from the video.

INVESTIGATION OF THE ADMINISTRATOR OF THE WEBSITE

On or about September 1, 2017, law enforcement reviewed the source code of The Website's homepage, which could be viewed by right-clicking on The Website in the Tor browser and selecting "View Page Source." In reviewing the source code, law enforcement discovered that The Website had failed to conceal an IP address, likely due to user error on the part of the administrator. This IP address resolved to a telecommunications provider in South Korea. Subsequent investigation confirmed that this IP address was registered in the name of Jong Woo Son and was serviced at his residence in South Korea.

[3] Bitcoin is volatile and the price of bitcoin can fluctuate on an hourly basis. Between January 2017 and February 2018, for example, 1 bitcoin fluctuated in price from approximately $1,000 to $20,000 USD.

On February 28, 2018, a federal magistrate judge in the United States District Court for the District of Columbia issued an arrest warrant for Jong Woo Son. *See* 1:18-mj-00019 (GMH) (Sealed). On or about March 5, 2018, South Korean law enforcement executed a search warrant at the residence of Jong Woo Son in South Korea. Pursuant to the search, South Korean law enforcement seized The Website's server and associated electronic storage media from the bedroom of Jong Woo Son – The Website's administrator. South Korean law enforcement then provided to U.S. law enforcement a forensic image of the server. U.S. law enforcement subsequently obtained a federal search warrant to review this forensic image. *See* 1:18-sw-00052 (RMM) (Sealed).

A review of the imaged data confirmed that The Website was hosted on the seized server. A review of a sample of the video files further corroborated that The Website was dedicated to the distribution of child pornography. The customer data generally identified which user was associated with which BTC payment to The Website. A review of a sample of the payments to The Website cross-referenced against the username and download data from the server revealed that each payment to The Website corresponded with the user downloading at least one video from The Website. A review of the forensic image of the server further revealed that certain customers that paid BTC into The Website were also co-conspirators who uploaded content to the site.

On August 8, 2018, a federal grand jury in the District of Columbia indicted Jong Woo Son on various counts, including Conspiracy to Distribute Child Pornography, in violation of 18 U.S.C. Sections 2252(a)(2) and (b)(1). *See* 1:18-mj-00243 (DAF) (Sealed).

IDENTIFICATION OF CO-CONSPIRATOR GALARZA (A/K/A THISTHISHOLD)

As part of the investigation, law enforcement reviewed the forensic image of the server to obtain leads on the customers of The Website. After law enforcement identified a unique BTC address that sent BTC to the site, law enforcement would send subpoenas to the virtual-currency exchanges that transacted with those addresses to identify who the person was behind the transaction. Law enforcement has arrested many of the subsequently identified customers.

A review of the forensic image of the server revealed a transfer of approximately 0.00228809 BTC (worth about $1.80 at the time of transaction) on December 17, 2016 from a BTC address to The Website's BTC address starting with 1Hrb.[4] Subpoena returns from a virtual-currency exchange in the United States ("BTC Exchange") revealed that the source of this BTC transfer was from BTC Exchange Account number starting with 5855 ("Subject BTC Exchange Account").[5]

[4] BTC addresses are identified by their first four characters, much like bank account are often identified by their last four numbers.

[5] On December 17, 2016, the, Subject Exchange Account sent approximately 0.1025 BTC and 0.005 BTC (worth about $80.97 and $3.95 respectively at the time of transactions) to a BTC mixer.

Law enforcement's review of the forensic image of the server revealed that The Website created the BTC address starting with 1Hrb for a user account in the name of thisthishold (as noted, each user account on The Website received a unique BTC address to receive payments from that person). A review of co-conspirator thisthishold's account revealed that between approximately May 31, 2017 and February 9, 2018, co-conspirator thisthishold downloaded approximately 174 videos from The Website with video file names and descriptions indicative of child pornography. Additionally, from approximately June 25, 2016 to December 21, 2016, co-conspirator thisthishold uploaded approximately 560 videos to The Website – all of which are videos that depict child pornography.

Your affiant reviewed co-conspirator thisthishold's uploads to The Website and confirmed the videos depicted child pornography. For example, video file EA - N2016H-034.mp4 with file description "EA - N2016H-part" was uploaded to The Website by co-conspirator thisthishold on November 20, 2016. The video is 19 seconds long and depicts a female child, approximately five to seven years old, nude from the waist up. The child appears to be laying on her back while an adult male stands over her and masturbates his penis near her mouth until he ejaculates on her face. The video ends with a collage of photographs of the same child with semen on her face. Users of The Website downloaded this video approximately two times.

Another video, entitled 20150805201415-031.mp4 with the file description "20150805201415-part" was uploaded to The Website by co-conspirator thisthishold on December 20, 2016. The video is 24 seconds long and depicts a female child, approximately five to seven years old, nude from the waist down. The child appears to be laying on her back, viewing a computer tablet, while a male adult inserts the head of his penis into the child's vagina. Users of The Website downloaded this video approximately three times.

Subpoena returns from the BTC Exchange revealed that the Subject BTC Exchange Account (which sent BTC to The Website) was created on or about December 17, 2016 with the following know-your-customer data:

- registered in the name of VINCENT GALARZA ("GALARZA");
- with a date of birth of XX/XX/XXXX;
- address of ;

A BTC mixer is a paid service that attempts to obfuscate the trail of BTC by mixing multiple clients' transactions together so that there is not a direct trail from the BTC sender to the recipient. On December 17, 2016, The Website BTC address starting in 1Hrb also received approximately 0.09882853 BTC from a mixer. Based on my discussions with IRS-CI Cyber Crimes Unit investigators, it appears GALARZA attempted to fund his account at The Website for a 0.1 BTC VIP account by sending the approximate 0.1025 BTC. However, he did not account for the normal BTC transactional fees and the mixer's fees. Thus, he had to send an additional smaller BTC amount from 1Hrb to The Website and he chose to forgo the mixer with his third transaction to The Website – *i.e.*, the approximately 0.00228809 BTC transaction described above.

- using a phone number of XXX-XXX-XXXX; and
- an email address of .

As part of the BTC Exchange's legally required customer due diligence rules, the BTC Exchange confirmed this email address and phone number by sending messages to which the user had to reply.

Subpoena returns from Oath revealed that the email address of [redacted] was created on December 15, 2002 and is registered to Vincent Galarza (GALARZA) with the same telephone number that GALARZA provided when he created the Subject BTC Exchange Account on December 17, 2016.

The Subject BTC Exchange Account was funded by a Cross County Savings Bank ("CCSB") checking account ending in 0160 and a Chase Bank credit card ending in 8140. Subpoena returns revealed that both of these payment methods were listed in GALARZA's name. The subpoena returns further revealed that GALARZA opened the account ending in 0160 in 2008. GALARZA provided the same date of birth, phone number, and address when he opened his accounts that he had provided to the BTC Exchange when he opened the Subject BTC Exchange Account. GALARZA had also provided copies of his driver's license and Social Security card when he opened his account with CCSB as well. Subsequent law enforcement investigation identified CCSB ATM security footage from December 26, 2017, which depicts an individual resembling GALARZA's driver's license photograph accessing a CCSB ATM.

CONCLUSION

Numerous co-conspirators, to include co-conspirator GALARZA, conspired with the administrator of The Website, co-conspirator Jong Woo Son, to upload child pornography videos files to The Website for dissemination to The Website's vast customers. The co-conspirators entered into this agreement to benefit:

a. co-conspirator Jong Woo Son, who obtained illicit income as co-conspirators uploaded more video files to The Website, which other customers then paid to access; and

b. co-conspirator GALARZA, who derived points from uploading videos and further points from the uploads when users of The Website downloaded his videos, and these points could then be redeemed to download new video files from The Website.

Accordingly, based on the above facts, your affiant submits that there is probable cause to believe that between at least on or about June 25, 2016 and on or about December 21, 2016, GALARZA committed the offense of Conspiracy to Distribute Child Pornography, in violation of Title 18, United States Code, Sections 2252(a)(2) and (b)(1).

SA Darrell Franklin
HSI

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 based on information communicated by telephone on this 4th day of December, 2018

Honorable Judge Robin M. Meriweather
United States Magistrate Judge