

STATE OF CONNECTICUT : Filed Under Seal
: ss: Bridgeport, Connecticut
COUNTY OF FAIRFIELD : December 12, 2022

AFFIDAVIT IN SUPPORT OF COMPLAINT AND ARREST WARRANT

I, Stephanie Kooharian, being duly sworn, depose and state as follows:

INTRODUCTION AND AFFIANT BACKGROUND

1. I submit this affidavit in support of a criminal complaint and arrest warrant charging CHRISTOPHER BATES JR. (“BATES”), an adult male born in 1986 and currently residing at an address known to me in Old Greenwich, Connecticut (the “Old Greenwich Address”), with the following criminal offenses: receipt of child pornography, in violation of 18 U.S.C. § 2252A(a)(2), and possession of child pornography, in violation of 18 U.S.C. § 2252(a)(5)(B) (collectively, the “TARGET OFFENSES”).

2. I have been employed as a Special Agent (“SA”) of Homeland Security Investigations (“HSI”) since May 2021, and am currently assigned to the HSI office of the Resident Agent in Charge in New Haven, CT. Prior to my employment with HSI, I was a Detective with the Manchester, NH Police Department from 2016 to 2021. Additionally, I was a Police Officer with the Central Intelligence Agency from 2014 to 2016 and the United States Capitol Police from 2012 to 2014. I graduated from the New Hampshire Police Standards and Training Academy Class 172, the Uniformed Police Training Program at the Federal Law Enforcement Training Center (“FLETC”) Class 212, and the Criminal Investigator Training Program at the FLETC Class 2204. I have received training from the Manchester NH Police Department, New Hampshire Police Standards and Training full-time Police Academy, United States Capitol Police, Central Intelligence Agency, and the FLETC. I have also received additional training from other police

agencies pertaining to the continued investigations of criminal activity. I have gained experience through training at the ICE-HSI Special Agent Training course and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media.

3. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7) in that I am empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516. I have personally participated in the investigation concerning the violations of the federal law listed in this affidavit.

4. The statements contained in this affidavit are based in part on information provided by other members of local, state, and federal law enforcement, my own investigation to include personal observations, documents and other investigative materials which I have reviewed, as well as my training and experience as a Special Agent with HSI. Since this affidavit is being submitted for the limited purpose of obtaining a criminal complaint and arrest warrant, I have not included 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 BATES committed the TARGET OFFENSE.

THE TARGET OFFENSES

5. As noted above, this investigation concerns possible violations of the following offenses:

a. 18 U.S.C. § 2252A(a)(2) provides that a person who “knowingly receives or distributes (A) any child pornography using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; or (B) any material that contains child pornography using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer . . . shall be [guilty of a crime.]”

b. 18 U.S.C. § 2252A(a)(5)(B) provides that a person who “knowingly possesses, or knowingly accesses with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any 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 in or affecting interstate or foreign commerce by any means, including by computer . . . shall be [guilty of a crime.]”

DEFINITIONS

6. The following definitions apply to this Affidavit:

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

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

7. “Sexually explicit conduct,” as used herein, is defined by 18 U.S.C. § 2256(2)(A) to mean actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the anus, genitals, or pubic area of any person.

BACKGROUND ON THE ONION ROUTER (“TOR”) AND THE “DARKWEB”

8. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are uniquely identified by Internet Protocol (“IP”) addresses, which are used to route information between Internet-connected devices. Every computer device connected to the Internet has an IP address assigned to it, which is used to route Internet traffic to or from the device. A device’s IP address can generally be used to determine the device’s physical location and, thereby, its user. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. On the Internet, data transferred between devices is split into discrete packets, each of which has two parts: a header with non-content routing and control information, such as the

packet's source and destination IP addresses; and a payload, which generally contains user data or the content of a communication.

9. "Tor," which is an acronym for "The Onion Router," is a special network of computers on the Internet, distributed around the world, that is designed to conceal the true IP addresses of computers on the network and, thereby, the identities of the network's users. To access the Tor network, a user must install Tor software. That is most easily done by downloading the free "Tor browser" from the Tor Project, the private entity that maintains the Tor network, via their website at www.torproject.org.¹ The Tor browser is a web browser that is configured to route a user's Internet traffic through the Tor network.

10. As with other Internet communications, a Tor user's communications are split into packets containing header information and a payload, and are routed using IP addresses. In order for a Tor user's communications to be routed through the Tor network, a Tor user necessarily (and voluntarily) shares the user's IP address with Tor network relay computers, which are called "nodes." This routing information is stored in the header portion of the packet. As the packets travel through the Tor network, each node is able to see the address information of the previous node the communication came from and the next node the information should be sent to. Those Tor nodes are operated by volunteers – individuals or entities who have donated computers or computing power to the Tor network in order for it to operate.

11. Because a Tor user's communications are routed through multiple nodes before reaching their destination, when a Tor user accesses such an Internet website, only the IP address of the last relay computer (the "exit node"), as opposed to the Tor user's actual IP address, appears

¹ Tor users may also choose to manually configure a web browser or other application to route communications through the Tor network.

on that website's IP address log. In addition, the content of a Tor user's communications is encrypted while the communication passes through the Tor network. That can prevent the operator of a Tor node from observing the content (but not the routing information) of other Tor users' communications.

12. The Tor Network also makes it possible for users to operate or access websites that are accessible only to users operating within the Tor network. Such websites are called "hidden services" or "onion services," which are utilized to access unmonitored portions of the internet, commonly referred to as the "darkweb." They operate in a manner that attempts to conceal the true IP address of the computer hosting the website. Like other websites, hidden services are hosted on computer servers that communicate through IP addresses. However, hidden services have unique technical features that attempt to conceal the computer server's location.

13. Unlike standard Internet websites, a Tor-based web address is comprised of a series of either 16 or 56 algorithm-generated characters, for example "asdlk8fs9dfiku7f," followed by the suffix ".onion." Ordinarily, investigators can determine the IP address of the computer server hosting a website (such as www.justice.gov) by simply looking it up on a publicly available Domain Name System ("DNS") listing. Unlike ordinary Internet websites, however, there is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a Tor hidden service. So, while law enforcement agents can often view and access hidden services that are facilitating illegal activity, they cannot determine the IP address of a Tor hidden service computer server via public lookups. Additionally, as with all Tor communications, communications between users' computers and a Tor hidden service webserver are routed through a series of intermediary computers. Accordingly, neither law enforcement nor hidden-service users

can use public lookups or ordinary investigative means to determine the true IP address – and therefore the location – of a computer server that hosts a hidden service.

PROBABLE CAUSE

DarkWeb Leads

14. HSI Boston, working with foreign law enforcement and a Child Exploitation Operational Unit within the FBI, is investigating individuals accessing darkweb sites/forums, operating on the Tor network, dedicated to the sexual abuse and exploitation of children. Through this investigation, law enforcement has identified hundreds of sexual abuse/child exploitation leads across the country.

15. Through this investigation, HSI Boston Special Agents received information, from a foreign law enforcement partner, that on April 24, 2019 at 04:32:49 UTC an individual using IP address 68.199.218.130 (the “Subject IP Address”) accessed a known darkweb chat site whose primary purpose is to share and distribute child pornography. The advertisement and distribution of child pornography and child erotica are regular occurrences on this site. On the front page of the site, it states that the site is intended for users to “post links with good photos and videos” depicting “[o]nly GIRLS 5 to 13 years [old].”

16. HSI Boston Special Agents also received information, from a foreign law enforcement partner, that on June 2, 2019 at 03:34:49 UTC an individual using the Subject IP Address accessed a known darkweb site that facilitated the sharing of child sexual abuse and exploitation material. This darkweb site contained child sexual abuse and exploitation material, with an explicit focus on the facilitation of sharing child abuse material (images, links and videos), emphasis on babies and toddlers (ages 0-5 years old). Users were required to create an account (username and password) in order to access the majority of the site and hosted material.

17. According to publicly available information, the Subject IP Address is owned/operated by Optimum Online. According to subscriber records provided by Optimum Online, the Subject IP address was assigned to subscriber “CHRISTOP BATES” at the Old Greenwich Address on April 24, 2019 at 04:32:49 UTC and June 2, 2019 at 03:34:49 UTC, which are the dates and times the Subject IP Address was used to access the child pornography websites described above.

18. A public records report accessed through CLEAR for information on an individual with a last name of Bates located at the Old Greenwich Address produced a result for Christopher Bates with a year of birth of 1986 and a possible last known address of the Old Greenwich Address. CLEAR listed a possible work affiliation with an international realty company, whose identity is known to me.

19. A driver query conducted in Connecticut for Christopher Bates with a year of birth of 1986 indicated that he has a current driver’s license with a primary contact address of the Old Greenwich Address.

20. An open source search on the internet revealed a publicly available LinkedIn profile for Christopher Bates in Greenwich, Connecticut that listed his current work experience at the international realty company described above. The LinkedIn profile further indicated that Christopher Bates is an attorney admitted to practice in New York and Connecticut.

Bates’ Interview with Law Enforcement on November 30, 2022

21. On November 29, 2022, HSI New Haven SAs Stephanie Kooharian and Brendan Lundt attempted to conduct an interview with BATES at the Old Greenwich Address with negative results. On the same date at approximately 1053 hours, SA Kooharian made contact with BATES

over the phone, who advised he was in Florida and would be flying home later in the day. SA Kooharian made arrangements to meet with BATES at his residence on November 30, 2022.

22. On November 30, 2022, at approximately 1020 hours, SA Kooharian made phone contact with BATES to confirm the location, at which time, BATES requested to meet at the Greenwich Police Department (“GPD”). At approximately 1115 hours, SA Kooharian and SA Steven Mullen, along with GPD Detective Jim Manning met BATES in the lobby of the GPD. SAs Kooharian and Mullen showed BATES their credentials and identified themselves and invited BATES to the interview room at the Detective Division of GPD.

23. The interview was audio and video recorded. BATES was advised the room was audio and video recorded and that he was free to leave at any time. SA Kooharian advised BATES the door was shut for privacy, but if he wanted to leave at any time, he was free to leave.

24. SA Mullen began the interview by confirming BATES’ personal information. BATES stated he has lived at the Old Greenwich Address, CT for approximately three to four years. BATES stated he lived alone and no one else has lived with him at that address. BATES confirmed that he is an attorney.

25. SAs Kooharian and Mullen explained the reason for the interview. SA Kooharian presented a report to BATES detailing some facts of the case to include, but not limited to, dates the Subject IP Address accessed the darkweb sites/forums and subscriber information from Optimum Online.

26. BATES stated he accessed the darkweb on several occasions over the years to view child pornography. BATES stated he most recently viewed child pornography approximately one month ago via a laptop that was currently stored in a storage unit located in the basement of the

building he resided in. BATES stated he recently moved the laptop to the storage unit as a way to deter him from accessing the darkweb to view child pornography.

27. BATES stated he utilized Tor to access the darkweb, and he identified two websites where he viewed child pornography. BATES stated he accessed additional websites that contained child pornography, but he could not remember the names.

28. SAs Kooharian and Mullen asked BATES if he would consent to a search of the laptop and other devices in which he utilized to access the darkweb. BATES agreed and signed a Consent to Search Form. At that time, BATES provided passwords for some of the devices.

29. At approximately 1220 hours the same day, BATES agreed to accompany SAs Kooharian and Mullen, and Detective Manning to his residence where he would voluntarily turn over several electronic devices. While at the residence, BATES turned over four laptop computers which he stated he “probably” utilized to view child pornography as well as six external hard drives and two tablets.

30. Because BATES is an attorney, SAs Kooharian and Mullen asked BATES if there would be any privileged information on the devices he provided. BATES indicated that there could be work related information on the devices, but there should not be any privileged information on the devices. BATES indicated that he did not turn over the computer that he currently uses for work purposes.

31. At approximately 1519 hours the same day, SA Mullen received the following email from the email address, cbatesjr[REDACTED]:

Dear Steven,

First, I wanted to thank you both for being very professional and very kind, even if I feel like I don't deserve it. You mentioned you could refer me to a therapist, and I'd very much appreciate it. My mother also recommended a therapist who had helped one of her

friends, I've left him a message and am waiting to hear how soon I can get in to see him. I hope that therapy can help me with some of my other problems as well; I think all of my issues with sexuality and self esteem and my weight seem to reinforce each other. My mother said she thought there was something wrong for a long time. I thought I was OK at faking being happy, but I was wrong. As bad as I feel right now, in a way it felt good to finally be honest with someone, and that makes me hopeful that therapy will help me, and maybe there's appropriate medication to help me as well.

I don't know if it's something you hear often from people in my situation, but I really do want to thank you, because it's awful to think about continuing to go on like I was, and I think maybe now I have a chance to change who I am. If you can relay that to Stephanie (or Stefanie, I didn't see how she spelled her name, sorry), I would appreciate it as well.

Best Regards,
Chris Bates

Forensic Examination of Bates' Laptop

32. On December 1, 2022, SA Colin Hartnett turned over all 12 items of electronic media BATES provided to Taskforce Officer ("TFO") Paul Fressola for electronic review. TFO Fressola conducted a forensic preview of one of the laptops, a Dell XPS laptop bearing serial number FPXTTF2 ("Laptop-1").²

33. On December 2, 2022, TFO Fressola notified SA Hartnett that he located approximately 1000 images of child pornographic material from the forensic preview of Laptop-1. Based on SA Hartnett's training and experience in working child exploitation cases and on his personal review of the images, he believes images depict child pornography and appear to focus on girls from the infant age to preteen/early teen ages. The images showed these young girls performing oral sex on adult males, being penetrated by adult male penises, and bondage.

² A full forensic examination of all of the electronic devices is ongoing.

34. I have reviewed some of these images and, based on my training and experience, I believe they depict child pornography. Three of the images are described below.³ The images are identified by their SHA1 hash value, which is a unique identifier associated to all digital images.

Item #	SHA1 Hash	Description
1	ab25acc3b817db68f775898d00c78162a884e10	An image depicting an infant child approximately 6 months of age with an adult penis ejaculating on the face of the infant child.
2	1db7ef49163ed851b4dcddd4f75e3fb27ace12f3b	An image depicting an approximately 6-8 year-old nude female with a knife pointed at her chest. The female's vagina is visible in the image. The words "cut me slut hurt me" are written on her body in red. The knife is being held by another individual.
3	3c451455c5139e87781f9f0b0719e37bdc780b46	An image depicting an approximately 5-7 year-old nude female performing oral sex on an adult male. A second adult male behind the female child appears to be having sexual intercourse with her.

CONCLUSION

35. Based upon the foregoing, there is probable cause to believe, and I do believe, that from on or about April 24, 2019, to on or about November 30, 2022, the exact dates being unknown, in the District of Connecticut, BATES committed the TARGET OFFENSES, that is he received and possessed child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2) and 2252A(a)(5)(b).

³ I have described images where I believe a minor (a person under the age of 18) is engaged in sexually explicit conduct. My assessment is based on my experience working child exploitation cases and on my personal review of the image. In making this assessment, I consider the totality of the circumstances including the "minor's" physical size (height/weight); hair in the auxiliary areas (pubic area or under the arms) and development of the sexual organs (such as breasts in females). In circumstances in which I am uncertain if an image depicts a minor, I would describe it as "age difficult" or "child erotica."

36. Therefore, I respectfully request the issuance of a criminal complaint and arrest warrant to charge and arrest BATES with the TARGET OFFENSES.

Stephanie M KOOHARIAN
Special Agent
Homeland Security Investigations
Digitally signed by STEPHANIE M KOOHARIAN
Date: 2022.12.12 12:51:04 -05'00'

The truth of the foregoing affidavit has been attested to me by Special Agent Stephanie Kooharian over the telephone on this 12th day of December, 2022, at Bridgeport, Connecticut in accordance with the requirements of Fed. R. Crim. P. 4.1.

S. Dave Vatti
Digitally signed by S. Dave Vatti
Date: 2022.12.12 14:06:13 -05'00'
HON. S. DAVE VATTI
UNITED STATES MAGISTRATE JUDGE