

AFFIDAVIT OF FBI SPECIAL AGENT ADAM STRODE

I, Adam Strode, having been duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (“SA”) of the Federal Bureau of Investigation (“FBI”). I have been so employed since 2015. I am currently assigned to the Boston Division, Worcester Resident Agency. My duties include the investigation of violations of the United States Code. Pursuant to my employment with the FBI, I have participated in various criminal investigations, and have been the affiant on federal search warrants and court orders. I have directly participated in numerous criminal investigations for violations of federal law to include bank fraud, identity theft, child exploitation, and healthcare fraud. I have received on-the-job training and have attended FBI-sponsored training courses on the investigation of criminal violations. I have conducted and participated in the execution of search and arrest warrants, physical surveillance, interviews of cooperating witnesses, and reviews of documents and evidence.
2. I submit this affidavit in support of an application for an arrest warrant and criminal complaint charging Gregory LISBY with possession of child pornography, in violation of Title 18, United States Code § 2252A(a)(5) (the “Subject Offense.”)
3. The facts in this affidavit come from my training and experience, my review of relevant records, and information obtained from other agents, law enforcement officers, and civilian witnesses. This affidavit includes only those facts I believe are necessary to establish probable cause for the issuance of the requested complaint warrant and does not include all of the facts uncovered during the investigation.

RELEVANT STATUTES

4. Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting or conspiring to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), 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.
5. “Child pornography” is defined in 18 U.S.C. § 2256(8) as 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.
6. The term “minor” is defined in 18 U.S.C. § 2256(1) as any person under the age of eighteen years.

FACTS ESTABLISHING PROBABLE CAUSE

A. Identification of Child Pornography within the TARGET ACCOUNT

7. On December 17, 2018 at 17:05:15 UTC, NCMEC received CyberTip Report #44377012 from Microsoft Corporation (“Microsoft”), a registered Electronic Service Provider.¹

¹ An “Electronic Communication Service Provider” (“ESP”) is defined in 18 U.S.C. § 2510(15) as any service which provides to users thereof the ability to send or receive wire or electronic communications.

8. According to Cybertip Report #44377012, on December 17, 2018 at 14:58:46 UTC, a digital file with the file name “6aae7237-fb28-40a3-85d6-52cee6b43516.jpg” (hereinafter the “SUBJECT FILE”) was uploaded to servers owned by Microsoft Corporation, specifically the OneDrive service, by an individual using the screen/user name “844427362124387,” i.e. the TARGET ACCOUNT. The user of the TARGET ACCOUNT utilized IP address 71.87.214.73 to upload the SUBJECT FILE. According to CyberTip Report #44377012, a Microsoft employee viewed the contents of the SUBJECT FILE and determined that it contained child pornography, then reported the upload to NCMEC.
9. NCMEC transmitted the SUBJECT FILE, along with CyberTip Report #44377012, to Massachusetts State Police on January 4, 2019 at 18:34:06 UTC.
10. I reviewed the SUBJECT FILE identified by Microsoft. The SUBJECT FILE depicts two males engaged in anal sex. Male1 appears to be kneeling on the ground facing a bed, resting his torso on the mattress. Male2 is kneeling behind Male1 and appears to be penetrating Male1’s anus with his penis. The penis of Male2 is partially visible. The faces of Male1 and Male2 are both partially visible. Neither boy has visible facial hair or body hair. Based upon their size and the lack of facial and body hair, I estimate that both boys are between 11 and 14 years old.
11. On August 27, 2019, Microsoft Corporation provided the contents of the TARGET ACCOUNT in response to federal search warrant 19-mj-4468-DHH that was issued on August 8, 2019.

12. Investigators reviewed the data provided by Microsoft for the TARGET ACCOUNT and identified approximately 180 images that appear to depict child pornography. Investigators also found approximately 15 videos that appear to depict child pornography.
13. Data from Microsoft was categorized as “preserved” and “current.” Within both directories, I located two folders named “Inside” and “CADE” that contained images. Based upon my training and experience, I believe that the designation “current” indicates that the file was active in the account as of the date Microsoft prepared the data, on approximately August 15, 2019. The data was produced to the FBI on August 27, 2019.
14. Specifically, within the “Inside” folder, which appears to have been added to the OneDrive account on December 17, 2018, there were approximately 140 images that, based upon my review, appear to depict child pornography. The “upload IP” address for all of the images contained within the “Inside” folder was 71.87.214.73, which is the same IP address used to upload the SUBJECT FILE.
15. Amongst the files saved within the “Inside” folder was a file named “twlba5j7o5gj5.onion.jpg” This file appears to me to contain the same image as the SUBJECT FILE from Microsoft’s initial Cybertip, more particularly described in paragraph 10, though it has a different filename. A comparison of the hash values of those two files confirmed that they are identical.
16. On September 4, 2019, the FBI computed the hash value of 146 files from the “Inside” folder. Those hash values were submitted to NCMEC.
17. On September 4, 2019, NCMEC sent a response to the FBI via an “Initial Hash Value Comparison Report”, which identified 33 of those submitted hash values as containing an “Identified Child.” Specifically, the file named “twlba57oo5g4kj5.onion.jpg” depicts two

males engaged in anal sex. Male1 is naked and his face is visible. Male1's anus is being penetrated by Male2's penis. Male2's face is not visible. Male1 has a small build and no facial or body hair. I estimate Male1's age to be between 8 years old and 12 years old. Only a portion of Male2's stomach, leg, hand, and penis are visible. Based on Male2's size and visible body hair, I estimate that Male2 is an adult over the age of 18.

18. The contents of the TARGET ACCOUNT also contained a folder entitled "CADE," which appears to have been added to the TARGET ACCOUNT on December 13, 2018. The "upload IP" address for all of the files in the "CADE" folder was 71.87.214.73, which is the same IP address used to upload the SUBJECT FILE.
19. I reviewed the contents of the CADE file and observed approximately 50 images that appear to be of one unidentified minor male. The majority of these images contain apparent child pornography. For example, a file named "467575ce-efbf-41dc-aa7c-1ea47c4882ca" depicts a naked male standing with his hands behind his head and his genitals fully visible. Based upon his slight frame, he appears to be approximately 12-15 years old. The image appears to be a picture taken by the boy of his own reflection in the mirror. His face is fully visible.
20. The CADE file also included several videos. The video file named "766e2b2c-5bac-4285-9cf6-9c44ef9b4310" appears to depict the same male as seen in the still images. In the video, the boy is naked and masturbating on a bed. The boy's face and penis can be seen.
21. On September 4, 2019, a NCMEC Initial Hash Value Comparison Report was generated containing the hash values from 54 files from the "CADE" folder. NCMEC responded that all of the hash values were unrecognized.

22. The records provided by Microsoft Corporation for the TARGET ACCOUNT included evidence of the download and use of a TOR Browser.² In addition, a number of the files containing apparent child pornography within the folder entitled “Inside” have file names that include “.onion.jpg.” “.onion”, is a domain suffix designating an anonymous onion service (also known as a “hidden service”) that can be reached via the TOR network. Based on my training and experience, I know that individuals will use TOR to share files containing child pornography in order to minimize detection of their online activity.

B. IDENTIFICATION OF LISBY

23. Account data provided by Microsoft for the TARGET ACCOUNT listed the subscriber name as “Greg Lisby,” with a sign-in name of “glisby@gmail.com” and an account creation date of May 19, 2009.

24. Further review of the data provided by Microsoft identified several word documents that appear to belong to Greg LISBY. A Word document entitled “Document 1” appears to be an introduction letter written by LISBY for an online course. The document states “...My name is Greg Lisby, and I recently applied to the PBTL in Early Childhood Education.” The letter then further states, “...If I could teach any grade, I would love to be a kindergarten teacher. The joy, spontaneity, and openness to learning of younger children is what attracts me to early childhood education. Plus, the energy of the kids, and the energy required of the teacher is exhilarating and tiring.” That file appears to have been added to the TARGET ACCOUNT on September 3, 2018 and modified on September 28, 2018.

² TOR (The Onion Router) is free and open-source software for enabling anonymous communications. TOR directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays to help conceal a user’s location and usage from anyone conducting network surveillance or traffic analysis. In order to access TOR specific websites a user needs to use a TOR browser or a proxy gateway.

25. A file entitled “Charge Letter 2 – 1-21-18” is a Word document which appears to have been added to the TARGET ACCOUNT on approximately January 23, 2018. It appears to be a letter from the Intake Coordinator for the diocese and is addressed to “The Rev. Gregory C. Lisby, [REDACTED] Whitman Rd, Worcester, MA 01609-1728.”

26. A Word document entitled “2018-Greg Lisby-School 3” appears to be LISBY’s resume. The document appears to have been added to the TARGET ACCOUNT August 13, 2018. The top of the document states, “Gregory C. Lisby, [REDACTED] Pleasant St. Worcester, MA 01602, (401) [REDACTED], [REDACTED]@gmail.com.”

27. On or about January 22, 2019, Charter Communications provided the following records in response to a subpoena requested by Massachusetts State Police for customer records related to the assignment of IP address 71.87.214.73, the IP address used to upload the SUBJECT FILE, the apparent child pornography within the “Inside” folder, and others:

Service Address: [REDACTED] Pleasant Street Worcester, MA

Lease record: November 4, 2018 through January 20, 2019

Name: Timothy Burger

Billing address: [REDACTED] Pleasant Street Worcester, MA 01602

Contact Email: [REDACTED]@gmail.com

Active Charter Identities: [REDACTED]@charter.net; [REDACTED]@charter.net.

Primary Phone Number: 401-[REDACTED]

28. On May 23, 2019, investigators conducted a public records database search for [REDACTED] Pleasant Street, Worcester, Massachusetts. That query identified Timothy Burger, born 1978, as living at this address from August 2015 to April 2019. That same query also identified LISBY as living at [REDACTED] Pleasant Street from August 2015 to May 2019.

29. An internet search of publicly available databases indicates that Timothy Burger and LISBY are married.

30. On May 23, 2019, a query of the Massachusetts Registry of Motor Vehicles (“RMV”) database identified an active Massachusetts license issued to Timothy H. Burger with an address of [REDACTED] Pleasant Street, Worcester. The query of the RMV database also identified an active Massachusetts license issued to LISBY with an address of [REDACTED] Pleasant Street, Worcester.

31. Publicly available information online indicates that LISBY was employed as a kindergarten teacher for the Holyoke Public Schools for the 2019-2020 school year. On September 10, 2019, a red 2017 Toyota Prius bearing Massachusetts registration 5XX463 registered to Gregory LISBY’s was observed parked in an elementary school parking lot in Holyoke.

C. EXECUTION OF SEARCH WARRANT AT 919 PLEASANT STREET

32. On September 11, the Court issued a warrant authorizing the search of [REDACTED] Pleasant Street, Worcester. 19-mj-4490-DHH. FBI executed the warrant that same day, at approximately 5:40 p.m., and encountered LISBY at the home.

33. After being advised of his rights pursuant to Miranda, LISBY stated that he used the email address [REDACTED]@gmail.com and phone number of (401) [REDACTED], i.e. the email address and phone number associated with the TARGET ACCOUNT. LISBY requested an attorney before agents asked him about the contents of the TARGET ACCOUNT.

34. Agents also interviewed Timothy Burger. Burger and LISBY separately identified a bedroom on the second floor of the home as belonging exclusively to LISBY.

35. Within LISBY’s bedroom, agents found an iPad and a OnePlus mobile phone. Both devices were secured with a passcode.

36. Agents were able to gain access to the iPad found in LISBY's bedroom. The iPad had an application for Microsoft OneDrive installed on it. The stored credentials within the application included a sign-in name of [REDACTED]@gmail.com.
37. Agents were also able to gain access to the OnePlus mobile phone. They found the Microsoft OneDrive application installed. The stored credentials for OneDrive included a sign-in name of [REDACTED]@gmail.com.
38. Agents performed a preliminary review of the contents of the OneDrive account on both the iPad and OnePlus phone. They found file names that match those of the Word documents stored within Target Account described in paragraphs 24, 25, and 26. They were unable to open the actual files. The images of apparent child pornography that were included in the Microsoft OneDrive return were not found during the initial review of the contents of the OneDrive account as accessed from the iPad and OnePlus mobile phone. The absence of these images and videos suggests that they were removed from the TARGET ACCOUNT at some point after Microsoft had produced records responsive to the federal search warrant in August 2019.
39. On September 12, 2019, the Receiver/Superintendent of Holyoke Public Schools, contacted the FBI to report an email that had been received from [REDACTED]@gmail.com. The email was directed to the principal of the elementary school that employed LISBY as a kindergarten teacher and read:

"From: **Gregory Lisby** [REDACTED]@gmail.com>
Date: Thu, Sep 12, 2019 at 2:32 AM
Subject: Resignation
To: [Principal]

Dear [Principal],

Last night, I was accused of an awful crime that could put our Holyoke children in harms way.

Please accept this email as my letter of resignation, effective immediately.

I will have my computer and key delivered to [elementary school] by early next week.

My apologies for this terrible situation and its affect on [elementary school].

Sincerely,

Greg Lisby”

CONCLUSION

40. Based on the foregoing, I submit that there is probable cause to believe that LISBY has committed violations of Title 18, United States Code § 2252A (a)(5)(B), namely the possession of child pornography.


41. WHEREFORE, your affiant respectfully requests that the Court issue a criminal complaint charging Gregory LISBY with the SUBJECT OFFENSE.

Sworn to under the pains and penalties of perjury,




Special Agent Adam Strode
Federal Bureau of Investigations

Subscribed and sworn to before me this 12th day of September, 2019.


Hon. David H. Hennessy
United States Chief Magistrate Judge

I have reviewed images described above in Paragraphs 10, 15, 17, and 19, as well as the still shot image from the video described in Paragraph 20, and I find probable cause to believe that those images depict minors engaged in sexually explicit conduct. The U.S. Attorney's Office shall preserve the images provided to the Court for the duration of the pendency of this matter, including any relevant appeal process.


Hon. David H. Hennessy
Chief United States Magistrate Judge