

UNITED STATES DISTRICT COURT
for the

United States of America
v. District of Massachusetts

Case No. 19-mj-5060-JGD

MATTHEW MURPHY

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of 11/22/18-12/13/18 and 7/21/18 in the county of Plymouth in the
District of Massachusetts, the defendant(s) violated:

Table with 2 columns: Code Section, Offense Description. Row 1: 18 U.S.C. §§ 2251 a) and e), sexual exploitation of children, on various dates between on or about November 22, 2018 and December 13, 2018. Row 2: 18 U.S.C. §§ 2251 a) and e), sexual exploitation of children, on or about July 21, 2018.

This criminal complaint is based on these facts:

Please see the affidavit of HSI Special Agent Janet Connolly, which is attached hereto and incorporated by reference.

Continued on the attached sheet.

[Redacted signature]

Complainant's signature

Janet Connolly, Special Agent, HSI

Printed name and title

Sworn to before me and signed in my presence.

Date: 03/26/2019

[Redacted signature]

City and state: Boston, MA

Hon. Judith G. Dein, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT OF SPECIAL AGENT JANET CONNOLLY
IN SUPPORT OF A CRIMINAL COMPLAINT**

I, Janet Connolly, Special Agent with the Department of Homeland Security, Homeland Security Investigations, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with United States Department of Homeland Security “DHS”), Immigrations and Customs Enforcement, Homeland Security Investigations “HSI”), and am assigned to the office of the Special Agent in Charge, Boston, MA. I have been an agent of HSI since 2008. As part of my duties, I am authorized to investigate violations of the laws of the United States, including criminal violations relating to child exploitation, child pornography, coercion and enticement, and transportation of minors, including but not limited to violations of 18 U.S.C. §§ 2422, 2423, 2251, 2252, and 2252A. I have received training in the investigation of child pornography, child exploitation, and transportation of minors, and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256). In my five years of investigating these types of cases, I have participated in the execution of numerous search warrants involving child exploitation and/or child pornography offenses.
2. I submit this affidavit in support of a criminal complaint charging MATTHEW MURPHY (YOB 1996) with two counts of sexual exploitation of children, in violation of 18 U.S.C. §§ 2251(a) and (e).
3. The facts in this affidavit come from my own observations and review of records, my training and experience, and information obtained from other agents and witnesses. Because this affidavit is intended to show merely that there is probable cause to secure a criminal complaint, I have not included each and every fact known to me concerning this

investigation. Where statements of others are set forth below, they are set forth in substance and in part.

STATEMENT OF PROBABLE CAUSE

The Underlying Investigation

4. In November 2018, HSI Boston began an investigation regarding an individual utilizing a Snapchat account hereinafter, the “Suspect Account”¹ to sexually exploit a 14-year-old boy (“Minor A”). As part of that investigation, I obtained the following information from Minor A’s father:
5. Minor A reported to his father that he initially met the user of the Suspect Account via the “Stories” feature² on Snapchat. According to Minor A, the Suspect Account user initially presented him/herself as a young female. They began communicating via Snapchat. At one point, according to Minor A, the Suspect Account user named the specific Middle School that Minor A attends and demanded that Minor A send a naked photo of himself. Minor A felt pressured to do so because the Suspect Account user knew where he went to school, so he complied and sent the Suspect Account a photo of himself in boxer shorts. The Suspect Account user demanded that Minor A send a nude photo, and threatened to distribute the photo of Minor A in his boxer shorts around Minor A’s school. Minor A complied with the demands out of fear that his other photo would be spread throughout his school. Minor A sent a full-body, unclothed photo of himself to the Suspect Account.
6. The Suspect Account user continued to make demands of Minor A to send additional

¹ The username assigned to the account is redacted here because of the ongoing nature of the investigation.

² A Snapchat “Story” is a collection of a user’s photos, grouped in chronological order, to create a narrative. (See paragraph 17.)

sexually explicit or naked photos and/or videos. The Suspect Account user threatened the victim that, if he did not comply, the Suspect Account user would report Minor A to the police so that he would face legal repercussions and that he would expose private information and/or photos of Minor A to his entire school.

7. Minor A disclosed the threats and the Snapchat conversation to his parents, which prompted his father to provide Minor A's mobile phone to HSI for investigation.
8. A preliminary examination of the phone located the Snapchat application. A preview of the application revealed communications between Minor A and the Suspect Account, including the following:

November 22, 2018

Suspect Account: *What is your decision*

Minor A: what are the choices
?
plz no ill do anything but send again

Suspect Account: *Let me watch you shower
you alone rn?
Hit vid*

Minor A: no

Suspect Account: *Yup*

Minor A: y

Suspect Account: *Cuz I said*

Minor A: i'd rather deal with the cops then send again

Suspect Account: *I can be meaner?*

Minor A: how

Suspect Account: *Who's with you*

Minor A: no one

Suspect Account: *I'm not deaf*
Last chance

Minor A: it's the tv

Suspect Account: *Don't lie or I'll go Rn*

Minor A: go where
to the cops
i'll deal with the cops

Suspect Account: *And ur whole school*

Minor A: what you are doing rn is more illegal than what i did

Suspect Account: *Hmu tomorrow*
Don't ignore me

Minor A: ok

Suspect Account: *Show ur face*
Wtf

Minor A: i with my family i can't talk

Suspect Account: *Bet*
Wtf

9. On December 28, 2018, this Court authorized a warrant to search the contents of the Suspect Account from January 1, 2018 to the date of service of the warrant for evidence of violations of 18 U.S.C. §§ 2251, 2422(b), and 2252A.
10. Following service of the warrant, Snap Inc. returned records in response (hereinafter, “the search warrant return”), including the contents of preserved chats involving the Suspect Account. A preliminary review of the chats revealed that the user of the Suspect Account communicated with approximately 386 individuals during the time frame encapsulated in the search warrant return, most if not all) of whom appear to be minors based on the content of their chats. The messages between the Suspect Account and the other users

primarily concern the trading of sexually explicit images and videos. The Suspect Account user portrays himself as a teenaged female, between the ages of 13 and 17, depending on the age of the individual with whom he is communicating, and frequently claims to be a resident of Hingham, Massachusetts. Most of the users with whom the Suspect Account user communicated identify themselves as Massachusetts residents ranging from 12 to 17 years old.

11. Also included within the search warrant return were more than 1,000 image files and more than 200 video files that were exchanged by or with the Suspect Account, many depicting sexually explicit material.
12. Within the search warrant return, I observed chats between the Suspect Account user and Minor A, including and in addition to those outlined above. I also observed chats between the Suspect Account and other apparently minor users that were similar in nature to the Suspect Account chats with Minor A; that is, in which the Suspect Account user instructs the other users to send nudes and issues overt threats to expose the minors' sexually explicit images if they do not comply. In many such chats, the Suspect Account user sends images that appear to be screenshots of the minor users' sexually explicit Snaps. Based on the context of the chats, I believe the Suspect Account user sent such transmissions to underscore his ability to carry out his threats to distribute the sexually explicit or otherwise embarrassing material to the victims' friends on social media, their school, or the police. In multiple chats, the Suspect Account user indicates by text or screen shot that he knows the identity or location of particular minor users' schools or home addresses.
13. For example, on July 21, 2018, the Suspect Account messaged another Snapchat user

(hereinafter “Minor B”)³: *“I’m sharing your pics. I’m done with your bullshit lies / I’ll just make a group chat and send to all at once.”* Minor B, who appears in a photograph to be a male between the ages of 12 and 14, protests. The Suspect Account responds, *“I have ur insta / I’ll add everyone off ur followers,”* and texts the minor’s Instagram username to prove it. On the same date, the Suspect Account later instructs the minor to send a photo of his genitals, even though the minor explained he was in the back seat of his friend’s car. The Suspect Account user writes, *“You have a blanket on just hold ur phone in ur pants and send / Well it’s either you do that or I share with ur insta followers rn / Send the pic / Send.”* Hours later, the suspect messages the minor with two attachments: 8A9827A7-92B2-4B25-B7E8-688059B19276 and DF7DFE37-142D-45B4-B088-FFA5807350C6. Both attachments are images depicting a male pulling his pants down to expose his penis, from the perspective of the male pointing the camera down the front of his body. The male’s penis does not appear to have any pubic hair.⁴

14. During further review of these chats, I located a conversation dated September 22, 2018 between the Suspect Account and an individual who describes himself as a 17-year-old male. The Suspect Account user confides in the minor, “tbh ima guy.”⁵ When asked why he would pretend to be a girl, the Suspect Account user responds, “I may of catfished a few people....Like pretended to be a girl to get nudes.”⁶ The minor user asks the Suspect Account user his age, to which the Suspect Account user responds, “22.”

³ The username is known to law enforcement but redacted here in the interest of the minor’s privacy. Law enforcement has not confirmed the identity of Minor B.

⁴ These images are available for the Court’s review.

⁵ I am aware that “tbh” is typically used as an abbreviation of “to be honest.”

⁶ To “catfish” someone means “to deceive someone) by creating a false personal profile online.” Merriam-Webster Online Dictionary, last accessed March 18, 2019.

The Identity of the Suspect Account User

15. The search warrant return also included subscriber information, including over 2,000 IP⁷ logs during the timeframe covered by the warrant. Based on my review of publicly-available information, I determined that some of those IP addresses resolve to Comcast Cable Communications (“Comcast”).
16. On January 17, 2019, HSI Boston issued a summons to Comcast directing the company to provide subscriber information associated with five IPv4 addresses that were included in the search warrant return and fell within Comcast’s retention period. In response, Comcast provided the following information for those IPv4 addresses:⁸
 - a. The Wellesley address
IP: [REDACTED]
 - b. The Milton address
IPs: [REDACTED]
 - c. The Whitman address
IP: [REDACTED]
 - d. The SUBJECT PREMISES
IP: [REDACTED]

⁷ An Internet Protocol (IP) address is a numerical label used to identify a device on the internet or local network. There are two primary types of IP address formats: IPv4 and IPv6. IPv4 refers to the Internet Protocol Version 4 addressing scheme, which is the most widely deployed Internet protocol used to connect devices to the Internet. IPv4 addresses are represented by four sets of numbers separated by periods. IPv6 refers to the Internet Protocol Version 6 addressing system, which was developed in anticipation of IPv4 address exhaustion. IPv6 addresses are represented as eight groups of four hexadecimal digits i.e., 0-9 and A-F) separated by colons.

⁸ The entirety of the subscriber information is known to law enforcement but redacted in the interest of the individuals’ privacy. For the purposes of this affidavit, I refer to the individual addresses as a) “the Wellesley address;” (b) “the Milton address;” (c) “the Whitman address;” and (d) “the SUBJECT PREMISES.”

17. In response to the summons, Comcast also provided ranges of IPv6 addresses associated with each of these residential accounts as of the date of the summons (i.e., not historical).

The records for the SUBJECT PREMISES listed the following range⁹ of IP addresses:

Start address: [REDACTED]

End address: [REDACTED]

18. On February 28, 2019, HSI Boston issued a summons directing Comcast to provide historical IP logs associated with the SUBJECT PREMISES's account. On March 1, 2019, Comcast provided records of all IP addresses associated with the account from September 2, 2018 through February 28, 2019.¹⁰ Comcast's response indicated that during that time period, the account was assigned the IPv4 address [REDACTED] and IPv6 range [REDACTED] through [REDACTED] [REDACTED] (i.e., the same IP addresses as reported above).

19. I compared the IPv6 address range provided by Comcast to the Snapchat IP History logs. Almost all of the IPv6 addresses documented in the Snapchat History logs fell within the range of IPv6 addresses assigned to the SUBJECT PREMISES's Comcast account.¹¹

20. I further compared the Snapchat IP History logs (including IPv4 and IPv6 addresses) for the month of December 2018, during which the Snapchat records reflected approximately 114 logged IP addresses, as follows:

⁹ During a February 28, 2019 telephone conversation, Comcast representatives explained to me that a subscriber can have any one of thousands of IPv6 addresses within a particular range, and the range is exclusive to that subscriber. The range is represented by the first four groupings of numbers in the IPv6 address, referred to as a prefix. While the prefix remains constant, the last four groupings of numbers may vary.

¹⁰ Comcast's retention period for this data is 180 days.

¹¹ I observed approximately five IPv6 addresses in the Snapchat History logs that were not assigned to the SUBJECT PREMISES.

- a. Approximately two-thirds of the logged IP addresses (IPv4 and IPv6) resolved to the SUBJECT PREMISES;
 - b. One IPv4 log resolved to the Whitman address;
 - c. 17 IPv4 logs resolved to the Wellesley address; and
 - d. the remaining 20 IPv4 logs resolved to Verizon Wireless.
21. Based on my review of publicly-accessible information, including social media, I have determined the following about the subscriber information provided by Comcast:
- a. The female subscriber to the Comcast account for the SUBJECT PREMISES is the mother of 22-year-old Matthew MURPHY (YOB 1996);
 - b. The female subscriber to the Comcast account for the Whitman address is related to MURPHY's mother and is married to an employee of an electrical contracting business based in Hingham, MA; and
 - c. MURPHY is also employed at the same electrical contracting business.
22. On February 25, 2019, I reviewed Massachusetts Registry of Motor Vehicles (RMV) databases and located the following registration details:
- Matthew T Murphy
Date of Birth: xx/xx/1996
Address: [REDACTED]
23. Based on my review of other records, I have determined the following:
- a. Online permit records show that the electrical contractor for whom MURPHY works applied for an electrical permit at the Milton address on January 9, 2018. I am aware that such permits typically allow work to be performed within one year of issue.
 - b. Town of Wellesley records indicate that the electrical contractor for whom MURPHY works applied for an electrical permit at the Wellesley address in

December 2017 and the site was inspected on November 21, 2018. On January 13, 2019, the electrical contractor for whom MURPHY works posted photographs and comments to social media regarding its “recent Wellesley project.”

24. HSI agents reviewed the dates and times of the Snapchat IP logs, and noted that login/logout information associated with the Wellesley and Milton addresses occurred Mondays through Fridays during daytime hours, while login/logout information associated with the Whitman addresses also occurred during evenings and weekends.
25. On March 7, 2019, I conducted surveillance of the SUBJECT PREMISES. I detected several wireless networks within range of the residence, which were all in a locked mode. Based on my training and experience, I know that persons often lock their wireless networks to prevent unauthorized users from accessing their wireless network. This also informs law enforcement that only limited users have access to the wireless network. In my experience, those accessing a locked wireless network are limited to occupants of the residence and persons known to and/or trusted by the occupants. For a user to gain access to a locked wireless network, the account owner must provide the user with a password.

Execution of the Search Warrant at the SUBJECT PREMISES

26. Based in part on the foregoing information, this Court authorized a warrant to search the SUBJECT PREMISES and the person of Matthew MURPHY for evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252A, and 2422(b). With the assistance of state and local law enforcement, HSI Boston agents executed the warrant on March 26, 2019 at approximately 6:00 a.m.
27. MURPHY was not present in the home at the time of execution. His younger sister was present and notified his mother, who returned to the home shortly thereafter.
28. During the execution of the search, agents located various digital devices, including:

- a. Two iPads, one of which was located on MURPHY's bed, unlocked, and one of which was located on a shelf above his bed. The second iPad was powered on but protected by a four-digit passcode.
 - b. A MacBook Air was located on a desk in MURPHY's room.
 - c. Two USB thumb drives were located on the same desk.
 - d. A micro-camera was located inside the desk.
29. Forensic analysts were able to conduct an onsite preview of some of the devices. On the unlocked iPad, analysts observed evidence of the Snapchat application, including the application icon on the home screen and evidence of the Suspect Account. Analysts also were able to determine that the Apple ID associated with the device incorporated the name of the Suspect Account.
30. On the MacBook Air, analysts were able to access the computer's photo library, where they located evidence of file names containing at least seven Snapchat usernames that I observed in the search warrant return (i.e., users with whom the Suspect Account was communicating). The images associated with those file names appeared to be sexually explicit photographs of males.
31. Family members contacted MURPHY soon after agents arrived and he thereafter returned to the SUBJECT PREMISES. MURPHY arrived driving a work van, which he parked on the street outside of the SUBJECT PREMISES. Agents on scene noticed that MURPHY left an iPhone in the console of the van.
32. MURPHY was advised of and executed a written waiver of his rights pursuant to Miranda and agreed to speak with agents on scene. The interview was recorded. The following statements are summary in nature.

33. MURPHY confirmed that the bedroom from which the above-listed devices were seized was his, and that he was the sole owner and user of the devices described above. He initially denied but ultimately admitted ownership and control of the Suspect Account, along with three other Snapchat accounts.
34. MURPHY denied meeting any of the boys with whom he communicated on Snapchat in real life. He told agents that he would “befriend” one at a time, and then add others based on those user’s contacts. Prior to our interview, I had reviewed MURPHY’s publicly-accessible social media account and realized that one of the Snapchat users MURPHY had been extorting through his use of the Suspect Account was included as one of MURPHY’s “friends.” When asked about this, MURPHY admitted that he helped out at local Boy Scout events and had met the child and his father through Boy Scouts.
35. During the course of the interview, MURPHY gave agents written consent to seize his cell phone from the work van that he had arrived in. Forensic analysts were able to preview the phone, and observed that the Snapchat application did not appear to be on the phone. MURPHY ultimately admitted that he had deleted the application on his way to the house.

CONCLUSION

29. Based on the foregoing, I respectfully submit that there is probable cause to believe that:
 - a. On dates between November 22, 2018 and December 13, 2018, MURPHY did knowingly employ, use, persuade, induce, entice, and coerce a minor, “Minor A,” to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct and the visual depiction was produced and transmitted using materials that had been mailed, shipped, and transported in and affecting interstate and foreign commerce by any means, including by computer, and the visual depiction was actually transported and transmitted using any means and

facility of and in and affecting interstate and foreign commerce, and attempted to do so, in violation of 18 U.S.C. §§ 2251(a) and (e); and

- b. on or about July 21, 2018, MURPHY did knowingly employ, use, persuade, induce, entice, and coerce a minor, "Minor B," to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct and the visual depiction was produced and transmitted using materials that had been mailed, shipped, and transported in and affecting interstate and foreign commerce by any means, including by computer, and the visual depiction was actually transported and transmitted using any means and facility of and in and affecting interstate and foreign commerce, and attempted to do so, in violation of 18 U.S.C. §§ 2251(a) and (e).

Sworn under the pains and penalties of perjury,

[REDACTED]

JANET CONNOLLY
Special Agent
Homeland Security Investigations

SUBSCRIBED and SWORN to before me on March 26, 2019.

[REDACTED]

HONORABLE JUDITH G. DEIN
UNITED STATES MAGISTRATE JUDGE

I have viewed the images described above in Paragraph 13 and I find probable cause to believe that they depict minors involved in sexually explicit conduct. The Affiant shall preserve said images for the duration of the pendency of this matter, including any relevant appeal process.

[REDACTED]

HONORABLE JUDITH G. DEIN
UNITED STATES MAGISTRATE JUDGE