EAG/NS/MCM
F. #2019R0029

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE CELLULAR DEVICE ASSIGNED CALL NUMBER (229) 418-8231, THAT IS STORED AT PREMISES CONTROLLED BY T-MOBILE	**TO BE FILED UNDER SEAL** **SEARCH WARRANT APPLICATION FOR HISTORICAL CELL-SITE INFORMATION** Case No. 20-MC-1584

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Sylvette Reynoso, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain cellular telephone assigned call number (229) 418-8231, (the "SUBJECT PHONE"), that is stored at premises controlled by T-Mobile, a wireless telephone service provider. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require T-Mobile to disclose to the government copies of the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

2. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"), and have been since 2008. I am currently assigned to HSI's New York Office and, more specifically, to a squad that investigates human trafficking

and alien smuggling matters. Previously, I was assigned to narcotics and counter-proliferation squads. I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for sex and human trafficking and related offenses. In that capacity, I have participated in investigations involving the debriefing of sex trafficking and sex abuse victims, review of telephone records, cell site location and GPS data, review of money transfer records, surveillance, analysis of pen register information, and the execution of search warrants, including the execution of search warrants on computers and other electronic media. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. 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.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 844(i) (arson); 1512(a)(2), 1512(b), 1512(c)(2) and 1512(d) (witness tampering); and 1513(e) (witness retaliation) have been committed, are being committed, and will be committed by the user of the SUBJECT PHONE. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, or fruits of these crimes as further described in Attachment B.

PROBABLE CAUSE

5. The U.S. Attorney's Office for the Eastern District of New York and HSI's New York Field Office are investigating ROBERT SYLVESTER KELLY, also known as

"R. KELLY," and others for their participation in a racketeering enterprise involving bribery, extortion, the production of child pornography; transportation of women and girls across state lines to engage in illegal sexual activity, including sexual contact with individuals who were too young to consent to such activity under state law and failure to notify sexual partners of a sexually transmitted disease prior to engaging in sexual intercourse in violation of state law, and related substantive offenses; and for arranging for travel in interstate commerce with intent to promote, manage, establish, and carry on an extortion, in violation of state law.

6. On June 20, 2019, a grand jury in the Eastern District of New York returned an indictment charging KELLY with racketeering involving predicate racketeering acts as to five different women and four Mann Act violations. See United States v. Robert Sylvester Kelly, Criminal Docket No. 19-286 (AMD) (E.D.N.Y.). On July 10, 2019, the grand jury returned a superseding indictment, which added a forfeiture allegation. On December 5, 2019, the grand jury returned a second superseding indictment, adding an additional predicate act of bribery. On March 12, 2020, the grand jury returned a third superseding indictment (the "Indictment") against KELLY. Among the charges against KELLY in the Indictment were offenses that carried a ten-year mandatory minimum sentence based on KELLY's sexual relationship with Azriel Clary, when she was just 17 years old.

7. On January 8, 2020, Azriel Clary began cooperating with federal law enforcement.[1] Several news outlets thereafter reported that Azriel Clary was cooperating with federal law enforcement.

---

[1] Based on my training, experience, and participation in the investigation, I and other law enforcement agents believe the information provided by Azriel Clary is reliable. Information provided by Azriel Clary has been corroborated by other evidence, including information

8. In or about April 2020, two Instagram accounts, muteazrielclary (the "account identifier" for Instagram User ID 32674765793) and mute_azrielclary (the "account identifier" for Instagram User ID 32947370872) (collectively, the "First Instagram Accounts") were created. The names of the accounts appear to be a play on the "Mute R. Kelly" movement, which began in or about 2017, following years of allegations of sex crimes by KELLY against women, and advocated for individuals to stop listening to R. Kelly's music. Based on my training, experience and knowledge of this investigation, including the information described herein, there is probable cause to believe that the individuals controlling the First Instagram Accounts are seeking to stop (i.e., "mute") Azriel Clary from continuing to cooperate with federal law enforcement in its investigation and prosecution of KELLY, including by intimidating her into not testifying at his upcoming federal trial in this district.

9. In or about April 2020, both of the First Instagram Accounts were publicly accessible and the content on each was very similar. When the accounts were publicly accessible, screenshots of the accounts were created. Based on those screenshots, the muteazrielclary account includes the following:

---

obtained from other witnesses, evidence seized from electronic devices, documentary evidence, telephone records, text messages and consensual recordings. Azriel Clary has engaged the services of a lawyer and may seek civil remedies against KELLY in the future. Prior to her cooperation with federal law enforcement, while still engaged in a relationship with KELLY, in a March 2019 television interview following KELLY's arrest on various sexual misconduct charges involving underage girls brought by the Cook County State's Attorney's Office, Azriel Clary publicly claimed that she did not have sex with KELLY when she was 17 years old. Azriel Clary has advised that such statements were false and made publicly at KELLY's direction.

- "Azriel Clary is a [turd emoji] eating wh0re #MuteAzrielClary"
- "Azriel will be dead by 2020 [skull emoji]"
- "Fuck Azriel Clary"
- "K!ll Azriel Clary"

Based also on those screenshots, the mute_azrielclary account includes the following:

- "Shoot Azriel Clary [skull emoji] [green toy gun emoji]"
- "Azriel will be dead by 2022"
- "Azriel Clary is a [turd emoji] eating whore"
- "Azriel Clary is a sh!t eating wh0re [three turd emojis]"
- "K!ll Azriel Clary"
- "Fuck Azriel Clary"

Both accounts contained the hashtag, #MuteAzrielClary.

10. According to screenshots of the accounts, the Instagram account "muteazrielclary" contained four (4) posts, had one (1) follower and was following six (6) other Instagram accounts, and the Instagram account "mute_azrielclary" contained eight (8) posts, had seven (7) followers and was following sixty-one (61) other Instagram accounts.

11. Records provided by Instagram reveal that the individuals who created the User IDs for the First Instagram Accounts provided Instagram with email addresses of "joycelynsavagee4@hotmail.com" (on March 30, 2020 in connection with "muteazrielclary") and "joisavageee@hotmail.com" (on April 4, 2020 in connection with "mute_azrielclary"), both apparently plays on the name Joycelyn Savage, who is a long-time girlfriend of KELLY and, at least publicly, remains supportive of KELLY. According to Microsoft, neither email account existed at the time that the government sought records related to the accounts.

12. While both of the First Instagram Accounts were initially public, the muteazrielclary account is now private and the mute_azrielclary account is no longer accessible on Instagram.

13. On or about May 10, 2020, a user of a Twitter account advised the Federal Bureau of Investigation ("FBI") of a threat to Azriel Clary via Clary's Twitter account. The FBI subsequently reviewed the account, took screenshots and conveyed the information and the screenshots to HSI. In sum, the screenshots show that on or about May 9, 2020, in response to a tweet by Azriel Clary on her Twitter account, @theonlyazriel, the user of the Twitter account associated with @rkellylovesme and https://twitter.com/rkellylovesme (the "Twitter Account") wrote, "You're on my death list and I know where you live can't wait to kill your punk ass and what do you mean downfall like you a celebrity bitch please you got clout off that man." Clary's father then responded on Twitter, "You come this way and I promise you you will be a shirt!!! You can play all the internet Gansta s@@t until someone really step to y'all! All facts!!" The user of the Twitter Account then wrote, "Stfu you can't stop me I'll murder all y'all ass'es bitch[.]" Based on my training, experience and knowledge of this investigation, there is probable cause to believe that "Stfu" refers to "Shut the fuck up."

14. On June 11, 2020, at approximately 2:50 a.m. Eastern Time, a black SUV (the "Vehicle"), which has been leased from Enterprise Rent-A-Car ("Enterprise"), a commercial vehicle rental establishment, and which was parked outside of 2101 Rock Drive, Kissimmee, Florida, the residence in Florida where Azriel Clary was staying (the "Residence"), was set on fire in an apparent arson. The neighborhood of the Residence is residential in nature, and in light of the time period during which the arson occurred (i.e., in the middle of the night) and the relative low density of residences in the vicinity of the Residence, it is unlikely that there were

substantial telephone communications at the time of day that were not related to the arson. The Vehicle sustained substantial damage as the result of the arson. Inside of the Residence at the time of the arson were four adults and two minors. One of the adults reported to law enforcement, in part and in substance, that upon hearing an explosion, s/he ran outside of the Residence and saw an individual fleeing from the scene of the fire, whose arm was apparently lit on fire. Fire investigators also determined that an accelerant was present along some or all of the outside perimeter of the Residence.

15. The SUV was rented in Florida by the father of Azriel Clary from Enterprise, a business that operates in interstate commerce and whose headquarters is located outside of Florida (and New York).

16. On June 29, 2020, the government learned of an additional Instagram account, this one titled mute.azriel.clary (the "account identifier" for Instagram account https://www.instagram.com/mute.azriel.clary). On the mute.azriel.clary account is a photo of Azriel Clary next to the burned vehicle (one that Clary posted to her Instagram account on or about June 25, 2020) and the text, "SHOOT AZRIEL CLARY" with an emoji of a skull and a gun and "K1LL AZRIEL CLARY". As of June 29, 2020, the mute.azriel.clary account contains three posts, has 57 followers and is following 141 other Instagram accounts.

17. On June 15, 2020, the Honorable Ramon E. Reyes, Jr., United States Magistrate Judge for the Eastern District of New York, authorized a search warrant to Google for users who had searched the address of the Residence close in time to the arson. Among the individuals who searched the address was an individual using IP addresses 2600:1005:b04e:2982:14e7:9a5:1fc1:4978 and 2600:1006:b157:d7b1:5148:9202:ba0a:7ceb (the "IP Addresses") on June 10, 2020 at 10:29 p.m. Eastern Time; June 11, 2020 at 12:59 a.m.

Eastern Time and June 11, 2020 at 1:04 a.m. Eastern Time. As noted above, the arson took place at approximately 2:50 a.m. Eastern Time on June 11, 2020. Verizon Wireless records show that the IP addresses at those particular times belonged to telephone number (786) 459-8432 (the "8432 Telephone"), which is subscribed to by Michael Williams at 202 Hollywood Street in Valdosta, Georgia. The investigation of KELLY previously revealed that Michael Williams at 202 Hollywood Street in Valdosta, Georgia was a family member of Cavonttey Jones, also known as "Kash Jones," who once served as a publicist for KELLY.

18. On June 11, 2020, the Honorable Roanne L. Mann, United States Magistrate Judge for the Eastern District of New York, authorized a search warrant on various phone companies that operated cell towers serving the Residence. The results of that search warrant showed that among the telephone numbers that were served by those cell towers on June 11, 2020 between 2:00 a.m. and 3:30 a.m. was the 8432 Telephone.[2]

19. On July 3, 2020, the Honorable James Orenstein, United States Magistrate Judge for the Eastern District of New York, authorized a search warrant on Verizon Wireless for location information associated with the 8432 Telephone. Verizon Wireless records show that the 8432 Telephone traveled from the vicinity of Valdosta, Georgia (where Michael Williams resides and where the 8432 Telephone was on June 10, 2020 at 7:40 p.m.), to the vicinity of Kissimmee, Florida (where the Residence is located and where the 8432 Telephone was on June

[2] The government is still awaiting receipt of the search warrant response from T-Mobile.

11, 2020 at 3:31 a.m.),[3] to the vicinity of Lake City, Florida (where the 8432 Telephone was on June 11, 2020 at 5:31 a.m.), and finally back to the vicinity of Valdosta, Georgia (where the 8432 Telephone was on June 11, 2020 at 2:09 p.m.).

20. As detailed in this paragraph, there is probable cause to believe that Cavonttey Jones, also known as "Kash Jones," has used telephone number (347) 835-2161 (the "2161 Telephone") since approximately January 2020. The 2161 Telephone is subscribed to by Michael Williams, but public records link the telephone to Jones. Furthermore, on March 17, 2020, Jones called the affiant from the 2161 Telephone.

21. As detailed in this paragraph, there is probable cause to believe that Michael Williams used the SUBJECT PHONE, in addition to the 8432 Telephone. Specifically, in or about 2015, Michael Williams submitted an application for a United States passport, on which he listed his email address as mikewill437@gmail.com. Google records indicate that the SUBJECT PHONE is listed as the recovery telephone number for the mikewill437@gmail.com email account. The SUBJECT PHONE is also subscribed to by Michael Williams. Moreover, a review of telephone records for the SUBJECT PHONE shows regular communications between the 2161 Telephone and the SUBJECT PHONE, including in June 2020. Significantly, a review of the telephone records for the SUBJECT PHONE shows that the user of the SUBJECT PHONE was using it both before and after the time of the arson. For example, on June 11, 2020, at 12:44 a.m., the 2161 Telephone placed a telephone call to the SUBJECT PHONE and the call

---

[3] During a second telephone call placed on June 11, 2020 at 3:31 a.m., the 8432 Telephone was in the vicinity of Winter Garden, Florida (approximately 30 miles from Kissimmee, Florida).

lasted approximately 193 seconds. At 3:20 a.m., the SUBJECT PHONE sent two text messages to (229) 973-2218, indicating the SUBJECT PHONE was being used at this time.

22. In my training and experience, I have learned that T-Mobile is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device ("GPS") data.

23. Based on my training and experience, I know that T-Mobile can collect cell-site data about the SUBJECT PHONE. I also know that wireless providers such as T-Mobile typically collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes.

24. Based on my training and experience, I know that T-Mobile also collects per-call measurement data, which T-Mobile also refers to as the "Real-Time Tool" ("RTT"), "Advanced Timing Data" and/or "Per Call Measurement Data" ("PCMD"). RTT, Advanced Timing Data

and PCMD data estimates the approximate distance of the cellular device from a cellular tower based on the speed with which signals travel between the device and the tower. This information can be used to estimate an approximate location range that is more precise than typical cell-site data.

25. Based on my training and experience, I know that wireless providers such as T-Mobile typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I also know that wireless providers such as T-Mobile typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the SUBJECT PHONE's user or users and may assist in the identification of co-conspirators and/or victims.

AUTHORIZATION REQUEST

26. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

27. I further request that the Court direct T-Mobile to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on T-Mobile, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

28. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to the targets of the investigation. Accordingly, there is good cause to seal these documents

because their premature disclosure may seriously jeopardize that investigation, including by giving targets an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

Respectfully submitted,

SYLVETTE REYNOSO
Special Agent
Department of Homeland Security, Homeland Security Investigations

Subscribed and sworn to before me by telephone this 13th day of July, 2020:

James Orenstein Digitally signed by James Orenstein
Date: 2020.07.13 15:58:44 -04'00'

HONORABLE JAMES ORENSTEIN
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

This warrant applies to records and information associated with the cellular telephone assigned call number (229) 418-8231 ("the Account"), that are stored at premises controlled by T-Mobile ("the Provider").

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time period June 10, 2020 at 6:00 p.m. Eastern Time until June 11, 2020 at 11:59 p.m. Eastern Time (which converts to June 10, 2020 at 10 p.m. UTC until June 12, 2020 at 3:59 a.m. UTC):

a. The following information about the customers or subscribers of the Account:

i. Names (including subscriber names, user names, and screen names);

ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

iii. Local and long distance telephone connection records;

iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

v. Length of service (including start date) and types of service utilized;

vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:

i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

ii. information regarding the cell tower and antenna face (also known as "sectors") through which the communications were sent and received as well as per-call measurement data (also known as the "real-time tool" or "RTT" data, "Advanced Timing Data," "Per Call Measurement" data and/or "PCMD")

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of Title 18, United States Code, Sections 844(i) (arson); 1512(a)(2), 1512(b), 1512(c)(2) and 1512(d) (witness tampering); and 1513(e) (witness retaliation) involving the user of the Account during the period from June 10, 2020 at 6:00 p.m. Eastern Time until June 11, 2020 at 11:59 p.m. Eastern Time.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the

government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate the things particularly described in this Warrant.