AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Cellular telephone numbers 614-598-8934 and 614-596-4378 that are stored at premises owned, maintained, controlled, or operated by TracFone Phone Wireless Inc. d/b/a Simple Mobile

Case No. 2:15-mj-306

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Cellular telephone numbers 614-598-8934 and 614-596-4378 that are stored at premises owned, maintained, controlled, or operated by TracFone Phone Wireless Inc. d/b/a Simple Mobile a wireless provider headquartered at 9700 NW 112 Avenue Miami, FL 33178(See Attachment C)

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

(See Attachment G)

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18	§2339A providing material support to terrorists, §2339B, providing material support to a designated foreign terrorist organization,§1117 by conspiring with two or more persons to violate§1114, knowing and intending that they were to be used

The application is based on these facts:

(See Attached Affidavit)

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Matthew W. Guinn
Applicant's signature

Matthew W Guinn, FBI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 4/9/2015

Elizabeth Preston Deavers
Judge's signature

City and state: Columbus, Ohio

U.S. Magistrate Judge Elizabeth Preston Deavers
Printed name and title

IN THE UNITED STATES DISTRICT COURT

FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR A SEARCH WARRANT FOR **TWITTER ACCOUNT**: @aden_stranger DATA USER ID: 414393179, LOCATED AT: https://www.twitter.com/aden_stranger, THAT IS STORED AT A PREMISES CONTROLLED BY TWITTER, INC.; **FACEBOOK ACCOUNT:** USER NAME: aden_abdiqani, Facebook Account User ID: 1119436488 LOCATED AT: https://www.facebook.com/aden.abdiqani THAT IS STORED AT A PREMISES CONTROLLED BY FACEBOOK, INC AND **CELL PHONE RECORDS:** 614-598-8934 and 614-596-4378 THAT ARE STORED AT PREMISES CONROLLED BY TRACFONE PHONE WIRELESS INC. D/B/A SIMPLE MOBILE AND T-MOBILE.

Case No. 2:15-mj-306

Filed Under Seal

AFFIDAVIT IN SUPPORT OF

AN APPLICATION FOR A SEARCH WARRANT

I, Matthew W. Guinn, Special Agent ("SA") with the Federal Bureau of Investigation ("FBI"), Cincinnati Field Office ("CFO"), Columbus, Ohio, (hereinafter "your affiant") 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 Twitter account that is stored at premises owned, maintained, controlled, or operated by Twitter, a social-networking company headquartered in San Francisco, CA. The information to be searched is described in the following paragraphs and in Attachment C. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b) (1)(A), and 2703(c)(1)(A) to require Twitter to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with Twitter account data user ID: 414393179:

2. I make this affidavit in support of an application for a search warrant for information associated with a certain Facebook user ID that is stored at premises owned, maintained, controlled, or operated by Facebook Inc. ("Facebook"), a social networking company headquartered in Menlo Park, California. 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(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the Facebook account user ID: 1119436488.

3. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises owned, maintained, controlled, or operated by TracFone Phone Wireless Inc. d/b/a Simple Mobile a wireless provider headquartered at 9700 NW 112 Avenue Miami, FL 33178 and T-Mobile, a wireless provider headquartered at 4 Sylvan Way Parsippany, New Jersey 07054. The information to be searched is described in the following paragraphs and in Attachment C and Attachment D. This

affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require TracFone Phone Wireless Inc. d/b/a Simple Mobile and T-Mobile to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications for telephone numbers 614-598-8934 and 614-596-4378.

4. I am a federal law enforcement officer within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have been a Special Agent with the Federal Bureau of Investigation (FBI) for three years, since April 2012. Your affiant is currently assigned to the FBI Joint Terrorism Rask Force (hereinafter "JTTF") where he has been a Case Agent or Co-Case Agent for numerous International Terrorism investigations for the past two and a half. During that time, your affiant has received specialized training in International Terrorism.

5. I have personally participated in the investigation set forth below. I am familiar with the facts and circumstances of the investigation through my personal participation; from discussions with other federal agencies, specifically the Federal Bureau of Investigation (FBI) and the Columbus, Ohio Police Department (CPD) and other law enforcement; from my discussions with witnesses involved in the investigation; and from my review of records and reports relating to the investigation. Unless otherwise noted, wherever in this affidavit I assert that a statement was made, the information was provided by another law enforcement officer or witness who may have had either direct or hearsay knowledge of that statement and to whom I or others have spoken or whose reports I have read and reviewed. Such statements are among many statements made by others and are stated in substance and in part unless otherwise indicated. Since this affidavit is being submitted for the limited purpose of securing a warrant authorizing the searches and seizure of the Requested Information, I have not included details of every aspect of the investigation.

6. As will be detailed in the paragraphs below, Abidqani A. ADEN (hereinafter ADEN) communicated with Abdirahman Sheikh MOHAMUD (hereinafter MOHAMUD) via social media pages at Facebook and Twitter, as well as wireless phone providers T-Mobile and

Simple Mobile and I allege the facts to show there is probable cause to believe that fruits and evidence of offenses involving violations of: (i) Title 18, United States Code §2339Aproviding material support to terrorists, (ii) Title 18, United States Code, §2339B, providing material support to a designated foreign terrorist organization, (iii) Title 18, United States Code §1117 by conspiring with two or more persons to violate (iv) Title 18, United States Code §1114, knowing and intending that they were to be used in preparation for and in carrying out, a violation of the murder of a member of the uniformed service while such officer or employee was engaged in or on account of the performance of official duties and (v) Title 18, United States Code § 1001, false statements involving international or domestic terrorism; may be found within Twitter account data user ID: 414393179, Facebook account user ID: 1119436488 and wireless telephone numbers 614-598-8934 and 614-596-4378.

7. Attachments A and B respectively describe the Twitter and Facebook Profiles with user names to be searched. Attachment C and Attachment D describe the telephone numbers from TracFone Phone Wireless Inc. d/b/a Simple Mobile and T-Mobile to be searched. Attachments E, F, G and H respectively describe the matters and things to be searched and seized within the Twitter and the Facebook Profiles and the Simple Mobile/T-Mobile phone numbers. All statements made in Attachments A, B, C, D, E, F, G and H are adopted into the body of this Affidavit as if fully set forth herein.

DEFINITIONS

TWITTER DESCRIPTION

8. Twitter owns and operates a free-access social-networking website of the same name that can be accessed at http://www.twitter.com. Twitter allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and location information. Twitter also permits users create and read 140-character messages called "Tweets," and to restrict their "Tweets" to individuals whom they approve. These features are described in more detail below.

9. Upon creating a Twitter account, a Twitter user must create a unique Twitter username and an account password, and the user may also select a different name of 20

characters or fewer to identify his or her Twitter account. The Twitter user may also change this username, password, and name without having to open a new Twitter account.

10. Twitter asks users to provide basic identity and contact information, either during the registration process or thereafter. This information may include the user's full name, e-mail addresses, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers. For each user, Twitter may retain information about the date and time at which the user's profile was created, the date and time at which the account was created, and the Internet Protocol ("IP") address at the time of sign-up. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a given Twitter account.

11. A Twitter user can post a personal photograph or image (also known as an "avatar") to his or her profile, and can also change the profile background or theme for his or her account page. In addition, Twitter users can post "bios" of 160 characters or fewer to their profile pages.

12. Twitter also keeps IP logs for each user. These logs contain information about the user's logins to Twitter including, for each access, the IP address assigned to the user and the date stamp at the time the user accessed his or her profile.

13. As discussed above, Twitter users can use their Twitter accounts to post "Tweets" of 140 characters or fewer. Each Tweet includes a timestamp that displays when the Tweet was posted to Twitter. Twitter users can also "favorite," "retweet," or reply to the Tweets of other users. In addition, when a Tweet includes a Twitter username, often preceded by the @ sign, Twitter designates that Tweet a "mention" of the identified user. In the "Connect" tab for each account, Twitter provides the user with a list of other users who have "favorited" or "retweeted" the user's own Tweets, as well as a list of all Tweets that include the user's username (i.e., a list of all "mentions" and "replies" for that username).

14. Twitter users can include photographs or images in their Tweets. Each Twitter account also is provided a user gallery that includes images that the user has shared on Twitter, including images uploaded by other services.

15. Twitter users can also opt to include location data in their Tweets, which will reveal the users' locations at the time they post each Tweet. This "Tweet With Location" function is off by default, so Twitter users must opt in to the service. In addition, Twitter users may delete their past location data.

16. When Twitter users want to post a Tweet that includes a link to a website, they can use Twitter's link service, which converts the longer website link into a shortened link that begins with http://t.co. This link service measures how many times a link has been clicked.

17. A Twitter user can "follow" other Twitter users, which means subscribing to those users' Tweets and site updates. Each user profile page includes a list of the people who are following that user (i.e., the user's "followers" list) and a list of people whom that user follows (i.e., the user's "following" list). Twitters users can "unfollow" users whom they previously followed, and they can also adjust the privacy settings for their profile so that their Tweets are visible only to the people whom they approve, rather than to the public (which is the default setting). A Twitter user can also group other Twitter users into "lists" that display on the right side of the user's home page on Twitter. Twitter also provides users with a list of "Who to Follow," which includes a few recommendations of Twitter accounts that the user may find interesting, based on the types of accounts that the user is already following and who those people follow.

18. In addition to posting Tweets, a Twitter user can also send Direct Messages (DMs) to one of his or her followers. These messages are typically visible only to the sender and the recipient, and both the sender and the recipient have the power to delete the message from the inboxes of both users. As of January 2012, Twitter displayed only the last 100 DMs for a particular user, but older DMs are stored on Twitter's database.

19. Twitter users can configure the settings for their Twitter accounts in numerous ways. For example, a Twitter user can configure his or her Twitter account to send updates to the user's mobile phone, and the user can also set up a "sleep time" during which Twitter updates will not be sent to the user's phone.

20. Twitter includes a search function that enables its users to search all public Tweets for keywords, usernames, or subject, among other things. A Twitter user may save up to 25 past searches.

21. Twitter users can connect their Twitter accounts to third-party websites and applications, which may grant these websites and applications access to the users' public Twitter profiles.

22. If a Twitter user does not want to interact with another user on Twitter, the first user can "block" the second user from following his or her account.

23. In some cases, Twitter users may communicate directly with Twitter about issues relating to their account, such as technical problems or complaints. Social-networking providers like Twitter typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Twitter may also suspend a particular user for breaching Twitter's terms of service, during which time the Twitter user will be prevented from using Twitter's services.

24. As explained herein, information stored in connection with a Twitter account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Twitter user's account information, IP log, stored electronic communications, and other data retained by Twitter, can indicate who has used or controlled the Twitter account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, communications, "tweets" (status updates) and "tweeted" photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Twitter account at a relevant time. Further, Twitter account activity can show how and when the account was accessed or used. For example, as described herein, Twitter logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical

location associated with the logged IP addresses; investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Twitter access, use, and events relating to the crime under investigation. Additionally, Twitter builds geo-location into some of its services. If enabled by the user, physical location is automatically added to "tweeted" communications. This geographic and timeline information may tend to either inculpate or exculpate the Twitter account owner. Last, Twitter account activity may provide relevant insight into the Twitter account owner's state of mind as it relates to the offense under investigation. For example, information on the Twitter account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a criminal plan) or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

25. Therefore, the computers of Twitter are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Twitter, such as account access information, transaction information, and other account information.

FACEBOOK DESCRIPTION

26. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

27. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

28. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

29. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. A Facebook user can also create "lists" of Facebook friends to facilitate the application of these privacy settings. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.

30. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

31. Facebook allows users to upload photos and videos, which may include any metadata such as location that the user transmitted when s/he uploaded the photo or video. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link

to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

32. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

33. If a Facebook user does not want to interact with another user on Facebook, the first user can "block" the second user from seeing his or her account.

34. Facebook has a "like" feature that allows users to give positive feedback or connect to particular pages. Facebook users can "like" Facebook posts or updates, as well as webpages or content on third-party (i.e., non-Facebook) websites. Facebook users can also become "fans" of particular Facebook pages.

35. Facebook has a search function that enables its users to search Facebook for keywords, usernames, or pages, among other things.

36. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

37. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

38. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.

39. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

40. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications ("apps") on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

41. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

42. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

43. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

44. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's "Neoprint," IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's

state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

45. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

WIRELESS PHONE PROVIDERS DESCRIPTION

46. Wireless phone providers often provide their subscribers with voicemail services. In general, a provider will store voicemail messages on behalf of a particular subscriber until the subscriber deletes the voicemail. If the subscriber does not delete the message, the message may remain in the system of TracFone Phone Wireless Inc. d/b/a Simple Mobile and T-Mobile for weeks or months. As Simple Mobile is a wholesale partner to T-Mobile, some records including voice mail are maintained by T-Mobile, while other records are maintained by Simple Mobile, thus both wireless phone providers maintain records for telephone numbers 614-598-8934 and 614-596-4378.

47. Among the services commonly offered by wireless phone providers is the capacity to send short text or multimedia messages (photos, audio, or video) from one subscriber's phone or wireless device to another phone or wireless device via one or more wireless providers. This service is often referred to as "Short Message Service" ("SMS") or "Multimedia Messaging Service" ("MMS"), and is often referred to generically as "text messaging" or "wireless messaging." Based on my knowledge and experience, I believe that stored electronic communications, including SMS and MMS messages that have been sent or received by subscribers, may be stored by TracFone Phone Wireless Inc. d/b/a Simple Mobile and/or T-Mobile for short periods incident to and following their transmission. In addition, providers occasionally retain printouts from original storage of text messages for a particular subscriber's account.

48. Wireless phone providers typically retain certain transactional information about the use of each telephone, voicemail, and text-messaging account on their systems. This information can include log files and messaging logs showing all activity on the account, such as local and long distance telephone connection records, records of session times and durations, lists of all incoming and outgoing telephone numbers or e-mail addresses associated with particular telephone calls, voicemail messages, and text or multimedia messages. Providers may also have information about the dates, times, and methods of connecting associated with every communication in which a particular cellular device was involved.

49. Many wireless providers retain information about the location in which a particular communication was transmitted or received. This information can include data about which "cell towers" (i.e., antenna towers covering specific geographic areas) received a radio signal from the cellular device and thereby transmitted or received the communication in question.

50. Wireless providers may also retain text messaging logs that include specific information about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Station Equipment Identity ("IMEI"). When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

51. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers' full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the

length of service, the types of service utilized, the ESN or other unique identifier for the cellular device associated with the account, the subscribers' Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates and times of payments and the means and source of payment (including any credit card or bank account number).

52. In some cases, wireless subscribers may communicate directly with a wireless provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Wireless providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

BACKGROUND INFORMATION

Designated Foreign Terrorist Organization Al-Nusrah Front

53. Per 8 U.S.C. § 1189 (Designation of foreign terrorist organizations), the U.S. Secretary of State is authorized to designate an organization as a Foreign Terrorist Organization (hereinafter "FTO"). On October 15, 2004, the Secretary of State designated al-Qa'ida in Iraq ("AQI"), then known as Jam'at al Tawhid wa'al-Jihad, as an FTO under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist under section 1(b) of Executive Order 13224.

54. On December 11, 2012, the Secretary of State amended the designation of AQI to include the following aliases: al-Nusrah Front ("al-Nusrah"), Jabhat al-Nusrah, Jabhet al-Nusra, The Victory Front, and Al-Nusrah Front for the People of the Levant.

55. On May 15, 2014, the Secretary of State, in response to the evolving nature of the relationships between al-Nusrah and AQI, amended the FTO designation of AQI to remove all

aliases associated with al-Nusrah Front. Separately, the Secretary of State then designated al-Nusrah Front, also known as Jabhat al-Nusrah, also known as Jabhet al-Nusra, also known as The Victory Front, also known as Al-Nusrah Front for the People of the Levant, also known as Al-Nusrah Front in Lebanon, also known as Support Front for the People of the Levant, and also known as Jabaht al-Nusra li-Ahl al-Sham min Mujahedi al-Sham fi Sahat al-Jihad, as an FTO under Section 219 of the Immigration and Nationality Act and as a Specially Designated GlobalTerrorist entity under section 1(b) of Executive Order 13224.

OVERVIEW OF THE INVESTIGATION

56. FBI has opened an investigation into Abdirahman Sheik MOHAMUD (Date of Birth: September 1, 1991, hereinafter MOHAMUD) who is a Columbus, Ohio resident and a Naturalized United States Citizen.

57. MOHAMUD departed the United States on April 18, 2014 for the purpose of fighting in Syria and to provide material support for al-Nusrah Front ("al-Nusrah"), which is designated by the U.S. Secretary of State as a foreign terrorist organization (FTO). MOHAMUD's brother, Abdifatah ADEN, was in Syria at that time fighting with al-Nusrah and Ahrar al-Sham, a group linked to al-Nusrah also fighting in Syria.

58. While in Syria, MOHAMUD trained with al-Nusrah on use of weapons and tactics and then was instructed by al-Nusrah to return to the U.S. and commit an act of terrorism domestically. MOHAMUD returned to the U.S. on June 8, 2014, and while in the United States, your Affiant believes MOHAMUD conspired with others, including Abdiqani A. ADEN, to plot the kidnapping and murder of military service members in the United States.

PROBABLE CAUSE

a) 18 U.S.C. §§ 2339A, 2339B, 1117, and 1114

59. The FBI has been investigating Abdiqani ADEN (hereinafter ADEN), and other individuals believed to be part of MOHAMUD's core group of friends and associates, as potential co-conspirators in MOHAMUD's plot to carry out a terrorist attack in the United States. Your Affiant believes ADEN also exchanged communications with MOHAMUD via Twitter, Facebook, and phone while MOHAMUD was in Syria, and that there is probable cause to believe a search of ADEN's Twitter account, Facebook account, and TracPhone Wireless/T-Mobile account will contain communications that reveal ADEN's knowledge of MOHAMUD's travel to Syria, and ADEN's involvement in the plot to carry out a terrorist attack in the United States.

60. Recently, under the advice of his attorney and pursuant to a proffer letter, MOHAMUD provided a statement against his own interests regarding the roles in the aforementioned plot involving himself, ADEN, Hassan JEYLANI (hereinafter JEYLANI), Jibril ALI (hereinafter ALI), Faisal ADEN (hereinafter FAISAL), and Abdullahi AHMED (hereinafter AHMED).

61. During his proffer session, MOHAMUD stated that he traveled to Syria and was told by a general and a leader in Jabhat al-Nusrah to do harm in the United States. MOHAMUD was told to save Aafia SIDDIQUI by grabbing and kidnapping American soldiers and taking them as hostages. After returning to the United States, MOHAMUD, ADEN, JEYLANI, ALI, FAISAL, and AHMED all agreed to participate in the plot. The group talked about the plan on more than one occasion and brought up new ideas in furtherance of the plan. ADEN and the other co-conspirators all said they could help with the plan by raising money. The plan was to go

down to Texas where SIDDIQUI was located, grab civilians or soldiers, and try to negotiate for her release. The group talked about how this would work and about getting guns and who to get guns from. They talked about clothing which was going to be military clothing to make people think they were Jabhat al-Nusrah. They talked about wearing ski masks to cover their faces and have handguns. The group discussed doing reconnaissance on military installations. Even after the group members knew they were being followed by the law enforcement (FBI), they all continued to meet and cultivate their plans. MOHAMUD told ADEN about his training and experience in Syria the first week after he returned from his travel to Syria.

62. Also during his proffer session, MOHAMUD admitted that he purchased a plane ticket to Texas, which he stated was for reconnaissance in furtherance of the plan. FBI received a notification separate from the proffer session that MOHAMUD was scheduled to travel on American Airlines flight 2310 departing Columbus, Ohio for Dallas, Texas. However, to your Affiant's knowledge, MOHAMUD never boarded that flight.

63. According to MOHAMUD, ADEN conducted reconnaissance on a military installation in Columbus, Ohio, along with AHMED and MOHAMUD. ADEN said they would look at the area and see if there were soldiers in Columbus to kidnap for a hostage situation. According to Unnamed Person #4, ADEN was the only member of the group who had a gun. ADEN had a gun, but he got rid of it after search warrants were executed on MOHAMUD's residence. It was a revolver that he used to keep in his house. ADEN told him that he got rid of it, but MOHAMUD could not know for sure. ADEN's role in the plan was to help out with money, gas, and hotels. Between on or about August, 2014 through approximately February, 2015, physical surveillance conducted by the FBI placed MOHAMUD either at ADEN's residence, placed ADEN at MOHAMUD's residence, placed MOHAMUD inside ADEN's known vehicle or physically observed MOHAMUD with ADEN.

64. On February 18, 2015 and February 19, 2015, the FBI interviewed Unnamed Person #1. Unnamed Person #1 is described as a peer and associate of MOHAMUD's. Your Affiant believes the following exchanges indicate that MOHAMUD was in the country of Syria in April to May of 2014, and received training and instruction from a high ranking jihadist to return to the United States and do something there, which caused MOHAMUD to develop the

plan to recruit a trusted core group of individuals and conduct an attack in the United States against military targets. As further explained below, MOHAMUD indicated that he knows some people on the west side of Columbus, and they are going to get together and go somewhere to kill troops.

65. During the interview, Unnamed Person #1 described statements MOHAMUD made to Unnamed Person #1 after MOHAMUD returned from overseas. While he (MOHAMUD) was in Syria, he talked with a high ranking jihadist who told him you have an American passport, you have lived in America for nineteen years, go back and do something there (in the United Sates). This high ranking leader in Syria gave him (MOHAMUD) the task to go kill groups in uniform, who work for the U.S. Government on an army base. According to Unnamed Person #1, MOHAMUD stated that is why he returned to the U.S. and that his plan was to lay low and get with a group of "guys." MOHAMUD told Unnamed Person #1 that he knows some people on the west side of Columbus and that they are going to get together and go somewhere to kill troops. Prior to this direction, MOHAMUD had received training in Syria on how to fire guns, clean guns, fix weapons jams, hand to hand combat, knives, tactics and explosives. MOHAMUD told Unnamed Person #1 that they would do different types of drills, including training on how to go into a house, kill the people inside and take what they could get.

66. Unnamed Person #1 was shown Ohio DMV photos of several individuals who FBI believes are MOHAMUD's co-conspirators, and Unnamed Person #1 identified several of them as being members of MOHAMUD's core group of friends. Specifically, Unnamed Person #1 identified the individuals in the photos as "WAACE" (true name Abdiqani ADEN), "FAZE" (true name Faisel Osman ADEN), and "Jibril" (true name Jibril ALI). Unnamed Person #1 also recognized a photo of Abdullahi Dahir AHMED, but did not know AHMED's name. Unnamed Person #1 identified all four of these individuals as the group that is always with MOHAMUDand stated that the group usually plays basketball at the Grove City "Y" on Mondays and Wednesdays from 7 to 10 pm.

67. Unnamed Person #1 provided FBI with the content of Direct Messages that Unnamed Person #1 exchange with MOHAMUD on Twitter while MOHAMUD was in Syria. In one series of communications, MOHAMUD told Unnamed Person #1 that he was in need of money.

68. On March 2, 2015, the FBI interviewed Unnamed Person #2. Unnamed Person #2 is described as a peer and associate of MOHAMUD's. Your affiant believes the following exchanges corroborate Unnamed Person #1's statements; that MOHAMUD was in the country of Syria, and received instruction and training to return to the United States to organize an attack.

69. According to Unnamed Person #2, a couple of weeks after MOHAMUD returned from his overseas trip, he and Unnamed Person #2 were together at MOHAMUD's house. MOHAMUD went on to tell Unnamed Person #2 that he went to SYRIA where he went to a training camp where he did a lot of exercises and got fit. There were other groups of people at the camp training. MOHAMUD stated he switched posts, got supplies, and at least once said he had the night post. MOHAMUD told Unnamed Person #2 that he tried to meet up with his brother (Abdifitah ADEN) while in Syria but was unable to because they were at different locations. MOHAMUD mentioned the names of groups that he was with but Unnamed Person #2 could not recall the names. The only name he could recall was, "DOLUTA ISLAMIA" but Unnamed Person #2 was not familiar with that name and did not know if it meant anything.

70. Unnamed Person #2 stated that MOHAMUD told him that he was involved in one small firefight and a couple of close calls. MOHAMUD never mentioned that he killed anyone. During the same conversation, MOHAMUD mentioned that he had an AK-47 while in Syria. While MOHAMUD was overseas, he sent Unnamed Person #2 a SNAPCHAT[1] video. The video was of MOHAMUD, walking around with an AK-47 slung over his shoulder. MOHAMUD was wearing a green Pakistani style robe and a white and black turban. In the video, MOHAMUD said something like, "got my AK, doing my training."

71. Also during this conversation, MOHAMUD expressed his opinions of the U.S. (United States) to Unnamed Person #2. MOHAMUD said this country (United States) is corrupt, Guantanamo is a huge problem and MOHAMUD wanted to fix it; MOHAMUD wanted to do something "big", like go to TEXAS, capture three to four soldiers and kill them, execution style. MOHAMUD wanted to get more people to help him and Unnamed Person #2 was sure

[1] Snapchat is a photo messaging application. Using the application, users can take photos, record videos, add text and drawings, and send them to a controlled list of recipients. These sent photographs and videos are known as "Snaps". Users set a time limit for how long recipients can view their Snaps, the range is from 1 to 10 seconds, after which they will be hidden from the recipient's device and deleted from Snapchat's servers.

MOHAMUD was trying to recruit him. He tried to recruit Unnamed Person #2 by asking him a lot of questions about his life, such as, what are you doing now, school is a waste of time, and there are more important things. Unnamed Person #2 believed that all of the questions implied that Unnamed Person #2 should help MOHAMUD.

72. When asked by Interviewing Agents if anyone else knew about MOHAMUD's activities or plans to carry out a domestic attack, Unnamed Person #2 replied that WAACE (ADEN) and JIBRIL (ALI) most likely do. They share similar opinions as MOHAMUD and know MOHAMUD's opinions very well. They dislike America but not to the same level as MOHAMUD. WAACE (ADEN) and JIBRIL (ALI) used to be really bad kids when they were younger but as they grew up they became more religious.

73. According to Unnamed Person #2, several kids used to play basketball with MOHAMUD but the core group was "The RIVERPOINTE kids." They included LE'BELL (Abdullahi AHMED), JIBRIL (ALI), WAACE (ADEN) or ABDIQANI, and another named person Unnamed Person #2 saw the guys with MOHAMUD a lot. Someone always had a car to drive them to the various locations.

74. When Interviewing Agents asked Unnamed Person #2 why MOHAMUD chose TEXAS for an attack, Unnamed Person #2 replied that MOHAMUD picked TEXAS because he had family or some close friends in TEXAS so he had a place to stay and he could tell his mother he was just going to visit them.

75. In connection with this matter, FBI has also interviewed Unnamed Person #3, who is described as an employee of the L.E.P.D. Firearms Range in Columbus, Ohio. Unnamed Person #3 reported that on September 5, 2014 – three months after MOHAMUD's return from Syria – MOHAMUD, FAISAL, JEYLANI, and AHMED visited the range, rented a FNS 9mm pistol, and purchased a box of ammunition, targets, and thirty minutes of range time. Your Affiant believes that the visit to the range represents an action taken by MOHAMUD to provide training to individuals who included members of the conspiracy.

c) Twitter, Facebook, and Simple Mobile Accounts

76. This affidavit is being submitted for the purpose of securing a search warrant for all the content and records associated with TracFone Phone Wireless Inc. d/b/a Simple Mobile and T-Mobile numbers 614-598-8934 and 614-596-4378 and with social-media accounts; Twitter account user ID: 414393179 and Facebook Account User ID: 1119436488, because there is probable cause to believe that fruits and evidence of offenses involving violations of: (i) Title 18, United States Code §2339Aproviding material support to terrorists, (ii) Title 18, United States Code, §2339B, providing material support to a designated foreign terrorist organization, (iii) Title 18, United States Code §1117 by conspiring with two or more persons to violate (iv) Title 18, United States Code §1114, knowing and intending that they were to be used in preparation for and in carrying out, a violation of the murder of a member of the uniformed service while such officer or employee was engaged in or on account of the performance of official duties; may be found within Twitter account data user ID: 414393179 and Facebook account user ID: 1119436488 and within the records of TracFone Phone Wireless Inc. d/b/a Simple Mobile and T-Mobile numbers 614-598-8934 and 614-596-4378. Your affiant believes that the Facebook and Twitter social media accounts belong to ADEN based on the photos on both of these accounts bearing strong resemblances to ADEN's driver's license photograph. Your affiant believes that cellular telephone number 614-598-8934 is used by ADEN since ADEN placed this number on a February 11, 2014 Ohio Driver License Application. Your affiant believes that cellular telephone number 614-596-4378 is used by ADEN based on a March 14, 2014 Facebook direct message in which ADEN requests MOHAMUD call him at 614-596-4378.

1) ADEN and MOHAMUD's Twitter Communications

77. On March 7, 2015, the FBI conducted an open source search of ADEN's Twitter Account: @Aden_Stranger, User ID: 414393179, revealing that he used the following image of a Black Flag on his Twitter page:

78. The Black Flag is a symbol with the Islamic Shahada [Islamic confession translated in English as "There is no god but God, Muhammad is the messenger of God"] in white Arabic script on a solid black background. It is believed in Islam to originally be one of the flags flown by the Prophet Muhammad. However, it has become used in the last two decades as a flag used by terrorist organizations to symbolize offensive war for the establishment of the Caliphate.

79. A review of ADEN's Twitter page revealed approximately 12 publically viewable communications, from on or about March 2014 through October, 2014 between ADEN's Twitter account Salahuddin Abdiqani @Aden_Stranger (USER NAME: 414393179) and MOHAMUD's Twitter account Al Haytham@alHaytham000 (previously; @Regroup1Ummah). Of particular note, on or about October 20, 2014, ADEN had a Twitter conversation with MOHAMUD, FAISAL, and another unnamed person, in which ADEN pays reverence to MOHAMUD stating, "I give bayah to Amir Al-Mas (Ayanle)." Your Affiant understands the term "bayah" to be similar to the Arabic word "bayat" which refers to an oath of allegiance to an "Amir" (Islamic ruler). Your Affiant understands the term "al-mas" to be an Arabic word for "diamond." The name "Ayanle" is a name by which numerous witnesses in the investigation know Abdirahman MOHAMUD. Thus, your Affiant believes that in this public posting, ADEN refers to "Ayanle" (MOHAMUD) as an Amir and pledges allegiance to him. On October 20, 2014 MWG at approximately 10:40PM, ADEN sent an open Tweet, "Allahu Akbar, In Shah Allah Masjid Taqwa for Fajr

[morning prayer] link-up[2]." On October 20, 2015 at approximately 10:41PM, MOAHMUD responded to ADEN's Tweet and included FAISAL and AHMED saying, "Ameen." Thus, your affiant believes that this series of communications shows ADEN communicating to other members of this conspiracy that they should "link-up" at Masjid Attaqwa, and MOHAMUD confirming the "link-up," while including other members of this conspiracy to his responding message.

80. From approximately April, 2013 through approximately December, 2013, leading up to MOHAMUD's departure for Syria, MOHAMUD sent numerous public tweets displaying his support for the Mujahideen in Syria. Your affiant believes that this is the precipice for MOHAMUD's recruitment of ADEN into the conspiracy. On April 16, 2013, MOHAMUD sent a tweet, "I fear that some of the Syrian Mujahideen are fighting not for the Shri'a, the law of Allah, but rather for Democracy. On April 18, 2018, MOHAMUD tweets, "I spit on every Flag including mine except the flag of" [Arabic writing follows, which translates as: "There is no God but God, Muhammad is the messenger of God."] As described above, the Black Flag used by al-Nusrah bears the same message in Arabic. Your Affiant therefore assesses that MOHAMUD stated that he spits on every flag except for the flag of al-Nusrah. ADEN responds to MOHAMUD's April 18, 2013 tweet, "Blame America." On December 25, 2013, ADEN re-tweeted an image to MOHAMUD of a male firing an assault rifle next to a female with what appeared to be a grenade launcher citing; "relationship like this please."

81. Further review of ADEN's Twitter page reveals that ADEN follows MIZANUR RAHMAN, a well-known British jihadist who was convicted in 2007 of solicitation to murder American troops. RAHMAN praised the 2013 beheading of a member of the British armed forces, on a public sidewalk in broad daylight. RAHMAN has also touted the idea of training children to use arms and believes that at age 15 they become adults who are ready to join terrorist groups as mujahideen. ADEN also follows ANJEM CHOUDARY on Twitter, who is a high profile jihadist in the United Kingdom. CHOUDARY has expressed admiration for Osama Bin Laden, the 9/11 hijackers, and the bombers who detonated explosives on the London public

[2] The sentence "Allahu Akbar, In Shah Allah Masjid Taqwa for Fajr" translates to "God is great, morning prayer at a Taqwa Mosque if God wills."

transportation system on July 7, 2005. CHOUDARY cofounded al-Muhajiroun, a group supportive of Al Qaeda.

82. ADEN is also following on Twitter: MOHAMUD, FAISAL, JEYLANI and AHMED, all members of this conspiracy.

2) ADEN and MOHAMUD's Facebook Communications

83. A review of private direct messages sent to and received from MOHAMUD's Facebook account (www.facebook.com/100002374550416) revealed multiple direct message contacts between ADEN and MOHAMUD prior to, during, and after MOHAMUD's travel to Syria. On or about April 20, 2014, shortly after MOHAMUD departed to Syria, ADEN received a Facebook direct message from MOHAMUD requesting that ADEN place money into a named US bank account. On or about April 21, 2014, ADEN replies, "I gotchu fam." Thus your affiant believes that ADEN was acknowledging MOHAMUD's request for funds. From approximately late April 2014 through early June 2014, while MOHAMUD was in Syria training, MOHAMUD and ADEN exchanged approximately eight private direct message communications in which they check on each other's well being. For example, one asks the other how his family is doing, and MOHAMUD sends a photo of himself drinking water out of a chalice. On or about July 14, 2014, after MOHAMUD had been back in Columbus for about one month, ADEN sent a direct message to MOHAMUD indicating that he (ADEN) would pick MOHAMUD up, thus demonstrating that ADEN and MOHAMUD continued their relationship after MOHAMUD's return. As stated above, MOHAMUD informed FBI that he told ADEN about his travel to Syria within one week of his return. Thus, your affiant believes ADEN and MOHAMUD may have already been conspiring to commit a domestic attack at the time the July 14, 2014 message was sent. ADEN is Facebook friends with MOHAMUD, FAISAL, and ALI, all of whom are members of this conspiracy.

3) ADEN and MOHAMUD's Telephone Communications

84. Through the course of this investigation, your Affiant has identified phone numbers associated with both ADEN and MOHAMUD. A traffic incident report from the Ohio Public Department of Safety dated January 5, 2014 provides 614-596-4378 as a phone number

for ADEN. Separately, records obtained from the Department of Motor Vehicles include an application that ADEN submitted to obtain a driver's license, in which he lists 614-598-8934 as a phone number. Records obtained from Facebook also show that ADEN provided one of these phone numbers to MOHAMUD during a Facebook conversation. According to toll records obtained for known phone numbers for MOHAMUD and ADEN, from on or about March, 2014 through on or about December, 2014, ADEN had approximately 720 telephonic contacts from his identified telephone numbers (614-598-8934 and 614-596-4378) with MOHAMUD's multiple known phone numbers.[3] MOHAMUD departed for Syria on April 18, 2014, and some of the communications therefore occurred while MOHAMUD was overseas. The remaining communications occurred after MOHAMUD returned to the United States and was conspiring with others, including ADEN, to carry out an attack in the United States.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

85. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b) (1)(A) and 2703(c)(1)(A), by using warrants to require Twitter, Facebook and TracFone Phone Wireless Inc. d/b/a Simple Mobile and T-Mobile to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachments E, F, G and H. Upon receipt of the information described in Section I of Attachments E, F, G and H, government-authorized persons will review that information to locate the items described in Section II of Attachments E, F, G and H.

CONCLUSION

86. Based on these facts, there is probable cause to believe that there are fruits and evidence, as further described in Attachments A, B, C, D, E F, G and H of: (i) Title 18, United States Code §2339A, providing material support to terrorists, (ii) Title 18, United States Code §2339B, providing material support to a designated foreign terrorist organization; and (iii) Title

[3] A number of different phone numbers associated with MOHAMUD have been identified during the course of this investigation. Two examples are provided: (1) during a voluntary interview with the FBI on February 20, 2014, MOHAMUD informed FBI agents that he used phone number 614-916-6474; (2) A report on November 20, 2014 by the Sheriff's Office in Franklin County, Ohio in an unrelated matter included 614-208-0393 as a phone number for MOHAMUD.

18, United States Code §1117 by conspiring with two or more persons to violate, (iv) Title 18, United States Code §1114, knowing and intending that they were to be used in preparation for and in carrying out, a murder of a member of the uniformed service while such officer or employee was engaged in or on account of the performance of official duties; may be found within **TWITTER ACCOUNT**: @aden_stranger, DATA USER ID: 414393179, LOCATED AT: https://www.twitter.com/aden_stranger, **FACEBOOK ACCOUNT** USER NAME: aden.abdiqani, Facebook Account User ID: 1119436488; LOCATED AT: https://www.facebook.com/aden.abdiqani and **CELL PHONE RECORDS** for 614-598-8934 and 614-596-4378 that are stored at premises controlled by TracFone Phone Wireless Inc. d/b/a Simple Mobile and T-Mobile. Specifically, the social media and cellular telephone account records may contain evidence of ADEN's communications with MOHAMUD which relates to the aforementioned offenses involving the planning and execution of the plot, in coordination with terrorism suspect MOHAMUD to conspire with others the murder of a member of the uniformed service while such officer or employee was engaged in or on account of the performance of official duties, and that this device may also contain contact information for other individuals who also participated in the plot with MOHAMUD.

Respectfully submitted,

Matthew W. Guinn

Special Agent

Federal Bureau of Investigation

Subscribed and sworn to before me

on April 9, 2015

U.S. Magistrate Judge Elizabeth Preston Deavers

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

This warrant applies to information associated with the Twitter profile with username @aden_stranger; USER ID: 414393179, LOCATED AT: https://www.twitter.com/aden_stranger, that is stored at premises owned, maintained, controlled, or operated by Twitter, Inc, a company headquartered at 1355 Market Street, Suite 900 San Francisco, CA 94103 .

ATTACHMENT B

DESCRIPTION OF PROPERTY TO BE SEARCHED

This warrant applies to information associated with the Facebook profile with username aden_abdiqani, Facebook Account User ID: 1119436488 LOCATED AT: https://www.facebook.com/aden.abdiqani, that is stored at premises owned, maintained, controlled, or operated by Facebook Inc, a company headquartered at 1601 Willow Road Menlo Park, CA 94025

ATTACHMENT C

DESCRIPTION OF PROPERTY TO BE SEARCHED

This warrant applies to information associated with cellular telephone numbers 614-598-8934 and 614-596-4378 that are stored at premises owned, maintained, controlled, or operated by TracFone Phone Wireless Inc. d/b/a Simple Mobile a wireless provider headquartered at 9700 NW 112 Avenue Miami, FL 33178.

ATTACHMENT D

DESCRIPTION OF PROPERTY TO BE SEARCHED

This warrant applies to information associated with cellular telephone numbers 614-598-8934 and 614-596-4378 that are stored at premises owned, maintained, controlled, or operated by T-Mobile 4 Sylvan Way Parsippany, New Jersey 07054 USA.

ATTACHMENT E

PARTICULAR THINGS TO BE SEIZED

I. Information to be disclosed by Twitter

To the extent that the information described in Attachment A is within the possession, custody, or control of Twitter, Inc., including any messages, records, files, logs, or information that have been deleted but are still available to Twitter, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Twitter is required to disclose the following information to the government for each account listed in Attachment A:

a. All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;

b. All past and current usernames, account passwords, and names associated with the account;

c. The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;

d. All IP logs and other documents showing the IP address, date, and time of each login to the account;

e. All data and information associated with the profile page, including photographs, "bios," and profile backgrounds and themes;

f. All "Tweets" and Direct Messages sent, received, "favorited," or retweeted by the account, and all photographs or images included in those Tweets and Direct Messages;

g. All information from the "Connect" tab for the account, including all lists of Twitter users who have favorited or retweeted Tweets posted by the account, as well as a

list of all Tweets that include the username associated with the account (i.e., "mentions" or "replies");

h. All photographs and images in the user gallery for the account;

i. All location data associated with the account, including all information collected by the "Tweet With Location" service;

j. All information about the account's use of Twitter's link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the account was clicked;

k. All data and information that has been deleted by the user;

l. A list of all of the people that the user follows on Twitter and all people who are following the user (i.e., the user's "following" list and "followers" list);

m. A list of all users that the account has "unfollowed" or blocked;

n. All "lists" created by the account;

o. All information on the "Who to Follow" list for the account;

p. All privacy and account settings;

q. All records of Twitter searches performed by the account, including all past searches saved by the account;

r. All information about connections between the account and third-party websites and applications;

s. All records pertaining to communications between Twitter and any person regarding the user or the user's Twitter account, including contacts with support services, and all records of actions taken, including suspensions of the account.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of (i) Title 18, United States Code §2339A, providing material support to terrorists, (ii) Title 18, United States Code, §2339B, providing material support to a designated foreign terrorist organization, (iii) Title 18, United States Code §1117 by conspiring with two or more persons to violate (iv) Title 18, United States Code §1114, knowing and intending that they were to be used in preparation for and in carrying out, a violation of the murder of a member of the uniformed service while such officer or employee was engaged in or on account of the performance of official duties involving ADEN since April 2014 including, for each user ID identified on Attachment A, information pertaining to the following matters:

a. Based on the foregoing, your affiant believes that ADEN was an active participant in conspiring with MOHAMUD, FAISAL, JEYLANI, ALI and AHMED to violate the aforementioned statutes, and that ADEN communicated with MOHAMUD via his Twitter URL based on your affiant's knowledge that MOHAMUD, FAISAL, AHMED and JEYLANI were Twitter followers of ADEN's.

b. Evidence indicating how and when the Twitter account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Twitter account owner;

c. Evidence indicating the Twitter account owner's state of mind as it relates to the crime under investigation;

d. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

ATTACHMENT F

PARTICULAR THINGS TO BE SEIZED

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment B is within the possession, custody, or control of Facebook Inc. ("Facebook"), including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for each user ID listed in Attachment B:

(a) All contact and personal identifying information, including [[for user IDs: full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.]] [[for group IDs: group identification number, a list of users currently registered to the group, and Group Contact Info, including all contact information for the creator and/or administrator of the group and a PDF of the current status of the group profile page.]]

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them;

(d) All profile information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All other records of communications and messages made or received by the user, including all private messages, chat history, video calling history, and pending "Friend" requests;

(f) All "check ins" and other location information;

(g) All IP logs, including all records of the IP addresses that logged into the account;

(h) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

(i) All information about the Facebook pages that the account is or was a "fan" of;

(j) All past and present lists of friends created by the account;

(k) All records of Facebook searches performed by the account;

(l) All information about the user's access and use of Facebook Marketplace;

(m) The types of service utilized by the user;

(n) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(o) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

(p) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of (i) Title 18, United States Code §2339A, providing material

support to terrorists, (ii) Title 18, United States Code, §2339B, providing material support to a designated foreign terrorist organization, (iii) Title 18, United States Code §1117 by conspiring with two or more persons to violate (iv) Title 18, United States Code §1114, knowing and intending that they were to be used in preparation for and in carrying out, a violation of the murder of a member of the uniformed service while such officer or employee was engaged in or on account of the performance of official duties ADEN since April 2014 including, for each user ID identified on Attachment B, information pertaining to the following matters:

(a) Based on the foregoing, your affiant believes that ADEN was an active participant in conspiring with MOHAMUD, FAISAL, JEYLANI, ALI and AHMED to violate the aforementioned statutes, and that ADEN communicated with MOHAMUD via his Facebook URL based on your affiant's knowledge that MOHAMUD, FAISAL, and ALI were Facebook friends of ADEN's.

(b) Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;

(c) Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(e) The identity of the person(s) who communicated with the user ID [[about matters relating to [describe relevant offense conduct]]], including records that help reveal their whereabouts.

ATTACHMENT G

PARTICULAR THINGS TO BE SEIZED

I. Information to be disclosed by TRACFONE PHONE WIRELESS INC. D/B/A SIMPLE MOBILE

To the extent that the information described in Attachment C is within the possession, custody, or control of TracFone Phone Wireless Inc. d/b/a Simple Mobile including any messages, records, files, logs, or information that have been deleted but are still available to TracFone Phone Wireless Inc. d/b/a Simple Mobile or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), TracFone Phone Wireless Inc. d/b/a Simple Mobile is required to disclose the following information to the government for each account or identifier listed in Attachment C:

a. All voice mail, text, and multimedia messages stored and presently contained in, or on behalf of the account or identifier;

b. All existing printouts from original storage of all of the text messages described above;

c. All transactional information of all activity of the telephones and/or voicemail accounts described above, including log files, messaging logs, local and long distance telephone connection records, records of session times and durations, dates and times of connecting, methods of connecting, telephone numbers associated with outgoing and incoming calls, cell towers used, and/or locations used from March 1, 2014 to present;

d. All text messaging logs, including date and time of messages, and identification numbers associated with the handsets sending and receiving the message;

e. All business records and subscriber information, in any form kept, pertaining to the individual accounts and/or identifiers described above, including subscribers' full names, addresses, shipping addresses, date account was opened, length of service, the types of service

utilized, ESN (Electronic Serial Number) or other unique identifier for the wireless device associated with the account, Social Security number, date of birth, telephone numbers, and other identifiers associated with the account;

f. Detailed billing records, showing all billable calls including outgoing digits, from March 1, 2014 to present;

g. All payment information, including dates and times of payments and means and source of payment (including any credit or bank account number), from March 1, 2014 to present;

h. Incoming and outgoing telephone numbers, from March 1, 2014 to present;

i. All records indicating the services available to subscribers of individual accounts and/or identifiers described above;

j. All records pertaining to communications between TracFone Phone Wireless Inc. d/b/a Simple Mobile and any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of (i) Title 18, United States Code §2339A, providing material support to terrorists, (ii) Title 18, United States Code, §2339B, providing material support to a designated foreign terrorist organization, (iii) Title 18, United States Code §1117 by conspiring with two or more persons to violate (iv) Title 18, United States Code §1114, knowing and intending that they were to be used in preparation for and in carrying out, a violation of the murder of a member of the uniformed service while such officer or employee was engaged in or on account of the performance of official duties ADEN since April 2014 including, for each cellular telephone number identified on Attachment C, information pertaining to the following matters:

a. Based on the foregoing, your affiant believes that ADEN was an active participant in conspiring with MOHAMUD, FAISAL, JEYLANI, ALI and AHMED to violate the aforementioned statutes, and that ADEN communicated with MOHAMUD via the two identified cellular telephone numbers based on your affiant's knowledge that ADEN, FAISAL, ALI and JEYLANI had extensive telephonic connectivity with MOHAMUD from March 1, 2014 through December 31, 2014.

b. The identity of the person(s) who created or used the telephone numbers, including records that help reveal the whereabouts of such person(s).

ATTACHMENT H

PARTICULAR THINGS TO BE SEIZED

I. Information to be disclosed by T-Mobile

To the extent that the information described in Attachment D is within the possession, custody, or control of T-Mobile including any messages, records, files, logs, or information that have been deleted but are still available to T-Mobile or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), T-Mobile is required to disclose the following information to the government for each account or identifier listed in Attachment D:

a. All voice mail, text, and multimedia messages stored and presently contained in, or on behalf of the account or identifier;

b. All existing printouts from original storage of all of the text messages described above;

c. All transactional information of all activity of the telephones and/or voicemail accounts described above, including log files, messaging logs, local and long distance telephone connection records, records of session times and durations, dates and times of connecting, methods of connecting, telephone numbers associated with outgoing and incoming calls, cell towers used, and/or locations used from March 1, 2014 to present;

d. All text messaging logs, including date and time of messages, and identification numbers associated with the handsets sending and receiving the message;

e. All business records and subscriber information, in any form kept, pertaining to the individual accounts and/or identifiers described above, including subscribers' full names,

addresses, shipping addresses, date account was opened, length of service, the types of service utilized, ESN (Electronic Serial Number) or other unique identifier for the wireless device associated with the account, Social Security number, date of birth, telephone numbers, and other identifiers associated with the account;

f. Detailed billing records, showing all billable calls including outgoing digits, from March 1, 2014 to present;

g. All payment information, including dates and times of payments and means and source of payment (including any credit or bank account number), from March 1, 2014 to present;

h. Incoming and outgoing telephone numbers, from March 1, 2014 to present;

i. All records indicating the services available to subscribers of individual accounts and/or identifiers described above;

j. All records pertaining to communications between T-Mobile and any person regarding the account or identifier, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of (i) Title 18, United States Code §2339A, providing material support to terrorists, (ii) Title 18, United States Code, §2339B, providing material support to a designated foreign terrorist organization, (iii) Title 18, United States Code §1117 by conspiring with two or more persons to violate (iv) Title 18, United States Code §1114, knowing and

intending that they were to be used in preparation for and in carrying out, a violation of the murder of a member of the uniformed service while such officer or employee was engaged in or on account of the performance of official duties ADEN since April 2014 including, for each cellular telephone number identified on Attachment D, information pertaining to the following matters:

a. Based on the foregoing, your affiant believes that ADEN was an active participant in conspiring with MOHAMUD, FAISAL, JEYLANI, ALI and AHMED to violate the aforementioned statutes, and that ADEN communicated with MOHAMUD via the two identified cellular telephone numbers based on your affiant's knowledge that ADEN, FAISAL, ALI and JEYLANI had extensive telephonic connectivity with MOHAMUD from March 1, 2014 through December 31, 2014.

b. The identity of the person(s) who created or used the telephone numbers, including records that help reveal the whereabouts of such person(s).