

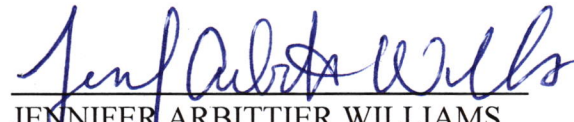
IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	CRIMINAL NO. 15-171
	:	
KEONNA THOMAS,	:	
a/k/a "Fatayat Al Khilafah,"	:	
a/k/a "YoungLioness"	:	

NOTICE OF UNSEALED FILINGS

In accordance with the Court's Order dated March 7, 2017, the government has redacted and is hereby publicly filing the attached documents previously filed under seal in this case.

LOUIS D. LAPPEN
ACTING UNITED STATES ATTORNEY



JENNIFER ARBITTIER WILLIAMS
Assistant United States Attorney

PAUL CASEY
Trial Attorney
Counterterrorism Section
U.S. Department of Justice

CERTIFICATE OF SERVICE

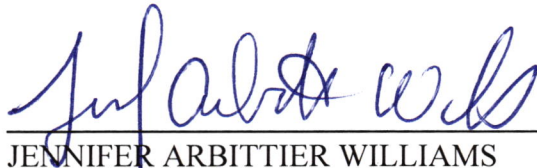
I certify that a copy of the Government's Notice of Unsealed Filings was served
by e-mail on the following counsel:

Counsel for Defendant:

Kathleen M. Gaughan, Esquire
Elizabeth L. Toplin, Esquire
Defender Association Of Philadelphia
Federal Court Division
The Curtis Center Building
601 Walnut Street, Suite 540 West
Independence Square West
Philadelphia, PA 19106

Counsel for Movant:

Paul Safier, Esq.
Levine Sullivan Koch & Schulz, LLP
1760 Market Street, Suite 1001
Philadelphia, PA 19103

A handwritten signature in blue ink, appearing to read "Jennifer Arbittier Williams", is written over a horizontal line.

JENNIFER ARBITTIER WILLIAMS
Assistant United States Attorney

Date: April 3, 2017

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Pennsylvania**REDACTED**In the Matter of the Search of :
(Briefly describe the property to be searched
or identify the person by name and address)

PA

Case No. 15-391-M-1

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Eastern District of Pennsylvania
(Identify the person or describe the property to be searched and give its location):

PA as more fully described in Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (Identify the person or describe the property to be seized):

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before _____ (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to the duty magistrate.☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued:

3/27/15 5:30


Judge's signature

City and state:

Philadelphia, PA

Honorable Elizabeth T. Hey

Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p>		
Date: _____	_____ <i>Executing officer's signature</i> _____ <i>Printed name and title</i>	

ATTACHMENT A

Place to be searched

The residence located at _____ PA _____ is a
_____ house, with the number _____ affixed to the wall of the home's exterior.

ATTACHMENT B

Items to be Seized

, attempting to provide,
and conspiracy to
provide

1. All records relating to violations of 18 U.S.C. § 2339B (providing material support to a designated foreign terrorist organization), including:
 - a. Any records or information, in whatever form, relating to ISIS and any other terrorist organization or group.
 - b. Records and information relating to the use of Facebook, Twitter, or any other online facility.
 - c. Records of names, addresses, telephone numbers, e-mail addresses, lists, mailing lists, appointment books, diaries, logs, ledgers, notebooks, mailing and shipping records, and encryption "keys."
 - d. Financial records and information, including but not limited to bank and financial records, negotiated and non-negotiated checks, money orders, cash, and records regarding any bank accounts or safety deposit boxes.
2. Calendars both in written form and/or electronic form.
3. All information relating to travel, potential travel, research about travel or geographic areas outside of Philadelphia, and any and all maps and/or documents showing geographic locations.
4. Any locked closet, drawer, filing cabinet, suitcase, briefcase, safe or lockbox which may contain any of the above items. Authorized officers of the United States are further

authorized to open and search and remove, if necessary, any safe or other locked receptacle or compartment, as some or all of the items described above may be maintained therein.

Authorized officers of the United States are further authorized to open and search any locked rooms, storerooms, or other storage areas, as some or all the items described above may be maintained therein. And authorized officers of the United States are authorized to use the services of locksmiths, who may not necessarily be federal law enforcement officers, in order to properly open and search any safe or other locked receptacle or compartment on the premises, or off the premises, if necessary, for the purpose of obtaining any items described in this search warrant, provided that such locksmiths operate under direction, control and supervision of any authorized officer of the United States.

5. Any and all computers or storage media which may have been used as a means to commit the violations described above or which may contain evidence, fruits, and instrumentalities of said violations. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"), the following items may also be seized:

- a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

- c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
 - e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
 - f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - h. evidence of the times the COMPUTER was used;
 - i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
 - j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - k. records of or information about Internet Protocol addresses used by the COMPUTER;
 - l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
6. contextual information necessary to understand the evidence described in this attachment.

7. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

MD 93 (Rev. 12-09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*

Case No.

Information associated with the
 following Twitter accounts:

- @KhilafahAl;
- @Saajidiah4life; and
- any and all accounts resolving to IP address 71.23.230.0

15-391-M-3

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Pennsylvania
(Identify the person or describe the property to be searched and give its location):

Twitter accounts @KhilafahAl, @Saajidiah4life, and any and all accounts resolving to IP address 71.23.230.0, as more fully described in Attachment A.

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized):*

See Attachment B.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before

April 10, 2015

(not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10 p.m.☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge

Honorable Elizabeth T. Hey

(name)

☒ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial); and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)*.☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 3/27/15 5:20 pm

Judge's signature

City and state:

Philadelphia PA

Honorable Elizabeth T. Hey

Printed name and title

AO 93 (Rev. 12-07) Search and Seizure Warrant (Page 2)

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of:		
Inventory of the property taken and name of any person(s) seized:		
Certification		
<p><i>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</i></p>		
Date: _____	_____ <i>Executing officer's signature</i>	
	_____ <i>Printed name and title</i>	

ATTACHMENT A

LOCATION TO BE SEARCHED:

Twitter accounts:

- **@KhilafahAl;**
- **@Saajidah4life;**
- **any and all accounts resolving to IP address 71.23.230.0;**

stored at premises controlled by Twitter, 1355 Market Street, Suite 900, San Francisco, CA 94103.

ATTACHMENT B

Part One: ITEMS TO BE SEIZED: (TO BE PROVIDED BY TWITTER)

All posts and communications, records, files, logs, or information, including those items 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), dated from June 2013 through the present, including:

- A. The contents of all posts and communications associated with the aforementioned accounts, including stored or preserved copies of posts and communications sent to and from the accounts, the source and destination addresses associated with each post and communication, the date and time at which each was sent, and the size and length of each;
- B. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which each account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account numbers);
- C. All records or other information stored at any time by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures and files; and
- D. All records pertaining to communications between the aforementioned accounts and any person regarding the accounts, including contacts with support services and records of actions taken.

attempting to provide,
and conspiracy to provide.

Part Two: ITEMS TO BE SEIZED: (TO BE EXECUTED BY LAW ENFORCEMENT AGENTS)

All information and data described above that constitute fruits, evidence, contraband and/or instrumentalities of violations or attempts to violate 18 U.S.C. § 2339B (providing material support to a designated foreign terrorist organization), along with any evidence that would tend to show the true identities of the persons committing this offenses.

All available log files showing dates, times and IP addresses for access to these accounts.

Records relating to who created, used, or communicated with the accounts described above, including records about their identities and whereabouts.

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of PennsylvaniaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address))
)
) Case No.

15-391-M-2

Information associated with the
following Facebook accounts:

- Fatayat.AIKhifah;
- al.kifah.3;
- al.kifah.9; and
- any and all accounts resolving to IP address 71.23.230.0

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Pennsylvania
(Identify the person or describe the property to be searched and give its location):

Facebook accounts Fatayat.AIKhifah, al.kifah.3, al.kifah.9, and any and all accounts resolving to IP address 71.23.230.0, as more fully described in Attachment A.

The person or property to be searched, described above, is believed to conceal (Identify the person or describe the property to be seized):

See Attachment B.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before

April 10, 2015

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m.☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge

Honorable Elizabeth T. Hey

(name)

☒ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30).☐ until, the facts justifying, the later specific date of _____.

Date and time issued:

3/27/15 5:20 pm

Judge's signature

City and state:

Philadelphia PA

Honorable Elizabeth T. Hey
Printed name and title

JD 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of:		
Inventory of the property taken and name of any person(s) seized:		
Certification		
<p><i>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</i></p> <p>Date: _____</p> <div style="display: flex; justify-content: space-between; margin-top: 20px;"> <div style="width: 45%;"></div> <div style="width: 50%;"> <p>_____ <i>Executing officer's signature</i></p> <p>_____ <i>Printed name and title</i></p> </div> </div>		

ATTACHMENT A

LOCATION TO BE SEARCHED:

Facebook accounts:

- FatayalAlKhilafah;
- al.kifah.3;
- al.kifah.9;
- any and all accounts resolving to IP address 71.23.230.0;

stored at premises controlled by Facebook, 1601 Willow Road, Menlo Park, CA 94025

ATTACHMENT B

**Part One: ITEMS TO BE SEIZED:
(TO BE PROVIDED BY FACEBOOK)**

All posts and communications, records, files, logs, or information, including those items 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), dated from June 2013 through the present, including:

- A. The contents of all posts and communications associated with the aforementioned accounts, including stored or preserved copies of posts and communications sent to and from the accounts, the source and destination associated with each post and communication, the date and time at which each post and communication was sent, and the size and length of each post and communication;
- B. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which each account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account numbers);
- C. All records or other information stored at any time by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures and files; and
- D. All records pertaining to communications between the aforementioned accounts and any person regarding the accounts, including contacts with support services and records of actions taken.

**Part Two: ITEMS TO BE SEIZED:
(TO BE EXECUTED BY LAW ENFORCEMENT AGENTS)**

All information and data described above that constitute fruits, evidence, contraband, and/or instrumentalities of violations or attempts to violate 18 U.S.C. § 2339B (providing material support to a designated foreign terrorist organization), along with any evidence that would tend to show the true identities of the persons committing these offenses.

All available log files showing dates, times and IP addresses for access to these accounts.

*, attempting to provide,
and conspiring to provide*

Records relating to who created, used, or communicated with the accounts described above, including records about their identities and whereabouts.

15-391-M

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH WARRANTS**

I, Martin McDonald, being first duly sworn, hereby depose and state as follows:

Introduction

1. I make this affidavit in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search:

a. The residence located at PA
including any and all computers, hard drives, and electronic storage devices
contained therein;

b. The following accounts, associated with the following online facilities:

i. **Facebook:**

- Fatayat.AlKhilafah;
- al.kifah.3;
- al.kifah.9;
- Any and all accounts associated resolving to IP address 71.23.230.0;

iii. **Twitter:**

- @KhilafahAl;
- @Saajidah4life;
- Any and all accounts resolving to IP address 71.23.230.0.

Agent Background

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") within the meaning of Title 18, United States Code, Section 3052, and as such I am an officer of the United States who is authorized to investigate laws of the United States and to execute warrants issued under the authority of the United States. I have been employed as an FBI Special Agent since

November 2010. I am currently assigned to Counter-Terrorism Squad CT1 of the FBI's Philadelphia Division, and I work National Security matters. I have participated in the execution of numerous search and arrest warrants during my career to date. I have also been involved in investigations of numerous types of offenses against the United States, including crimes of terrorism such as material support of foreign terrorist organizations, and other violations as set forth in 18 U.S.C. § 2331, et seq.

3. The facts in this affidavit come from my personal observations, my training and experience, subpoenaed records, and information obtained from other agents and witnesses. This affidavit is being submitted for the limited purpose of obtaining search warrants. It does not contain every fact known to the United States about this matter.

Applicable Law

4. Title 18, United States Code, Section 2339B ("Providing material support or resources to designated foreign terrorist organizations") provides that, "[w]hoever knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so, shall be fined under this title or imprisoned not more than 15 years, or both."

5. Pursuant to Federal Rule of Criminal Procedure 41 ("Search and Seizure"), "a magistrate judge – in an investigation of domestic terrorism or international terrorism – with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district." Fed. R. Crim. P. 41(b)(3). As set forth below, activities related to international terrorism occurred within the Eastern District of Pennsylvania. Therefore, an Eastern District of Pennsylvania magistrate has authority to issue all related search warrants.

Technical Terms

6. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. **IP Address**: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. **Internet**: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. **Storage medium**: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

Statement of Probable Cause

7. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, § 2339B (providing material support or resources to a ^{attempting to provide, + conspiracy to provide} designated foreign terrorist organizations) will be found in the following locations: *M.M.*

~~_____~~

- a. The residence located at _____, PA _____, including any and all computers, hard drives, and electronic storage devices contained therein;
- b. The following online facilities, regarding the following usernames, user IDs and accounts:
 - i. Facebook:
 - Fatayat.AIKhilafah;
 - al.kifah.3;
 - al.kifah.9;
 - Any and all accounts resolving to IP address 71.23.230.0; and
 - iii. Twitter:
 - @KhilafahAI;
 - @Saajidah4life;
 - Any and all accounts resolving to IP address 71.23.230.0.

8. The FBI is conducting an investigation focused on the use of the Internet by Al Qaeda-affiliated terrorists and other terrorist groups to promote violent jihad. I am assigned to this investigation and have been investigating this activity since July of 2013. Over the course of this investigation, the FBI has identified specific individuals who use electronic communications and social networking websites to radicalize, recruit and provide material support to those who desire to participate in violent jihad and support the terrorist group the Islamic State of Iraq and al- Sham (ISIS), in violation of 18 U.S.C. § 2339B.

A. The Islamic State of Iraq and al-Sham (ISIS)

9. On October 15, 2004, the United States Secretary of State designated al-Qa'ida in Iraq (AQI), then known as Jam'at al Tawhid wa'al-Jihad, as a Foreign Terrorist Organization under Section 219 of the Immigration and Nationality Act, and as a Specially Designated Global Terrorist under section 1(b) of Executive Order 13224.

10. On May 15, 2014, the Secretary of State amended its AQI designations to add the alias "Islamic State of Iraq and the Levant" (ISIL) as its primary name. The Secretary also added additional aliases to the listing, including "the Islamic State of Iraq and al-Sham" and "the Islamic State of Iraq and Syria" (ISIS).

11. As a consequence of these Department of State designations, there is a prohibition against knowingly providing, or attempting or conspiring to provide, material support or resources to, or engaging in transactions with ISIS.

12. On or about August 19, 2014, ISIS claimed responsibility for the videotaped beheading of an American aid worker. On or about September 9, 2014, ISIS claimed responsibility for the videotaped beheading of another American aid worker. On or about September 13, 2014, ISIS claimed responsibility for the videotaped beheading of a British aid worker. On or about October 3, 2014, ISIS claimed responsibility for the videotaped beheading of another British aid worker. On or about February 3, 2015, ISIS released a video of a captured Jordanian Air Force Pilot being burned alive in a cage. On or about February 15, 2015, ISIS released a video of the beheading of 21 Coptic Christians in Libya. On or about February 24, 2015, ISIS kidnapped approximately 70-100 Assyrian Christians located in Northeast Syria, including men, women, and children.

B. Keonna Thomas, a/k/a "Fatayat Al Khilafah," residing at . PA

13. Keonna Thomas first came to the attention of the FBI in the Summer of 2013, based on her public online postings expressing support for violent jihad.

14. Investigation has confirmed that Keonna Thomas, a/k/a "Fatayat Al Khilafah," resides at . PA, which is a . home more fully described in Attachment A.

a. In February 2015, Keonna Thomas submitted an application for a United States Passport, listing her home address as . PA

b. Documents produced by an Internet Service Provider reveal that internet service is provided to Keonna Thomas, at . PA , and that her account is associated with IP address 71.23.230.0, as well as with various online accounts using username "Fatayat Al Khilafah."

c. Over the course of this investigation, IP address 71.23.230.0 has never been found to resolve anywhere other than to the address .

15. Public records searches and surveillance indicate that Keonna Thomas resides with only a few people, all of whom are close family, including two young children.

C. Use of Online Communication Facilities by Keonna Thomas, a/k/a "Fatavat Al Khilafah," to Provide Material Support to of ISIS

16. As set forth below, there is probable cause to believe Keonna Thomas, a/k/a "Fatayat Al Khilafah," is using and/or has used Twitter and Facebook to connect and communicate with other ISIS supporters, as well as to provide material support for ISIS in the

form of recruiting, fundraising, encouraging martyrdom, and making plans to travel overseas in order personally to achieve martyrdom for ISIS.

i. Twitter accounts

a. @KhilafahAl

17. Twitter account @KhilafahAl was assigned to a Twitter subscriber with the username "Fatayat Al Khilafah."

18. In response to a grand jury subpoena, Twitter produced records revealing that the @KhilafahAl account was associated with IP address 71.23.230.0, which as set forth above resolved to Keonna Thomas, PA. Twitter account @KhilafahAl is no longer active.

19. Between August 2013 and December 2014, Twitter account @KhilafahAl tweeted repeatedly in support of ISIS and its mission of violence, including messages indicating a plan to encourage and achieve martyrdom for ISIS. The government has had an opportunity to see these Twitter posts because they were posted in a manner that allowed the public to view them:

a. On August 14, 2013, @KhilafahAl posted on Twitter the following statement: "We love to die for Allah the way you love to live for shaytaan [Satan]."

b. On or about August 18, 2013, @KhilafahAl re-posted on Twitter a photograph of a young male child wearing firearm magazine pouches and camouflage attire, with the following caption: "Ask yourselves, while this young man is holding magazines for the Islamic state, what are you doing for it? #ISIS."

c. On or about October 1, 2013, @KhilafahAl posted on Twitter a photograph of former al-Qa'ida in the Arabian Peninsula leader Anwar Al Awlaki aiming an

AK-47, with the following caption: "My beloved sheikh Rahimahullah [Allah have mercy on him]."

d. On or about October 16, 2013, @KhilafahAl posted on Twitter a picture of U.S. Currency, with the following captions; "US Dollar notes donated by Kuwait nationals to the ISIS brothers;" and "Allahu Akbar [God is great]!! Support the Muslims by giving sadaqah [charity]."

e. On or about December 9, 2013, @KhilafahAl posted on Twitter the following statement: "Currently listening 2 virtues of martyrs by Sheikh Al Mujahid [violent jihadi fighter] Anwar Al Awlaki (RH)."¹

f. On or about December 14, 2013, @KhilafahAl re-posted on Twitter the following statement by another Twitter user; "'Happiness is the day of my martyrdom' – Sheikh Khalid al Husainan."

g. On or about December 23, 2013, @KhilafahAl re-posted on Twitter a video along with text advising that the video constitutes "a message to #muslims in the west from a British brother with #ISIS #Mujahideen #Syrin." The video is titled, "A message from a mujahid," and is accompanied by the following description: "ISIS mujahid gives some advice. Rayat al Tawheed. Official Media of the mujahideen."

h. On or about January 1, 2014, @KhilafahAl posted on Twitter the following statement: "I see why the mujahideen [violent jihadi fighters] Sacrifice Dunya [life on earth] for Akhirah [the afterlife] there's no comparison."

¹ "Virtues of Martyrs" is known to be a lecture by Anwar Al Awlaki, available online, during which he describes the spiritual rewards to be attained through engaging in violent jihad and dying as a martyr. Among other things, Awlaki stresses during this lecture that jihadist martyrs are held in the highest regard by Allah, and therefore that engaging in violent jihad and dying as a martyr is the most righteous path that a Muslim can take.

i. On or about January 1, 2014, @KhilafahAI re-posted on Twitter the following statement by another Twitter user: "Than why not come to the path of jihad which is more rewarding than any other acts that we can do. It's about time we stop being cowards."

j. On or about January 3, 2014, @KhilafahAI posted on Twitter the following statement: "Only thing I'm jcalous of is when I see the smiles of shuhadaa [martyrs]."

k. On or about January 15, 2014, @KhilafahAI posted on Twitter a photograph with the following text: "By the Lord of the Kaaba [a shrine in Mecca] I have succeeded." Accompanying this photograph, @KhilafahAI posted the following statement: "I want these to be my last words."

l. On or about January 30, 2014, @KhilafahAI re-posted on Twitter a photograph of an individual carrying an AK-47 weapon, with the following text: "Sponsor a Mujahid [violent jihadi fighter]." Accompanying the photograph, @KhilafahAI re-posted the following statement by another Twitter user: "Did you know... For as little as \$100 you can provide a #Mujahid with his basic necessities for 1 month?"

m. On or about February 23, 2014, @KhilafahAI re-posted on Twitter the following statement by another Twitter user: "It's so ajeeb [miraculous] when u see so called jihadis speaking against sisters who make Hijra [travel] 4 jihad as if females sahaba [associates of the prophet Muhammad] never fought fi subilillah [in the way of God]."

n. On or about March 9, 2014, @KhilafahAI posted on Twitter an image containing the following phrase: "KEEP CALM SUPPORT ISLAMIC STATE IRAQ AND SHAAM." Accompanying this post, @KhilafahAI posted the following statement: "Support dawla [referring to ISIS]."

o. On or about March 19, 2014, @KhilafahAI re-posted on Twitter the following statement by another Twitter user: "Imagine receiving glad tidings of Jannah [paradise] Come to Jihad and maybe this will be a reality."

p. On or about March 23, 2014, @KhilafahAI re-posted on Twitter the following statement by another Twitter user: "If you long for #martyrdom then be extra kind to orphans. Perhaps one day you will leave some behind."

q. On or about April 10, 2014, @KhilafahAI posted on Twitter the following statement, followed by images of a skull, flames, and a gun: "I need a permanent vacation that can only mean one thing." In response, another user of Twitter posted the following statement: "istishhaadi [martyrdom]."

r. On or about April 27, 2014, @KhilafahAI posted on Twitter the following statement regarding her history of being deleted from Facebook: "I would prefer the shahada [martyrdom] of being in the bodies of green birds² but FB shahada [Facebook martyrdom] means your doing something right lol."

s. On or about June 13, 2014, @KhilafahAI posted on Twitter the following statement: "For every violent action there's a violent reaction."

t. On or about June 23, 2014, @KhilafahAI posted on Twitter the following statement: "When you're a mujahid [violent jihadi fighter] your death becomes a wedding. #HoorAIAYn [pleasures in paradise]."

u. On or about September 24, 2014, @KhilafahAI posted on Twitter the following statement: "Dawah [a call to Islam] & jihad goes hand and hand."

² Based on my experience and expertise, the Affiant knows that a green bird is an Islamic symbol of martyrdom.

v. On or about October 9, 2014, @KhilafahAI posted on Twitter the following statement: "For u to die as a Muslim is a great blessing."

w. On or about October 10, 2014, @KhilafahAI posted on Twitter the following statement: "May Allah Ta Ala [God] give victory to the Muj [violent jihadi fighters] & destroy the kuffar & munabfiqeen [infidels & hypocrites] Ameen."

x. On or about November 15, 2014, @KhilafahAI re-posted on Twitter the following advice from another Twitter user about communication security: "Important: To all #IslamicState supporters Stop using Kik messenger n whatsapp Try chatsecure and cryptocat instead."

y. On or about December 6, 2014, @KhilafahAI re-posted on Twitter a photograph of a small male child with an AK-47 assault rifle around his neck, containing the following statement: "And if I were in Shaam [greater Syria], I wouldn't be pleased till I became soldier of the Islamic State."

20. The profile page associated with Twitter account @KhilafahAI has displayed an image of clouds and the text: "Fly with me As a green bird." As set forth above, @KhilafahAI also tweeted about the desire for martyrdom in the form "of being in the bodies of green birds."

b. @Saajidah4life

21. In response to a grand jury subpoena, Twitter associated account @Saajidah4life with IP address 71.23.230.0, which as set forth above resolved to Keonna Thomas,

PA. In addition, the profile pictures associated with Twitter account @Saajidah4life are known to be associated with Keonna Thomas.

22. As recently as December 2014, Twitter account @Saajidah4life communicated with a known overseas ISIS fighter about her desire to travel and evade the attention of law enforcement.

a. On or about December 2, 2014, the fighter posted a public tweet to Twitter account @Saajidah4life, stating: "i arrived and now going through training. Follow on this account until I get my phone." Twitter account @Saajidah4life responded with the public tweet, "I'm so happy for u." In response, the ISIS fighter sent a message to Twitter account @Saajidah4life stating, "You have no idea the blessing is it is to be in Raqqa [a city in Syria]." to which Twitter account @Saajidah4life responded, "alhumduillah Rabil Alameen [Thanks be to God]."

b. On or about December 2, 2014, Twitter account @Saajidah4life received a public tweet from this fighter stating, "children of the syrians is the future generation mujahidin [violent jihadi fighters]. Walaah They love Dawla [ISIS]."

c. On or about December 2, 2014, Twitter account @Saajidah4life received a public tweet from this fighter, stating, "trust me u haven't seen anything yet. U need to be here to see it."

2. Facebook accounts

23. Investigation has uncovered at least three Facebook accounts that appear to belong to the same "Fatayat Al Khilafah" who subscribes to the aforementioned Twitter accounts, including: (a) Fatayat.AlKhilafah; (b) al.kifah.3; and (c) al.kifah.9. These accounts not only use similar usernames, but all are identified by Facebook as belonging to a subscriber named "Fatayat Al Khilafah," they trace back to the same subscriber home address, and in some

instances they have been identified to contain similar pro-ISIS content revealing an intent to travel overseas, evade government scrutiny, and accomplish martyrdom for ISIS.

24. For example, from December 2013 – January 2014, one Facebook account belonging to subscriber “Fatayat Al Khilafah” exchanged a series of messages with another Facebook user who identified himself as a “mujahid [violent jihadi fighter],” and who is known to be a Somalia-based violent jihadi fighter originally from Minnesota. The government has had an opportunity to see these Facebook posts because they were produced to the government by Facebook in response to other lawful search warrants. In these messages, Facebook user “Fatayat Al Khilafah” discussed her jealousy of the fighter’s status as a violent jihadi fighter, her desire to travel overseas, and her desire to evade law enforcement because she has “moves to make”:

a. On or about May 25, 2014, Facebook user “Fatayat Al Khilafah” sent a message to the fighter stating: “I need to ask a question how is the situation for the mujajireen [emigrants] there.” In response, the fighter responded, “Jihad is hard but you always need sabr [patience or endurance] and to be firm.”

b. On or about December 12, 2013, Facebook user “Fatayat Al Khilafah” sent a message to this fighter advising that she should be “able to travel I should be getting some money soon.”

c. On or about December 13, 2013, Facebook user “Fatayat Al Khilafah” sent a message to this fighter advising that and that she “plan[ned] to leave the land of kufr [non-believers],” but cautioning that “[s]peaking here [on Facebook] about certain things is not . . . wise.”

d. On or about December 17, 2013, Facebook user "Fatayat Al Khilafah" sent a message to this fighter advising, "I have moves to make so I will be spending less time on here"

e. On or about December 31, 2013, Facebook user "Fatayat Al Khilafah" sent a message to this fighter advising that she feels "more comfortable to speak freely" on Paltalk, because "They don't monitor it."

f. On or about January 8, 2014, Facebook user "Fatayat Al Khilafah" sent a message to this fighter advising that she is "jealous" because her associate is "chilling like a Mujahid."

g. On or about January 11, 2014, Facebook user "Fatayat Al Khilafah" sent a message to this fighter advising that she is trying "to watch what I post here also giving my situation and what I want to do it's not good to draw attention to yourself." Facebook account Fatayat.AIKhilafah further explained that some people who "try to make moves" are unsuccessful because they put "their self out there."

a. Fatayat.AIKhilafah

25. Facebook account Fatayat.AIKhilafah is identified on Facebook as belonging to a subscriber named "Fatayat Al Khilafah (Al Kifah)." The government has had an opportunity to see some of the Facebook posts by Fatayat.AIKhilafah because they were made publicly viewable.

26. On or about December 31, 2013, Facebook account Fatayat.AIKhilafah posted the image of clouds, along with the text "Fly with me As a green bird" (which is also displayed by Twitter account @KhilafahAI). This posting caused another Facebook user to respond: "In the promised land, where our mission is to join the caravan of martyrs. May Allah choose us,

amen." Facebook account Fatayat.AIKhilafah responded with an Arabic phrase expressing agreement.

27. On or about August 24, 2014, Facebook user "Fatayat Al Khilafah" posted on Facebook the following statement: "yes im married to the geehad [jihad]."

28. The Facebook page for the Fatayat.AIKhilafah account has publicly displayed numerous photographs of people who appear to be women on battlefields armed with AK-47 weapons, captioned with the text: "Supporting the Fighters in the Battlefield."

b. al.kifah.3

29. Facebook account "al.kifah.3" is identified by Facebook as belonging to a subscriber named "Fatayat Al Khilafah."

30. In response to a grand jury subpoena, Facebook produced records revealing that the al.kifah.3 account is associated with IP address 71.23.230.0, which is the same IP address used by Twitter account @KhilafahAl. IP address 71.23.230.0 resolved to Keonna Thomas, PA.

c. al.kifah.9

31. Facebook account "al.kifah.9" is identified by Facebook as belonging to a subscriber named "Fatayat Al Khilafah."

32. In response to a grand jury subpoena, Facebook produced records revealing that al.kifah.9 is associated with phone number . A follow-up grand jury subpoena to the telephone company (Sprint) revealed that phone number . is associated with , PA, which is the same last name and home address associated with IP address 71.23.230.0, Twitter account @KhilafahAl, and Facebook account al.kifah.3.

33. The al.kifah.9 Facebook account not only shares a similar account name and username as the aforementioned Twitter and Facebook accounts, but its Facebook page includes similar postings, friends and followers. For example, the al.kifah.9 Facebook page has "liked" the Facebook page named "We are all Islamic State of Iraq & Shjaam – ISIS." In addition, the al.kifah.9 Facebook profile page has displayed the text: "I don't trust words, I trust actions. Keep calm and marry a Salafi Jihadi [member of the Silafi Muslim movement espousing violent jihad]."

3. Other Accounts Belonging to Keonna Thomas, a/k/a "Fatayat Al Khilafah," and/or resolving to IP Address 71.23.230.0

34. Based on the information contained in this Affidavit, the FBI is requesting authority to search all Twitter and Facebook accounts associated with Keonna Thomas's known IP address 71.23.230.0. Thomas "met" her associates and developed her plans online, both by way of email communications and social media postings. During discussions with her associates, Thomas maintained multiple online accounts and discussed with her associates the need to vary their account use in order to evade government scrutiny. Thus, FBI has probable cause to believe that evidence related to Thomas's criminal activity may reside on one or multiple Thomas accounts. Further, the most reliable way to establish Thomas's ownership of undiscovered accounts possibly containing evidence is by searching for accounts associated with her known IP address. I would therefore request that the search warrants direct providers to accounts linked to Thomas's known IP address, even if the user or channel names are not specified.

D. Last-Minute Purchase of Tickets to Travel Overseas

35. In February 2015, Keonna Thomas submitted an application for a United States Passport. Prior to this, Thomas had never before possessed a United States Passport. In this Passport application, Thomas listed her home address as _____, PA.

36. On or about March 26, 2015, Keonna Thomas purchased airline tickets to fly on March 29, 2015 (three days later), from Philadelphia International Airport, to Barcelona, Spain, returning to the United States on April 15, 2015.

37. In early 2015, ISIS published an advice manual designed to help individuals evade detection when traveling to Syria and Iraq in order to join ISIS. Step-by-step travel instructions contained therein advise such travelers to purchase round-trip tickets to popular vacation spots, specifically suggesting Spain, and to purchase a ticket to their final destination once overseas.

38. The ISIS manual further advises travelers to use various secure communication methods, such as Chat Secure, which Keonna Thomas has recommended to her associates.

Background about Facebook

39. Facebook is a company located at 1601 Willow Road, Menlo Park, CA 94025.

40. 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.

41. 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.

42. 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 "Facebook 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 "Facebook Friends" and a "News Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

43. 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.

44. 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 "Facebook Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

45. Facebook allows users to upload photos and videos. 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.

46. 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.

47. 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.

48. 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.

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

50. 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.

51. 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.

52. 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.

53. 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.

54. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications 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.

55. Some Facebook pages are affiliated with groups of users, rather than one individual user. Membership in the group is monitored and regulated by the administrator or head of the group, who can invite new members and reject or accept requests by users to enter. Facebook can identify all users who are currently registered to a particular group and can identify the administrator and/or creator of the group. Facebook uses the term "Group Contact Info" to describe the contact information for the group's creator and/or administrator, as well as a PDF of the current status of the group profile page.

56. 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.

57. Every device that connects to the Internet must use an IP address. Therefore, IP address and log information can help to identify which computers or other devices were used to access the Internet at any given time. Facebook retains IP logs for each username and IP address. These logs may contain information about the actions taken by the username or IP

address on Facebook, including information about the type of action, the date and time of the action, and the username 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.

58. 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.

59. Your affiant is aware that social networking, such as the use of Facebook, is an increasingly common way for persons to communicate. Your affiant is further aware that Facebook users often use the Facebook messaging and posting functions to provide one another alternate contact information, such as additional Facebook accounts, e-mail accounts, phone numbers, and/or other social networking contact information in order to continue and facilitate their communications privately.

60. 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.

Background about Twitter

61. Twitter, a business located at 1355 Market Street, Suite 900, San Francisco, CA 94103, owns and operates a free-access social-networking website of the same name that can be accessed at <http://www.twitter.com>. Twitter allows each user to create their own profile page, 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.

62. 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.

63. 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 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.

64. 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.

65. 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.

66. 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," "re-tweet," 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 re-tweeted 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).

67. 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.

68. 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.

69. 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.

70. 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). Twitter 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.

71. 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.

72. 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.

73. 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.

74. 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.

75. 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.

76. 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.

77. Your affiant is aware that social networking, such as the use of Twitter, is an increasingly common way for persons to communicate. Your affiant is further aware that Twitter users often use the Twitter messaging and posting functions to provide one another alternative contact information, such as additional Twitter accounts, e-mail accounts, phone numbers, and/or other social networking contact information in order to continue and facilitate their communications privately.

78. 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.

Computers, Electronic Storage, and Forensic Analysis

79. As described above and in Attachment B, this application seeks permission to search for records that might be found at : PA (the “premises”), in whatever form they are found. One form in which the records might be found is data stored on a computer’s hard drive or other electronic storage media, because voluminous relevant and inculpatory electronic communications have been identified during the course of this investigation which resolve to IP address 71.23.230.0, associated with Keonna Thomas, PA Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

80. *Probable cause.* I submit that if a computer or storage medium is found on the premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by

an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

81. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online

nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media 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, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime

under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a

computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

c. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

82. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can

take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. **Technical requirements.** Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. **Variety of forms of electronic media.** Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

83. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(c)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

84. Because several people share the premises as a residence, it is possible that the premises will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the

things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

Legal Discussion Regarding Online Accounts

85. Under 18 U.S.C. § 2703(g), a law enforcement officer does not have to be present for either the service or execution of the warrant. It is sufficient for us to serve it by fax or by mail upon Facebook and Twitter ("the Providers"), which host and operate the accounts that are the subject of these search warrants. I request that the Providers be required to produce the electronic communications and other information identified in Attachment A and Part One of Attachment B hereto. Because the Providers are not aware of the facts of this investigation, their employees are not in a position to search for relevant evidence. In addition, requiring the Providers to perform the searches would be a burden upon them. If the Providers are asked to do is produce all the files in the accounts, an employee can do that easily. Requiring the Providers to search the materials to determine what content is relevant would add to their burden.

86. With regard to the online accounts being searched, I request that the Court authorize law enforcement agents to seize only those items identified in Part Two of Attachment B, from what is produced by the Providers pursuant to the search warrants. In reviewing these items, I will treat them in the same way as if I were searching a file cabinet for certain documents. Items will be scanned quickly to determine if they are relevant to my search. If they are, they will be read. If I determine that they are not relevant, I will put them aside without reading them in full. This method is similar to what a law enforcement officer would do in the search of a filing cabinet or a seized computer.

87. Under 18 U.S.C. § 2703(b)(1)(A), notice to the customer or subscriber is not required when the government obtains the contents of electronic communications using a search warrant.

88. Under 18 U.S.C. §§ 2711(3) and 3127, this Court has the authority to issue this warrant directing the Providers, even though they are not located in this district, because the Court has jurisdiction over the offense being investigated.

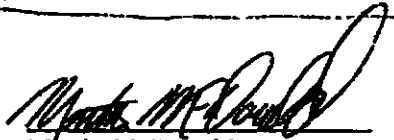
89. I also ask that the warrant direct the Providers to produce records and other information pertaining to the aforementioned accounts. The government may obtain such records either by filing a motion under 18 U.S.C. § 2703(d), or by means of a search warrant under § 2703(c)(1)(A). Since I need a search warrant to obtain the electronic communications anyway, I am proceeding in the request for records by search warrant as well. The facts set forth above to show probable cause also constitute specific and articulable facts, showing that there are reasonable grounds to believe that the records and other information sought are relevant and material to an ongoing criminal investigation, as required by 18 U.S.C. § 2703(d).

CONCLUSION

90. There is thus probable cause to believe that the aforementioned premises and online accounts, as described in Attachment A, contain evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2339B (providing material support to a designated foreign terrorist organization), as set forth in Attachment B.

M.M.

, attempting to provide,
and conspiracy to provide


Martin McDonald
Special Agent,
Federal Bureau of Investigation

SWORN TO AND
SUBSCRIBED
BEFORE ME THIS

27th day of March 2015


HONORABLE ELIZABETH T. HEY
UNITED STATES MAGISTRATE JUDGE

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

REDACTED

In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address)

)
)
) Case No. 15-477
)
)

Information associated with the
 following Google, Inc. accounts:

- Almuhajir84@gmail.com;
- KThomas2984@gmail.com; and
- any and all accounts resolving to
 IP address 71.23.230.0

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Pennsylvania
 (identify the person or describe the property to be searched and give its location):

Google Inc. accounts Almuhajir84@gmail.com; KThomas2984@gmail.com; and any and all accounts resolving to IP address 71.23.230.0, as more fully described in Attachment A.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Attachment B.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before

May 1, 2015

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m.

☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge

Honorable _____

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

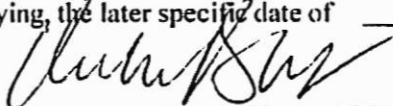
☐ for _____ days (not to exceed 30).

☐ until, the facts justifying, the later specified date of _____.

Date and time issued:

April 17, 2015

3:40 pm



Judge's signature

City and state:

Philadelphia PA

Honorable Richard A. Lloret

Printed name and title

REMOVED

At 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

<i>Return</i>		
<i>Case No.:</i>	<i>Date and time warrant executed:</i>	<i>Copy of warrant and inventory left with:</i>
<i>Inventory made in the presence of:</i>		
<i>Inventory of the property taken and name of any person(s) seized:</i>		
<i>Certification</i>		
<p><i>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</i></p>		
<i>Date:</i> _____	_____ <i>Executing officer's signature</i>	
	_____ <i>Printed name and title</i>	

ATTACHMENT A

LOCATION TO BE SEARCHED:

Google, Inc. accounts:

- Almuhajir84@gmail.com;
- KThomas2984@gmail.com; and
- Any and all accounts resolving to IP address 71.23.230.0

stored at premises controlled by Google, Inc., 1600 Amphitheatre Parkway, Mountain View, California, 94043

ATTACHMENT B

Part One: ITEMS TO BE SEIZED: (TO BE PROVIDED BY GOOGLE, INC.)

All communications, records, files, logs, or information, including those items that have been deleted but are still available to Google, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), dated from June 2013 through the present, including:

- A. The contents of all communications associated with the aforementioned accounts, including stored or preserved copies of communications sent to and from the accounts, the source and destination associated with each communication, the date and time at which each communication was sent, and the size and length of each communication;
- B. All records or other information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which each account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account numbers);
- C. All records or other information stored at any time by an individual using the accounts, including address books, contact and buddy lists, calendar data, pictures and files; and
- D. All records pertaining to communications between the aforementioned accounts and any person regarding the accounts, including contacts with support services and records of actions taken.

Part Two: ITEMS TO BE SEIZED: (TO BE EXECUTED BY LAW ENFORCEMENT AGENTS)

All information and data described above that constitute fruits, evidence, contraband, and/or instrumentalities of violations or attempts to violate 18 U.S.C. § 2339B (providing, attempting to provide, and conspiracy to provide material support to a designated foreign terrorist organization), along with any evidence that would tend to show the true identities of the persons committing this offenses.

All available log files showing dates, times and IP addresses for access to these accounts.

Records relating to who created, used, or communicated with the accounts described above, including records about their identities and whereabouts.

15-477

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR SEARCH WARRANTS**

I, Martin McDonald, being first duly sworn, hereby depose and state as follows:

Introduction

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search Google, Inc., for information from the following accounts:

- Almuhajir84@gmail.com;
- KThomas2984@gmail.com; and
- Any and all accounts resolving to IP address 71.23.230.0.

Agent Background

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") within the meaning of Title 18, United States Code, Section 3052, and as such I am an officer of the United States who is authorized to investigate laws of the United States and to execute warrants issued under the authority of the United States. I have been employed as an FBI Special Agent since November 2010. I am currently assigned to Counter-Terrorism Squad CT1 of the FBI's Philadelphia Division, and I work National Security matters. I have participated in the execution of numerous search and arrest warrants during my career to date. I have also been involved in investigations of numerous types of offenses against the United States, including crimes of terrorism such as material support of foreign terrorist organizations, and other violations as set forth in 18 U.S.C. § 2331, et seq.

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

affidavit is being submitted for the limited purpose of obtaining a search warrant. It does not contain every fact known to the United States about this matter.

Applicable Law

4. Title 18, United States Code, Section 2339B (“Providing material support or resources to designated foreign terrorist organizations”) provides that, “[w]hoever knowingly provides material support or resources to a foreign terrorist organization, or attempts or conspires to do so, shall be fined under this title or imprisoned not more than 15 years, or both.”

5. Pursuant to Federal Rule of Criminal Procedure 41 (“Search and Seizure”), “a magistrate judge – in an investigation of domestic terrorism or international terrorism – with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district.” Fed. R. Crim. P. 41(b)(3). As set forth below, activities related to international terrorism occurred within the Eastern District of Pennsylvania. Therefore, an Eastern District of Pennsylvania magistrate has authority to issue all related search warrants.

Technical Terms

6. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is,

long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

Statement of Probable Cause

7. The FBI is conducting an investigation focused on the use of the Internet by Al Qaeda-affiliated terrorists and other terrorist groups to promote violent jihad. I am assigned to this investigation and have been investigating this activity since July of 2013. Over the course of this investigation, the FBI has identified specific individuals who use electronic communications and social networking websites to radicalize, recruit and provide material support to the terrorist group the Islamic State of Iraq and the Levant (ISIL), in violation of 18 U.S.C. § 2339B.

8. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, § 2339B (providing, attempting to provide, and conspiracy to provide material support or resources to a designated foreign terrorist organization) will be found at Google, Inc. on the following accounts:

- Almuhajir84@gmail.com;
- KThomas2984@gmail.com; and
- Any and all accounts associated resolving to IP address 71.23.230.0.

A. The Islamic State of Iraq and the Levant (ISIL)

9. On October 15, 2004, the United States Secretary of State designated al-Qa'ida in Iraq (AQI), then known as Jam'at al Tawhid wa'al-Jihad, as a Foreign Terrorist Organization ("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.

10. On May 15, 2014, the Secretary of State amended the designation of al-Qa'ida in Iraq ("AQI") as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist entity under section 1(b) of Executive Order 13224 to add the alias Islamic State of Iraq and the Levant ("ISIL") as its primary name. The Secretary also added the following aliases to the ISIL listing: the Islamic State of Iraq and al-Sham ("ISIS"), the Islamic State of Iraq and Syria ("ISIS"), ad-Dawla al-Islamiyya fi al-'Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furqan Establishment for Media Production. Although the group has never called itself "Al-Qaeda in Iraq (AQI)," this name has frequently been used to describe it through its history. To date, ISIL remains a designated FTO.

11. As a consequence of these Department of State designations, there is a prohibition against knowingly providing, or attempting or conspiring to provide, material support or resources to, or engaging in transactions with ISIL.

12. On or about August 19, 2014, ISIL claimed responsibility for the videotaped beheading of an American aid worker. On or about September 9, 2014, ISIL claimed responsibility for the videotaped beheading of another American aid worker. On or about September 13, 2014, ISIL claimed responsibility for the videotaped beheading of a British aid worker. On or about October 3, 2014, ISIL claimed responsibility for the videotaped beheading

of another British aid worker. On or about February 3, 2015, ISIL released a video of a captured Jordanian Air Force Pilot being burned alive in a cage. On or about February 15, 2015, ISIL released a video of the beheading of 21 Coptic Christians in Libya. On or about February 24, 2015, ISIL kidnapped approximately 70-100 Assyrian Christians located in Northeast Syria, including men, women, and children.

B. Keonna Thomas, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness"

13. Keonna Thomas first came to the attention of the FBI in the Summer of 2013, based on her public online postings expressing support for violent jihad. The FBI has since identified many postings and communications by Thomas, on multiple online sites and facilities, and under various aliases including "Fatayat Al Khilafah" and "YoungLioness."

14. Prior to her incarceration on or about April 3, 2015, investigation confirmed that Keonna Thomas resided at _____ Documents produced by an Internet Service Provider reveal that internet service was provided to Keonna Thomas, at _____, and that her account was associated with IP address 71.23.230.0.

15. Over the course of this investigation, IP address 71.23.230.0 has never been found to resolve anywhere other than to the address _____

C. Use of Online Communication Facilities by Keonna Thomas to Provide Material Support to of ISIL

16. There is probable cause to believe Keonna Thomas has used multiple online accounts to connect and communicate with other ISIL supporters, as well as to provide material support for ISIL in the form of recruiting, fundraising, encouraging martyrdom, and making plans to travel overseas in order personally to fight with and achieve martyrdom for ISIL.

17. On April 3, 2015, Keonna Thomas was charged in a Criminal Complaint with knowingly attempting to provide material support and resources, as defined by 18 U.S.C. Section 2339A(b), to a designated foreign terrorist organization, to wit: ISIL, in violation of Title 18, United States Code Section 2339B. On April 9, 2015, the Complaint was upheld in a preliminary hearing before a U.S. Magistrate Judge.

18. The Affidavit attached to the Complaint alleges in relevant part as follows:

- a. On or about August 18, 2013, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," re-posted on Twitter a photograph of a young male child wearing firearm magazine pouches and camouflage attire, with the following caption: "Ask yourselves, while this young man is holding magazines for the Islamic state, what are you doing for it? #ISIS."
- b. On or about October 16, 2013, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," posted on Twitter a picture of U.S. Currency, with the following captions: "US Dollar notes donated by Kuwait nationals to the ISIS brothers;" and "Allahu Akbar [God is great]!! Support the Muslims by giving sadaqah [charity]."
- c. On or about December 12, 2013, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," sent an electronic communication to a known Somalia-based violent jihadi fighter originally from Minnesota (Co-Conspirator (CC) #1), who identified himself in his electronic communications as a "mujahid [violent jihadi fighter]." In this message, THOMAS stated that she should be "able to travel I should be getting some money soon."
- d. On or about December 13, 2013, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," sent an electronic communication to CC#1 advising that she "plan[ned] to leave the land of kufr [non-believers]," but cautioning that "[s]peaking here [online] about certain things is not . . . wise."
- e. On or about December 17, 2013, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," sent an electronic communication to CC#1 advising, "I have moves to make so I will be spending less time on here . . ."
- f. On or about December 17, 2013, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," re-posted on Twitter the following statement by another Twitter user: "'Happiness is the day of my martyrdom' – Sheikh Khalid al Husainan."
- g. On or about December 23, 2013, KEONNA THOMAS, a/k/a "Fatayat Al

Khilafah," a/k/a "YoungLioness," re-posted on Twitter a video along with text advising that the video constitutes "a message to #muslims in the west from a British brother with #ISIS #Mujahideen [violent jihadi fighter] #Syria." The video is titled, "A message from a mujahid," and is accompanied by the following description: "ISIS mujahid gives some advice. Rayat al Tawheed. Official Media of the mujahideen."

- h. On or about January 1, 2014, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," posted on Twitter the following statement: "I see why the mujahideen [violent jihadi fighters] Sacrifice Dunya [life on earth] for Akhirah [the afterlife] there's no comparison."
- i. On or about January 4, 2014, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," posted on Twitter the following statement: "Only thing I'm jealous of is when I see the smiles of shuhadaa [martyrs]."
- j. On or about January 15, 2014, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," posted on Twitter the following statement: "I want these to be my last words." Accompanying this statement was a photograph of the following text: "By the Lord of the Kaaba [a shrine in Mecca] I have succeeded."
- k. On or about January 30, 2014, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," re-posted on Twitter a photograph of an individual carrying an AK-47 weapon, with the following text: "Sponsor a Mujahid [violent jihadi fighter]." Accompanying the photograph, THOMAS re-posted the following statement by another Twitter user; "Did you know... For as little as \$100 you can provide a #Mujahid with his basic necessities for 1 month?"
- l. On or about April 10, 2014, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," posted on Twitter the following statement, followed by images of a skull, flames, and a gun: "I need a permanent vacation that can only mean one thing." In response, another user of Twitter posted the following statement: "istishhaadi [martyrdom]."
- m. On or about April 27, 2014, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," posted on Twitter the following statement: "I would prefer the shahada [martyrdom] of being in the bodies of green birds." Based on my experience and expertise, this is a reference to the belief that the souls of martyrs are held in the hearts of green birds.
- n. On or about June 23, 2014, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," posted on Twitter the following statement: "When you're a mujahid [violent jihadi fighter] your death becomes a wedding. #HoorAlAyn [pleasures in paradise]."
- o. On or about October 10, 2014, KEONNA THOMAS, a/k/a "Fatayat Al

Khilafah," a/k/a "YoungLioness," posted on Twitter the following statement: "May Allah Ta Ala [God] give victory to the Muj [violent jihadi fighters] & destroy the kuffar & munabfiqeen [infidels & hypocrites] Ameen."

- p. On or about December 2, 2014, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," posted on Twitter the following statement: "If we truly knew the realities . . . we all would be rushing to join our brothers in the front lines pray ALLAH accept us as shuhada [martyrs]."
- q. On or about December 2, 2014, a known overseas ISIL fighter (CC#2) sent an electronic communication to KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," stating "i arrived and now going through training. Follow on this account until I get my phone." THOMAS responded with the electronic communication, "I'm so happy for u." CC#2 responded, "You have no idea the blessing is it is to be in Raqqa [a city in Syria]," to which THOMAS responded, "alhumduillah Rabil Alameen [Thanks be to God]."
- r. On or about December 2, 2014, CC#2 sent an electronic communication to KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," stating, "children of the syrians is the future generation mujahidin [violent jihadi fighters]. Walaah They love Dawla [ISIL]."
- s. On or about December 2, 2014, CC#2 sent an electronic communication to KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," stating, "trust me u haven't seen anything yet. U need to be here to see it."
- t. On or about December 6, 2014, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," re-posted on Twitter a photograph of a small male child with an AK-47 assault rifle around his neck, containing the following statement: "And if I were in Shaam [greater Syria], I wouldn't be pleased till I became soldier of the Islamic State."
- u. On or about January 30, 2015, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," sent an electronic communication to a radical Islamic cleric located in Jamaica (CC#3) stating, "i don't want to say much here . . . as of now im still here in the states but will be leaving soon."
- v. On or about February 4, 2015, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," submitted an application for a United States Passport.
- w. On or about February 14, 2015, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," sent an electronic communication to CC#3 stating, "deactivated my twitter till i leave for sham [greater Syria]. . . don't want to draw attention of the kuffar [non-believers] and it mess my plans and they take my pass port and i get stuck here."

- x. On or about February 14, 2015, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," sent an electronic communication to CC#3 advising that she sought help from CC#2 regarding "routes" and her "travel plan."
- y. On or about February 17, 2015, CC#2 sent an electronic communication to KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," stating, "Even my wife . . . If she turned out after all these yrs to be a spy I will personally blow her brains all over the bedroom . . . Even to u if I married U and u betrayed me But if my wife comes and it turns out she was a spy after all these yrs . . . I will personally behead her." In response, THOMAS stated, "cutting head is more personal."
- z. On or about February 17, 2015, CC#2 sent an electronic communication to KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," stating, "U probably want to do Istishadee [martyrdom operations] with me." In response, THOMAS stated, "that would be amazing. . . . a girl can only wish." CC#2 then responded, "I can make that wish come true."
- aa. In February and March 2015, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," conducted online research into various indirect travel routes to Turkey.
- bb. On or about March 23, 2015, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," purchased an electronic visa, in her own name, for travel to Turkey.
- cc. Turkey is known to be the most common and most direct transit point for individuals traveling from locations in Europe who are seeking to enter Syria and join ISIL. In addition, an ISIL manual published in early 2015 recommends that ISIL recruits travel to Turkey in order to slip over the border into neighboring Syria. This manual further advises such ISIL travelers to purchase round-trip tickets to popular vacation spots, specifically suggesting Spain, and to purchase tickets to the final destination once overseas.
- dd. On or about March 25, 2015, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," conducted online research into "buses from Barcelona to Istanbul."
- ce. On or about March 26, 2015, KEONNA THOMAS, a/k/a "Fatayat Al Khilafah," a/k/a "YoungLioness," purchased airline tickets to fly on March 29, 2015 (three days later), from Philadelphia International Airport, to Barcelona, Spain, returning to the United States on April 15, 2015.

E. Google Accounts Linked to Keonna Thomas

- 19. Investigation has revealed two different Google email accounts linked to Keonna

Thomas. One such account (almuhajir84@gmail.com) is linked to her online alias communications regarding violent jihad and ISIL. The other account (KThomas2984@gmail.com) is linked to the travel arrangements she ultimately made in her true name.

a. Almuhajir84@gmail.com

20. In March 2014, the FBI received grand jury subpoena returns from Twitter which revealed that Keonna Thomas's Twitter account was associated with email address almuhajir84@gmail.com, and IP address 71.23.230.0, which, as set forth above, resolved to Thomas's home.

21. On or about March 27, 2015, U.S. Magistrate Elizabeth T. Hey signed a warrant to search the home of Keonna Thomas. Agents conducting this search recovered a laptop computer from Thomas's bedroom, on which had been preserved various electronic communications and programs containing Thomas's online discussions of her desire to achieve martyrdom on behalf of ISIL. A search of one such program's publicly available directory revealed that Thomas's online account is associated with email address almuhajir84@gmail.com.

b. KThomas2984@gmail.com

22. When agents searched the home of Keonna Thomas, they recovered from her person a smart phone containing a Google application accessing email address kthomas2984@gmail.com. Further analysis of the telephone revealed that Thomas had used this gmail address to make travel plans to Spain and Turkey in her real name, as set forth in the Complaint, including the following items recovered from the phone:

a. A receipt for Thomas's airplane ticket to Barcelona, which was purchased using email address kthomas2984@gmail.com.

b. Thomas's electronic visa application, which was obtained using email address kthomas2984@gmail.com.

Background About Google

23. Google Inc. (1600 Amphitheatre Parkway, Mountain View, California, 94043) is an internet service provider that allows subscribers to obtain e-mail accounts at the domain "gmail.com."

24. The computers of Google Inc. ("Google") often contain fruits, instrumentalities, and evidence of crimes in which the participants are subscribers who communicate electronically with one another:

a. Google's computers are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for their subscribers) and information concerning subscribers and their use of Google, Inc.' services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may reveal the means, method, participants, and occasions of committing criminal activity, and also can be used to identify an account's user or users.

b. A subscriber can also store with Google files in addition to e-mails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an e-mail account may be found in such address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

c. In my training and experience, e-mail providers generally ask their

subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account numbers). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

d. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. 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 the e-mail account.

e. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail 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. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to

identify the account's user or users.

Legal Discussion Regarding Online Accounts

25. Under 18 U.S.C. § 2703(g), a law enforcement officer does not have to be present for either the service or execution of the warrant. It is sufficient for us to serve it by fax or by mail upon Google, Inc., which host and operate the accounts that are the subject of these search warrants. I request that Google, Inc. be required to produce the electronic communications and other information identified in Attachment A and Part One of Attachment B hereto. Because Google, Inc. is not aware of the facts of this investigation, their employees are not in a position to search for relevant evidence. In addition, requiring Google, Inc. to perform the searches would be a burden upon it. If Google, Inc. is asked only to produce all the files in the accounts, an employee can do that easily. Requiring Google, Inc. to search the materials to determine what content is relevant would add to their burden.

26. With regard to the online accounts being searched, I request that the Court authorize law enforcement agents to seize only those items identified in Part Two of Attachment B, from what is produced by Google, Inc. pursuant to the search warrant. In reviewing these items, I will treat them in the same way as if I were searching a file cabinet for certain documents. Items will be scanned quickly to determine if they are relevant to my search. If they are, they will be read. If I determine that they are not relevant, I will put them aside without reading them in full. This method is similar to what a law enforcement officer would do in the search of a filing cabinet or a seized computer.

27. Under 18 U.S.C. § 2703(b)(1)(A), notice to the customer or subscriber is not required when the government obtains the contents of electronic communications using a search warrant.

28. Under 18 U.S.C. §§ 2711(3) and 3127, this Court has the authority to issue this warrant directing Google, Inc., even though it is not located in this district, because the Court has jurisdiction over the offense being investigated.


29. I also ask that the warrant direct Google, Inc. to produce records and other information pertaining to the aforementioned accounts. The government may obtain such records either by filing a motion under 18 U.S.C. § 2703(d), or by means of a search warrant under § 2703(c)(1)(A). Since I need a search warrant to obtain the electronic communications anyway, I am proceeding in the request for records by search warrant as well. The facts set forth above to show probable cause also constitute specific and articulable facts, showing that there are reasonable grounds to believe that the records and other information sought are relevant and material to an ongoing criminal investigation, as required by 18 U.S.C. § 2703(d).

CONCLUSION

30. There is thus probable cause to believe that the aforementioned online accounts, as described in Attachment A, contain evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2339B (providing, attempting to provide, and conspiracy to provide material support to a designated foreign terrorist organization), as set forth in Attachment B.

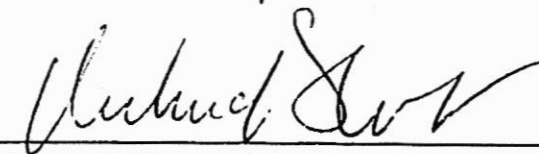
31. Based on the information contained in this Affidavit, the FBI is requesting authority to search all Google accounts associated with Keonna Thomas's known IP address 71.23.230.0. Thomas "met" her associates and developed her plans online, both by way of email

communications and social media postings. During discussions with her associates, Thomas maintained multiple online accounts and discussed with her associates the need to vary their account use in order to evade government scrutiny. Thus, FBI has probable cause to believe that evidence related to Thomas's criminal activity may reside on one or multiple Thomas accounts. Further, the most reliable way to establish Thomas's ownership of undiscovered accounts possibly containing evidence is by searching for accounts associated with her known IP address. I would therefore request that the search warrants direct providers to accounts linked to Thomas's known IP address, even if the user or channel names are not specified.


Martin McDonald
Special Agent,
Federal Bureau of Investigation

SWORN TO AND
SUBSCRIBED
BEFORE ME THIS

17th day of April 2015


HONORABLE RICHARD A. LLORET
UNITED STATES MAGISTRATE JUDGE

mmB

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

35

UNITED STATES OF AMERICA

v.

KEONNA THOMAS,
a/k/a "Fatayat Al Khilafah,"
a/k/a "YoungLioness"

FILED

DEC 2 2015

CRIMINAL NO. 15-171

MICHAEL S. PIZ, Clerk
By [Signature] Dep. Clerk

NOTICE OF CLASSIFIED EX PARTE ORDER

THIS MATTER is before the Court on an *ex parte*, *in camera* submission by the Government in the above-captioned matter, filed on November 13, 2015 (Docket No. 31). The Court hereby provides notice that on this date, the 1st day of December, 2015, 2015, it entered a classified, *ex parte* order through the Classified Information Security Officer.

BY THE COURT:

[Signature]
HONORABLE MICHAEL M. BAYLSON
Judge, United States District Court

REDACTED

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

UNITED STATES OF AMERICA

v.

KEONNA THOMAS

:
:
:
:
:
:
:

CRIMINAL NUMBER 15-171-1

FILED UNDER SEAL

SEALING ORDER

AND NOW, this day of , 2016, upon consideration of the
Defendant's Reply to the Government's Motion in Opposition to a Bill of Particulars, it is
ORDERED that said reply is **FILED UNDER SEAL**.

BY THE COURT:

**_____
THE HONORABLE MICHAEL M. BAYLSON
Senior United States District Court Judge**

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA

V.

KEONNA THOMAS

:
:
:
:
:
:

CRIMINAL NUMBER 15-171-1

FILED UNDER SEAL

ORDER

AND NOW, this day of 2016, upon consideration of the Defendant Keonna Thomas's Motion for a Bill of Particulars, and the Government's response thereto, it is **ORDERED** that the Government file a Bill of Particulars, as set forth in Defendant's Motion, and serve a copy of same on counsel for Keonna Thomas within ____ days.

BY THE COURT:

THE HONORABLE MICHAEL M. BAYLSON
Senior United States District Court Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA

V.

KEONNA THOMAS

:
:
:
:
:
:

CRIMINAL NUMBER 15-171-1

FILED UNDER SEAL

**REPLY IN SUPPORT OF DEFENDANT'S
MOTION FOR A BILL OF PARTICULARS**

DISCUSSION

Without A Bill Of Particulars, Ms. Thomas Cannot Adequately Prepare A Defense To The Government's Non-Specific Allegations.

Ms. Thomas still requires clarity as to the nature of the allegations against her because the Complaint, Indictment, and discovery fail to elucidate what the Government means when it accuses Ms. Thomas of attempting to provide herself as *personnel* to ISIL. Applying 18 U.S.C. § 2339B(h)'s specific definition of "personnel" in this context, Ms. Thomas must know what the Government believes constituted her attempt "to work under [ISIL's] direction or control, or to organize, manage, supervise, or otherwise direct the operation of that organization" between August 2013 and March 2015. Without this information, Ms. Thomas cannot adequately prepare a meaningful defense, nor can she plead this case as a bar to double jeopardy, since the Government could, hypothetically, file a subsequent indictment with the same charge during the same dates in question, but with different conduct in mind. Accordingly, a bill of particulars is necessary.

The Government claims that its discovery to date is sufficient to facilitate Ms. Thomas's understanding of the nature of the allegations against her, but this is not true. *See* Motion in

Opposition, Pacer Entry 43 at 6. Taken as a whole, the Government's discovery can be divided into two categories: (1) online communications between Ms. Thomas and her three alleged co-conspirators in which they discuss Ms. Thomas's marital status and the possibility of her moving to Syria, interspersed with esoteric exchanges concerning "jihad" and Islamic martyrdom, and (2) content from her telephone, home computer, and social media accounts that, at worst, suggests that she had a fascination with radical Islamic literature and teachings. What's missing is any concrete information detailing how Ms. Thomas attempted to offer herself to ISIL as "personnel" under § 2339B(h)'s restrictive definition – unless, of course, it is the Government's theory that Ms. Thomas's alleged marriage to an ISIL fighter and alleged travel plans to Syria *alone* exposed her to criminal liability.

But this does not seem to be the case, particularly given the Government's vague assertion in its Opposition that "[t]he Indictment, Complaint Affidavit, and discovery, taken together, outline conduct beyond attempted marriage and a desire to move." *See* Motion in Opposition, Pacer Entry 43 at 10, note 2. Ms. Thomas can only assume that this statement alludes to excerpts of certain online communications _____ she exchanged with a purported ISIL fighter, alleged co-conspirator number 2 (CC#2), which took place in February 2015. In one of the exchanges that the Government frequently references (*see, e.g.*, Motion in Opposition, Pacer Entry 43 at 3), _____

(attached hereto as Ex. A).

Ms. Thomas then answered, "[A] girl can only

wish,” to which CC#2 promised, “I can make that wish come true.” *Id.*

Based on this and other similar exchanges, it remains unclear whether Ms. Thomas and CC#2 actually discussed the possibility of Ms. Thomas’s participation in ISIL operations, or whether they were just flirting with one another. Regardless, if the Government actually believes or intends to prove that Ms. Thomas planned on managing, directing, or even participating in any suicide bombings or other ISIL-sponsored terror attacks, it must say so. Otherwise, Ms. Thomas is left guessing as to the full extent of the allegations against her, limiting her ability to prepare for trial.

Further, the Government cannot credibly reply upon *United States v. Pugh*, 2015 WL 9450598 (E.D.N.Y. Dec. 21, 2015) in support of its Motion in Opposition because *Pugh* is absolutely distinguishable from Ms. Thomas’s situation. In *Pugh*, the defendant was also charged with attempting to provide himself as personnel to ISIL, and he moved for a bill of particulars seeking clarity on the “material support and resources that he attempted to provide” the organization. *Id.* at *27. In denying the defendant’s motion, the court explained that “Pugh has not demonstrated that he is unable to determine the nature of the charges leveled against him,” an entirely reasonable decision given that the defendant was a former member of the U.S. Air Force who “received training in the installation and maintenance of aircraft engine, navigation, and weapons systems,” and later worked as a private military contractor in Iraq. *Id.* at *1. Pugh not only “expressed his desire to travel to the Middle East to fight Jihad,” but he also purchased a *one-way* ticket from Cairo, Egypt, to Istanbul, Turkey, in January 2015. *Id.* Upon arriving in Istanbul on January 10, Pugh was seized by Turkish officials, denied entry, returned to Cairo, and detained by Egyptian officials that same day. *Id.* Shortly thereafter, Pugh returned to JFK Airport, and told an undercover agent that he “had traveled to Turkey in an attempt to join ISIL,”

explaining that he had “gained experience working with airplanes during his service in the U.S. Air Force.” *Id.* at *2.

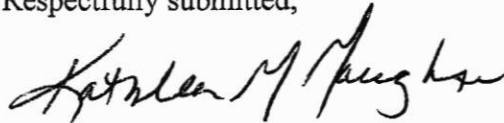
Thus, because Pugh possessed specialized weapons and aerospace training, purchased and executed a one-way ticket to Istanbul, and allegedly bragged about his military expertise to an undercover agent, it is no surprise that the court denied his request for a bill of particulars. Indeed, given Pugh’s background alone, the Government’s specific theory underlying his indictment seems obvious: Pugh attempted to travel to Syria in order to “organize, manage, supervise, or otherwise direct” ISIL’s weapons and aerospace operations. 18 U.S.C. § 2339B(h).

In contrast, Ms. Thomas is a far less sophisticated actor than Pugh, a mother of two from North Philadelphia with no high school diploma, specialized training, military expertise, or experience in the Middle East. Rather than purchasing and effectuating a one-way ticket to Istanbul, Ms. Thomas purchased a round-trip ticket to Spain and never even made it to the airport. Accordingly, the Government’s theory as to how Ms. Thomas attempted to provide herself to ISIL as “personnel” is far from obvious, especially since the discovery to date is devoid of any concrete plans by Ms. Thomas to participate in, manage, supervise, or otherwise direct any ISIL activities. The only discernible allegation supported by the discovery is Ms. Thomas’s desire to marry an ISIL fighter and travel to Syria. If this is the extent of the Government’s allegations, then so be it, but the Government must make that clear. Trial preparation issues aside, Ms. Thomas’s double jeopardy concerns are serious and cannot be assuaged simply by the fact that the indictment is limited to a specific date range. Again, “personnel” can encompass a myriad of activities, anything from participating in suicide attacks to managing social media accounts. Therefore, the Government must clarify its allegations against Ms. Thomas and articulate the particulars underlying its belief that Ms. Thomas

attempted to provide herself to ISIL as "personnel," pursuant to § 2339B(h)'s specific definition.

WHEREFORE, Keonna Thomas respectfully requests that the Court order the Government to issue the Bill of Particulars sought for all of the above stated reasons, the reasons stated in her initial motion, and any other reason that this Court deems just.

Respectfully submitted,



/s/ Kathleen M. Gaughan

KATHLEEN M. GAUGHAN
Assistant Federal Defender



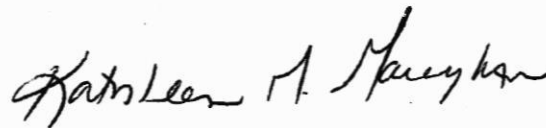
/s/ Elizabeth L. Toplin

ELIZABETH L. TOPLIN
Assistant Chief, Trial Unit

Exhibit A

CERTIFICATE OF SERVICE

I, Kathleen M. Gaughan, Assistant Federal Defender, Federal Community Defender Office for the Eastern District of Pennsylvania, hereby certify that I have filed under seal and served a copy of the Defendant's Motion for a Bill of Particulars Pursuant to Rule 7(f) of the Federal Rules of Criminal Procedure thereof, upon Jennifer A. Williams, Assistant United States Attorney, United States Attorney's Office, Suite 1250, 615 Chestnut Street, Philadelphia, Pennsylvania 19106.

A handwritten signature in black ink, appearing to read "Kathleen M. Gaughan", written in a cursive style.

/s/ Kathleen M. Gaughan
KATHLEEN M. GAUGHAN
Assistant Federal Defender

DATE: April 19, 2016

MMB

48

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA :

v.

KEONNA THOMAS

FILED

APR 25 2016

MICHAEL E. KUNZ, Clerk
By  Dep Clerk

CRIMINAL NUMBER 15-171-1

FILED UNDER SEAL

SEALING ORDER

AND NOW, this 25th day of April, 2016, upon consideration of the

Defendant's Reply to the Government's Motion in Opposition to a Bill of Particulars, it is

ORDERED that said reply is **FILED UNDER SEAL**.

BY THE COURT:



THE HONORABLE MICHAEL M. BAYLSON
Senior United States District Court Judge

MMB

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

62

UNITED STATES OF AMERICA

v.

KEONNA THOMAS

CRIMINAL NUMBER 15-171-1

FILED UNDER SEAL

FILED

JUN 30 2016

MICHAEL E. KUNTZ, CLERK
U.S. DISTRICT COURT

SEALING ORDER

AND NOW, this 30th day of June, 2016, upon consideration of
the Defendant's Motion for Notice and Discovery of Surveillance Used in the Government's
Investigation of the Defendant, it is **ORDERED** that said motion is **FILED UNDER SEAL**.

BY THE COURT:



THE HONORABLE MICHAEL M. BAYLSON
Senior United States District Court Judge

MMB

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

64

UNITED STATES OF AMERICA :

v. :

CRIMINAL NO. 15-171

KEONNA THOMAS,
a/k/a "Fatayat Al Khilafah,"
a/k/a "YoungLioness" :

FILED UNDER SEAL

FILED

JUN 30 2016

ORDER

AND NOW, this 30th day of June, 2016, upon

consideration of the Government's Unopposed Motion for Extension of Time to Respond to Motion, it is ORDERED AND DECREED that the government's motion is GRANTED. The government's response to Defendant's Motion for Notice and Discovery of Surveillance Used in the Government's Investigation of the Defendant shall be filed and served no later than July 19, 2016.

IT IS FURTHER ORDERED that the government's Motion, this Order, and the accompanying docket papers, shall be FILED UNDER SEAL.

BY THE COURT:


HONORABLE MICHAEL M. BAYLSON
Judge, United States District Court

email copy to:
J. Williams, AUSA
E. Toplis, Fed Def.
K. Gough, Fed Def.

MMB

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

70

UNITED STATES OF AMERICA :

v. :

CRIMINAL NO. 15-171

KEONNA THOMAS,
a/k/a "Fatayat Al Khilafah,"
a/k/a "YoungLioness" :

FILED UNDER SEAL

FILED

JUL 25 2016

SEALING ORDER

LUCY V. CHIN, Interim Clerk
By FK Dep. Clerk

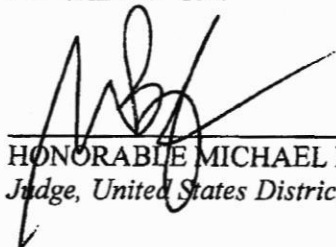
AND NOW, this 22nd day of

July

, 2016, upon

consideration of the Government's Response in Opposition to Defendant's Motion for Notice and
Discovery of Surveillance Used in the Government's Investigation of the Defendant, it is hereby
ORDERED that said Response is FILED UNDER SEAL.

BY THE COURT:



HONORABLE MICHAEL M. BAYLSON
Judge, United States District Court