

UNITED STATES DISTRICT COURT

FILED

for the

Eastern District of California

MAR 01 2016

CLERK, U.S. DISTRICT COURT EASTERN DISTRICT OF CALIFORNIA BY DEPUTY CLERK

In the Matter of the Search of (1) Samsung Galaxy cell phone, model number: SM-G900V, IMEI: 990004943238596; (2) Apple iPhone 6S, FCC ID: BCG-E2946A, white in color, CURRENTLY LOCATED AT SACRAMENTO FBI EVIDENCE CONTROL ROOM

Case No.

2:16-SW-0123 EFB

APPLICATION FOR A SEARCH WARRANT

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

SEE ATTACHMENT A, attached hereto and incorporated by reference.

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

SEE ATTACHMENT B, attached hereto and incorporated by reference

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

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

The search is related to a violation of

18 USC section 1001, providing materially false, fictitious, and fraudulent statements and representations in a matter within the jurisdiction of an agency of the United States, an offense involving international terrorism as defined as 18 USC section 2331; and

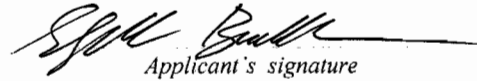
18 USC section 2339A attempting to provide or providing material support or resources, namely, personnel (including himself), knowing or intending that they were to be used in preparation for, or in carrying out, a violation of Title 18 USC section 956(a)(1)(conspiracy to kill, kidnap, main, or injure persons outside the United States)

The application is based on these facts:

SEE AFFIDAVIT, attached hereto and incorporated by reference.

- checkbox Continued on the attached sheet. checkbox Delayed notice days (give exact ending date if more than 30 days) is requested

under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



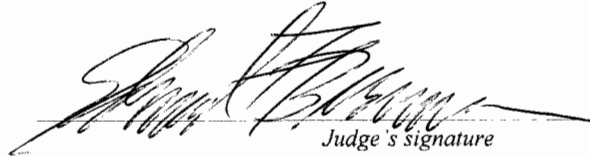
Applicant's signature

Elizabeth Buckmiller, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 3-1-2016



Judge's signature

City and state: Sacramento, California

Edmund F. Brennan, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A

The property to be searched is **(1) Samsung Galaxy cell phone, model number: SM-G900V, IMEI: 990004943238596; (2) Apple iPhone 6S, FCC ID: BCG-E2946A, white in color**, hereinafter the “Devices.” The Devices are currently located in the SACRAMENTO FBI EVIDENCE CONTROL ROOM.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

ITEMS TO BE SEIZED

1. All records relating to violations of 18 U.S.C. § 2339A, those violations involving Aws Mohammed Younis Al-Jayab (“Al-Jayab”) and any accomplices, and all records relating to violations of 18 U.S.C. § 1001, involving Al-Jayab, and, namely:
 - a. Records, documents, programs, applications, and materials pertaining to use of, and/or ownership interest in, the **SUBJECT DEVICES** (as described more fully in Attachment A);
 - b. Records, documents, programs, applications, and materials pertaining to communications sent or received or accessed by Al-Jayab that relate to the provision of money, goods, personnel, or services to individuals outside the United States; terrorist or military-like activities; violent acts; individuals or groups who have committed or intend to commit violent acts or acts against non-Muslims or persons who do not comply with the interpretation of Islam advocated by Islamic extremists; and travel outside the United States; all of the above as they relate to the offenses described in this affidavit, 18 U.S.C. § 1001 and 2339A;
 - c. Records, documents, programs, applications, and materials tending to show Al-Jayab’s associates, including address books, telephone numbers, and contacts or friends lists; all of the above as they relate to the offense described in this affidavit, 18 U.S.C. § 1001 and 2339A;
 - d. Records, documents, programs, applications, and materials tending to show the activities of Al-Jayab, including journals, calendars, and diaries; all of the above as they relate to the offense described in this affidavit, 18 U.S.C. § 1001 and 2339A;

- e. Records, documents, programs, applications, and materials tending to show the financial activities of Al-Jayab; all of the above as they related to the offense described in this affidavit, 18 U.S.C. § 1001 and 2339A;
- f. Records, documents, programs, applications, and materials pertaining to travel, including information related to passports, travel receipts, tickets, reservations, and schedules; all of the above as they related to the offense described in this affidavit, 18 U.S.C. § 1001 and 2339A;
- g. Records, documents, programs, applications, and materials pertaining to Cyprus, Great Britain, Iraq, Israel, Jordan, Palestine, Syria, or Turkey;
- h. Records, documents, programs, applications, and materials pertaining to any designated foreign terrorist organization, terrorist group, or terrorist;
- i. Records, documents, programs, applications, and materials pertaining to Islamic extremism;
- j. Records, documents, programs, applications, and materials related to Islamic extremism or violent jihad;
- k. Records, documents, programs, applications, and materials pertaining to martyrdom or suicide;
- l. Evidence of who used, owned, or controlled the device 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, e-mail, e-mail contacts, chat and messaging logs, photographs, and correspondence;

- m. Evidence of the presence or absence of software that would allow others to control the device, 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;
- n. Evidence of the attachment of other devices;
- o. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;
- p. Evidence of the times the device was used;
- q. Passwords, encryption keys, and other access devices that may be necessary to access the device;
- r. Applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;
- s. Records of or information about Internet Protocol addresses used by the device; and,
- t. Records of or information about the device'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.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include information created, modified, or stored in any form, including in digital form on any digital device.

3. Any and all names, words, telephone numbers, email addresses, time/date information, messages or other electronic data in the memory of the mobile telephone or on a serve and associated with the mobile telephone and described as the mobile telephones':

Incoming call history;

Outgoing call history;

Missed call history;

Outgoing text messages;

Incoming text messages;

Draft text messages;

Telephone book;

Data screen or file identifying the telephone number associated with the mobile telephone searched;

Data screen, file, or writing containing serial numbers or other information to identify the mobile telephone searched;

Voicemail,

User-entered messages (such as to-do lists); and

Photographs.

Any passwords used to access the electronic data described above.

BENJAMIN B. WAGNER
United States Attorney
JILL M. THOMAS
Assistant United States Attorney
501 I Street, Suite 10-100
Sacramento, CA 95814
Telephone: (916) 554-2700
Facsimile: (916) 554-2900

Attorneys for Plaintiff
United States of America

IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA

In the Matter of the Search of:

(1) Samsung Galaxy cell phone, model number: SM-G900V, IMEI: 990004943238596; (2) Apple iPhone 6S, FCC ID: BCG-E2946A, white in color
CURRENTLY LOCATED AT
SACRAMENTO FBI EVIDENCE CONTROL
ROOM

CASE NO.

AFFIDAVIT IN SUPPORT OF AN APPLICATION
UNDER RULE 41 FOR A WARRANT TO
SEARCH TWO DEVICES

1. I, Elizabeth Buckmiller, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B. I submit that there is probable cause to believe that the devices in question may contain evidence of violations of 18 U.S.C. § 1001 (providing materially false statements to federal agents in a matter involving international terrorism) and 18 U.S.C. § 2339A (attempting to provide or providing material support to terrorists).

3. I am an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510 (7), who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in 18 U.S.C. 2516. I am a Special Agent with the Federal Bureau of Investigation (“FBI”), and have been so employed since February 2013. I am currently assigned to the Sacramento Joint Terrorism Task Force at the Sacramento Field Division, and I am on the FBI’s Evidence Response Team. I have training in the preparation, presentation, and service of criminal complaints and arrest and search warrants. I have participated in numerous investigations into terrorism-related activities and am familiar with tactics, methods, tradecraft, and techniques of terrorists and their agents. I have received training regarding counterterrorism investigations, operations, and strategies, and have knowledge of various extremist groups, their ideologies, and their involvement in terrorist activity. I am involved in the investigation of offenses against the United States, including crimes of terrorism as set forth in Title 18, United States Code, Section 2331, *et seq.* I have training in digital evidence handling procedures and experience in the use of various digital tools to conduct investigations. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

II. IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched is: **(1) Samsung Galaxy cell phone, model number: SM-G900V, IMEI: 990004943238596; (2) Apple iPhone 6S, FCC ID: BCG-E2946A, white in color**, hereinafter the “Devices.” The Devices are currently located in the SACRAMENTO FBI EVIDENCE CONTROL ROOM.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

III. PROBABLE CAUSE

6. Aws Mohammed Younis Al-Jayab was arrested on January 7, 2016, pursuant to a

federal criminal complaint charging him with providing materially false statements to federal agents in a matter involving international terrorism, in violation of Title 18, United States Code, Section 1001 (EDCA Case No. 2:16-MJ-1-EFB). At the time of Al-Jayab's arrest, FBI agents also executed search warrants for Al-Jayab's vehicle (EDCA Case No. 2:16-SW-3), his parents' apartment (2:16-SW-4) and his own apartment (2:16-SW-5), which were authorized pursuant to an omnibus affidavit. The omnibus affidavit also included verbiage seeking authorization to search Al-Jayab's person. The court also authorized a search warrant for four Facebook accounts associated with Al-Jayab (2:16-SW-2). The affidavit presently before the Court incorporates by reference the four prior search warrants, which are identified by Case Numbers 2:16-SW-2, 2:16-SW-3, 2:16-SW-4, and 2:16-SW-5. The warrants for Al-Jayab's vehicle and the two residences authorized the seizure and search of any digital devices, including mobile phones.

7. In a search of Al-Jayab's person incident to arrest on January 7, 2016, FBI special agents recovered two mobile phones, "the Devices." The Devices are currently in the lawful possession of the Sacramento FBI. The government believes that it has authority under the previously-authorized omnibus affidavit, which included a request to search Al-Jayab's person, *inter alia*, for digital devices. However, out of an abundance of caution, the government seeks this additional search warrant authorizing a search of the Devices recovered from Al-Jayab incident to his arrest.¹

8. The prior affidavits incorporated herein by reference detailed a lengthy narrative in which Al-Jayab regularly communicated with persons about his desire to travel to Syria to fight with terrorists. Given the capabilities of digital devices including mobile phones, as specified in paragraph nine, below, it is reasonable to conclude that a search of the Devices may reveal evidence of violations of 18 U.S.C. §§1001 and 2339A.

¹ On or about February 8, 2016, an FBI special agent, trained as a computer analysis response team forensic examiner, bypassed the lock on the Samsung Galaxy cell phone, model number SM-G900V, and made a copy of the contents. This image was made in order to preserve the evidence. This image is now being kept in FBI evidence. Agents have neither reviewed nor searched the information contained on the image. If the Court authorizes the requested search warrant, the FBI will proceed with the search of both phones.

IV. TECHNICAL TERMS

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

- a) **Wireless telephone:** A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b) **Digital camera:** A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c) **Portable media player:** A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or

photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d) GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.
- e) PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving

them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.

- f) Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- g) 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.
- h) IP Address: An Internet Protocol address (or simply “IP address”) is a unique numeric address used by devices on the Internet. Every device attached to the Internet computer must be assigned an IP address so that Internet traffic sent to and from that device may be directed properly from its source to its destination.

10. Based on my training, experience, and research, I know that the Devices have capabilities that include allowing each device to serve as a mobile telephone, PDA, portable media player, and digital camera, provide GPS navigation, utilize mobile applications including social media and voice over internet protocol (VOIP) applications, and provide access to the Internet. Based on my knowledge, training, and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the devices.

V. ELECTRONIC STORAGE AND FORENSIC ANALYSIS

11. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the devices. This information can sometimes be recovered with forensics tools.

12. There is probable cause to believe that things that were once stored on the Devices may still be stored there, 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 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 mobile phone’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c) Wholly apart from user-generated files, storage media – in particular, mobile phones’ and computers’ internal hard drives – contain electronic evidence of how the device 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.”

13. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of each device’s use, who used each device, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices 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. 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 usernames 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 device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b) Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c) A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d) The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process.

Electronic 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.

- e) Further, in finding evidence of how a device 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.

14. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

15. Manner of execution. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

VI. CONCLUSION

16. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



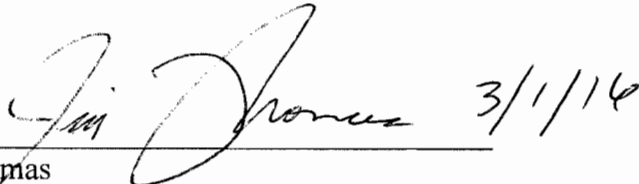
Elizabeth Buckmiller
Special Agent, FBI

SUBSCRIBED to and SWORN before me
this 1 day of March, 2016.



HONORABLE EDMUND F. BRENNAN
UNITED STATES MAGISTRATE JUDGE

Approved as to form:



Jill Thomas
Assistant United States Attorney

ATTACHMENT A

The property to be searched is **(1) Samsung Galaxy cell phone, model number: SM-G900V, IMEI: 990004943238596; (2) Apple iPhone 6S, FCC ID: BCG-E2946A, white in color**, hereinafter the “Devices.” The Devices are currently located in the SACRAMENTO FBI EVIDENCE CONTROL ROOM.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

ITEMS TO BE SEIZED

1. All records relating to violations of 18 U.S.C. § 2339A, those violations involving Aws Mohammed Younis Al-Jayab (“Al-Jayab”) and any accomplices, and all records relating to violations of 18 U.S.C. § 1001, involving Al-Jayab, and, namely:
 - a. Records, documents, programs, applications, and materials pertaining to use of, and/or ownership interest in, the **SUBJECT DEVICES** (as described more fully in Attachment A);
 - b. Records, documents, programs, applications, and materials pertaining to communications sent or received or accessed by Al-Jayab that relate to the provision of money, goods, personnel, or services to individuals outside the United States; terrorist or military-like activities; violent acts; individuals or groups who have committed or intend to commit violent acts or acts against non-Muslims or persons who do not comply with the interpretation of Islam advocated by Islamic extremists; and travel outside the United States; all of the above as they relate to the offenses described in this affidavit, 18 U.S.C. § 1001 and 2339A;
 - c. Records, documents, programs, applications, and materials tending to show Al-Jayab’s associates, including address books, telephone numbers, and contacts or friends lists; all of the above as they relate to the offense described in this affidavit, 18 U.S.C. § 1001 and 2339A;
 - d. Records, documents, programs, applications, and materials tending to show the activities of Al-Jayab, including journals, calendars, and diaries; all of the above as they relate to the offense described in this affidavit, 18 U.S.C. § 1001 and 2339A;

- e. Records, documents, programs, applications, and materials tending to show the financial activities of Al-Jayab; all of the above as they related to the offense described in this affidavit, 18 U.S.C. § 1001 and 2339A;
- f. Records, documents, programs, applications, and materials pertaining to travel, including information related to passports, travel receipts, tickets, reservations, and schedules; all of the above as they related to the offense described in this affidavit, 18 U.S.C. § 1001 and 2339A;
- g. Records, documents, programs, applications, and materials pertaining to Cyprus, Great Britain, Iraq, Israel, Jordan, Palestine, Syria, or Turkey;
- h. Records, documents, programs, applications, and materials pertaining to any designated foreign terrorist organization, terrorist group, or terrorist;
- i. Records, documents, programs, applications, and materials pertaining to Islamic extremism;
- j. Records, documents, programs, applications, and materials related to Islamic extremism or violent jihad;
- k. Records, documents, programs, applications, and materials pertaining to martyrdom or suicide;
- l. Evidence of who used, owned, or controlled the device 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, e-mail, e-mail contacts, chat and messaging logs, photographs, and correspondence;

- m. Evidence of the presence or absence of software that would allow others to control the device, 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;
 - n. Evidence of the attachment of other devices;
 - o. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;
 - p. Evidence of the times the device was used;
 - q. Passwords, encryption keys, and other access devices that may be necessary to access the device;
 - r. Applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;
 - s. Records of or information about Internet Protocol addresses used by the device; and,
 - t. Records of or information about the device'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.
2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include information created, modified, or stored in any form, including in digital form on any digital device.

3. Any and all names, words, telephone numbers, email addresses, time/date information, messages or other electronic data in the memory of the mobile telephone or on a server and associated with the mobile telephone and described as the mobile telephones':

- Incoming call history;
- Outgoing call history;
- Missed call history;
- Outgoing text messages;
- Incoming text messages;
- Draft text messages;
- Telephone book;
- Data screen or file identifying the telephone number associated with the mobile telephone searched;
- Data screen, file, or writing containing serial numbers or other information to identify the mobile telephone searched;
- Voicemail,
- User-entered messages (such as to-do lists); and
- Photographs.

Any passwords used to access the electronic data described above.

UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of
(1) Samsung Galaxy cell phone, model number:
SM-G900V, IMEI: 990004943238596; (2) Apple
iPhone 6S, FCC ID: BCG-E2946A, white in color,
CURRENTLY LOCATED AT SACRAMENTO FBI
EVIDENCE CONTROL ROOM

Case No.

2:16 - SW - 0123 EFB

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 California
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A, attached hereto and incorporated by reference.

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, attached hereto and incorporated by reference.

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: any authorized U.S. Magistrate Judge in the Eastern District of California.

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: 3-1-2016 at 2:50 p.m.

Judge's signature

City and state: Sacramento, California

Edmund F. Brennan, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2) (modified)

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

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

Subscribed, sworn to, and returned before me this date.

Signature of Judge

Date

ATTACHMENT A

The property to be searched is **(1) Samsung Galaxy cell phone, model number: SM-G900V, IMEI: 990004943238596; (2) Apple iPhone 6S, FCC ID: BCG-E2946A, white in color**, hereinafter the “Devices.” The Devices are currently located in the SACRAMENTO FBI EVIDENCE CONTROL ROOM.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

ITEMS TO BE SEIZED

1. All records relating to violations of 18 U.S.C. § 2339A, those violations involving Aws Mohammed Younis Al-Jayab (“Al-Jayab”) and any accomplices, and all records relating to violations of 18 U.S.C. § 1001, involving Al-Jayab, and, namely:

- a. Records, documents, programs, applications, and materials pertaining to use of, and/or ownership interest in, the **SUBJECT DEVICES** (as described more fully in Attachment A);
- b. Records, documents, programs, applications, and materials pertaining to communications sent or received or accessed by Al-Jayab that relate to the provision of money, goods, personnel, or services to individuals outside the United States; terrorist or military-like activities; violent acts; individuals or groups who have committed or intend to commit violent acts or acts against non-Muslims or persons who do not comply with the interpretation of Islam advocated by Islamic extremists; and travel outside the United States; all of the above as they relate to the offenses described in this affidavit, 18 U.S.C. § 1001 and 2339A;
- c. Records, documents, programs, applications, and materials tending to show Al-Jayab’s associates, including address books, telephone numbers, and contacts or friends lists; all of the above as they relate to the offense described in this affidavit, 18 U.S.C. § 1001 and 2339A;
- d. Records, documents, programs, applications, and materials tending to show the activities of Al-Jayab, including journals, calendars, and diaries; all of the above as they relate to the offense described in this affidavit, 18 U.S.C. § 1001 and 2339A;

- e. Records, documents, programs, applications, and materials tending to show the financial activities of Al-Jayab; all of the above as they related to the offense described in this affidavit, 18 U.S.C. § 1001 and 2339A;
- f. Records, documents, programs, applications, and materials pertaining to travel, including information related to passports, travel receipts, tickets, reservations, and schedules; all of the above as they related to the offense described in this affidavit, 18 U.S.C. § 1001 and 2339A;
- g. Records, documents, programs, applications, and materials pertaining to Cyprus, Great Britain, Iraq, Israel, Jordan, Palestine, Syria, or Turkey;
- h. Records, documents, programs, applications, and materials pertaining to any designated foreign terrorist organization, terrorist group, or terrorist;
- i. Records, documents, programs, applications, and materials pertaining to Islamic extremism;
- j. Records, documents, programs, applications, and materials related to Islamic extremism or violent jihad;
- k. Records, documents, programs, applications, and materials pertaining to martyrdom or suicide;
- l. Evidence of who used, owned, or controlled the device 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, e-mail, e-mail contacts, chat and messaging logs, photographs, and correspondence;

- m. Evidence of the presence or absence of software that would allow others to control the device, 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;
 - n. Evidence of the attachment of other devices;
 - o. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;
 - p. Evidence of the times the device was used;
 - q. Passwords, encryption keys, and other access devices that may be necessary to access the device;
 - r. Applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;
 - s. Records of or information about Internet Protocol addresses used by the device; and,
 - t. Records of or information about the device'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.
2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include information created, modified, or stored in any form, including in digital form on any digital device.

3. Any and all names, words, telephone numbers, email addresses, time/date information, messages or other electronic data in the memory of the mobile telephone or on a server and associated with the mobile telephone and described as the mobile telephones':

- Incoming call history;
- Outgoing call history;
- Missed call history;
- Outgoing text messages;
- Incoming text messages;
- Draft text messages;
- Telephone book;
- Data screen or file identifying the telephone number associated with the mobile telephone searched;
- Data screen, file, or writing containing serial numbers or other information to identify the mobile telephone searched;
- Voicemail,
- User-entered messages (such as to-do lists); and
- Photographs.

Any passwords used to access the electronic data described above.