

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

INFORMATION ASSOCIATED WITH FACEBOOK
USER ID 100004739910411 THAT IS STORED AT
PREMISES CONTROLLED BY FACEBOOK, INC.

Case No. 19-M-003 (DEJ)

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:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

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

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

The search is related to violations of: Title 18 U.S.C. § 2339B and Title 18 U.S.C. § 1028A

The application is based on these facts: See attached affidavit.

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



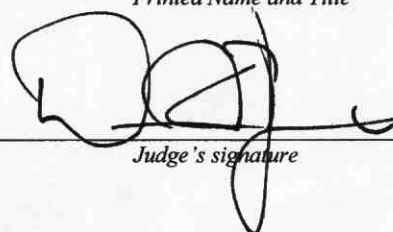
Applicant's signature

Special Agent Maria Miller, FBI

Printed Name and Title

Sworn to before me and signed in my presence:

Date: Jan. 7, 2019



Judge's signature

City and State: Milwaukee, Wisconsin

Honorable David Jones, U.S. Magistrate Judge

Printed Name and Title

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Maria Miller, being duly sworn, hereby depose and state the following:

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 information associated with Facebook user ID 100004739910411 that is stored at premises controlled by Facebook (referred to as the "ACCOUNT").
2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since June 2014. I am currently assigned to the Joint Terrorism Task Force at the Milwaukee Field Office, where I conduct a variety of investigations in the area of counterterrorism in the performance of my duties. I have investigated and assisted in the investigation of matters involving violations of federal law related to international terrorism, weapons of mass destruction, the distribution of bomb-making materials, and material support, including in the preparation and service of criminal complaints and search and arrest warrants. I have conferred with colleagues who have received specialized training from the FBI in investigating crimes related to explosives, biological weapons, and weapons of mass destruction.
3. The statements contained in this affidavit are based in part on my personal knowledge, as well as on information provided to me by other law enforcement officers and civilians. This affidavit is being submitted for the limited purpose of securing the requested search warrant, and I have not included each and every fact known to me concerning this investigation.

4. Based on facts set forth in this affidavit, I submit there is probable cause to believe that WAHEBA ISSA DAIS committed aggravated identity theft by hacking a Facebook account in order to provide material support to a Foreign Terrorist Organization (FTO) in violation of Title 18, United States Code, Section 1028A. DAIS is also known by an alias referred to here as "H.S.E." On June 12, 2018, DAIS was charged by a criminal complaint signed by a United States Magistrate Judge with attempting to provide material support or resources to ISIS, in violation of 18 U.S.C. § 2339B(a)(1). On June 26, 2018, DAIS was indicted by a Federal Grand Jury on two counts of violating 18 U.S.C. 2339B(a)(1). I submit there is also probable cause to search the Facebook ACCOUNT for evidence, fruits, and instrumentalities of the above mentioned crime.

STATUTORY AUTHORITY

5. This investigation concerns an alleged violation of 18 U.S.C. § 1028A, relating to aggravated identity theft. Elements of the offense are the following: the defendant knowingly transferred, possessed, or used another person's means of identification or identification documents; without lawful authority; and during and in relation to the eligible felony. In this case, the felony is the above mentioned violation of 18 U.S.C. § 2339B, with which DAIS has already been charged.

BACKGROUND OF INVESTIGATION AND FACTS ESTABLISHING

PROBABLE CAUSE

6. The FBI Joint Terrorism Task Force has been investigating WAHEBA ISSA DAIS (DAIS) as a suspect involved in the provision of material support to ISIS, in violation of 18 U.S.C. § 2339B. The investigation has revealed that DAIS, through the use of multiple social

media accounts that have been hacked and taken over from unwitting victims and private social media platforms, promotes ISIS ideology, recruits adherents to ISIS, advocates that her followers conduct attacks in the name of ISIS, collects information on how to make explosives and biological weapons and on how to conduct terrorist attacks, and distributes that information to individuals so they can conduct attacks on behalf of ISIS. For instance, DAIS used one of her pro-ISIS Facebook accounts (an account that was hacked and taken over from an unwitting victim) to direct an individual, whom she believed to be an ISIS supporter planning to conduct an attack in the name of ISIS, to her password-protected social media channel to find instructions on how to make Ricin and then suggested the individual introduce the Ricin to a government post or water reservoirs.

7. According to information provided by the Department of Homeland Security, DAIS was born on or about August 22, 1972, in Jerusalem, Israel, and was allowed to enter the United States without a passport arriving in Chicago, Illinois (via Paris, France), in approximately November 1992 because of her marriage to a U.S. Citizen (her husband filed for divorce in 2003). On DAIS's visa application, she indicated she intended to stay in the United States permanently as a housewife; that she was from Jerusalem; and that she could speak, read, and write in English and Arabic. DAIS is now a Lawful Permanent Resident of the United States and lived in Cudahy, Wisconsin, with five of her children, including three minors, prior to her arrest on June 13, 2018.

8. The FBI's investigation indicates that DAIS used multiple Facebook, Twitter, identified social media, and email accounts that contain pro-ISIS statements and information on how to make biological weapons, explosives, and explosive vests. DAIS was charged by criminal complaint signed by a United States Magistrate Judge on June 12, 2018, with providing material

support to ISIS in violation of Title 18, U.S.C. § 2339B. Specifically, the complaint alleged that DAIS promoted ISIS ideology, recruited adherents to ISIS, advocated that her followers conduct attacks in the name of ISIS, collected and shared information on how to make explosives and biological weapons and on how to conduct terrorist attacks, and distributed that information to individuals so they can conduct attacks on behalf of ISIS. The complaint further explained that DAIS used multiple hacked Facebook accounts to conduct this activity. DAIS was then indicted by a Federal Grand Jury on June 26, 2018, on two counts of Title 18, U.S.C. § 2339B.

DAIS'S HACKING OF VICTIM FACEBOOK ACCOUNTS

9. Open source searches and information provided by Facebook pursuant to 18 U.S.C. § 2702 indicate that DAIS and the individuals who were communicating with DAIS on Facebook were using hacked Facebook accounts as a way to avoid law enforcement detection of their communications. When DAIS took over a Facebook account, she changed the display name to a variant of "H.S.E." (written in English and/or Arabic) and changed the profile picture. The profile picture used by DAIS on these hacked Facebook accounts was taken by a professional photographer and is of a young girl wearing a blue dress. The photograph was taken as part of a series documenting Yazidi, a minority population in northern Iraq, fleeing their hometown to escape violence caused by the Islamic State militants. This photograph can be found on the internet. DAIS also typically changed the Facebook "friends" list, adding her own contacts and removing contacts that belonged to the hacking victim.

10. In her post-arrest, Mirandized interview on June 13, 2018, DAIS stated that she hacked Facebook accounts that were associated with Hotmail email addresses. After a Hotmail policy change, hacking became more difficult and DAIS began to receive hacked Facebook accounts

from other individuals. DAIS stated that she made a video describing how to hack Facebook accounts and posted it on social media.

11. DAIS also made statements online about her own hacking activities. For example, utilizing Facebook account with UID 100004693445122, DAIS stated on or about April 17, 2018, that it had been two months since she hacked the last account because she did not have time. At that point, she was getting her hacked accounts from other people.

12. One of the accounts used by DAIS was the Facebook account with UID 100004739910411. Subpoena returns indicate that Facebook UID 100004739910411 was created on November 17, 2012, with registration IP address 37.60.147.85. This IP address resolved to Palestine. An IP address for a log-in on December 6, 2017, also resolved to Palestine. The phone number associated with the account has country code 972 which is Israel.

13. Subpoena returns related to Facebook UID 100004739910411 revealed that, beginning around mid-December of 2017, some of the IP addresses for log-ins to this account resolved to Cudahy, WI, which is where DAIS resided at the time. Through subpoena returns, the FBI determined that many of the Facebook accounts taken over and used by DAIS were accessed using IP addresses resolving to Cudahy, WI.

14. For instance, Facebook UID 100003394781813 – which, as described in the complaint, was utilized by DAIS to post detailed instructions on how to make explosive vest bombs in support of ISIS – was also accessed using IP addresses that also resolved to Cudahy, WI. Additionally, Facebook UID 100003394781813 was forensically linked to several accounts by reviewing cookie data provided by Facebook pursuant to 18 U.S.C. § 2702. In particular, the FBI determined that Facebook UID 100004739910411 had been accessed from the same device that accessed Facebook UID 100003394781813.

15. The FBI has thus assessed that DAIS likely hacked the Facebook account with UID 100004739910411 in approximately mid-December 2017, from a victim residing in Palestine.

The email address associated with this account is XXX@hotmail.com, which is consistent with DAIS'S post-arrest statement that she hacked accounts with Hotmail email address.

16. The account was closed on December 26, 2017. The requested search is from November 1, 2017, to December 26, 2017, to cover the time period shortly before the hacking occurred and until the account was closed.

17. Based on the information detailed below and on the results of the FBI's investigation into DAIS'S material support activities, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2339B and 18 U.S.C. §1028A will be found in the subject ACCOUNT.

INFORMATION ABOUT FACEBOOK

18. 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.

19. 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.

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

21. 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.

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

“Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

23. Facebook has a Photos application, where users can upload an unlimited number of albums and photos. Another feature of the Photos application is 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 associated with a user’s account will include all photos uploaded by that user that have not been deleted, as well as all photos uploaded by any user that have that user tagged in them.

24. 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.

25. 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.

26. 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.

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

28. 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.

29. 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.

30. 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.

31. 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.

32. 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.

33. 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.

34. 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.

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

36. 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.

37. 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.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

38. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

39. Based on the forgoing, I request that the Court issue the proposed search warrant.

40. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) &

(c)(1)(A). Specifically, the Eastern District of Wisconsin has jurisdiction over the offense being investigated: 18 U.S.C. § 1028A.

41. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

ATTACHMENT A

This warrant applies to Facebook UID 100004739910411, stored at premises owned, maintained, controlled, or operated by Facebook, a company headquartered in Menlo Park, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Facebook, Inc.:

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

a. All contact and personal identifying information, including: full name, name changes (including past names and dates of name changes), user identification number, birth date, gender, contact e-mail addresses, e-mail address changes (including past e-mail addresses and dates of e-mail changes), Facebook passwords, Facebook password changes (including past passwords and dates of password changes), Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, telephone number changes (including past telephone numbers and dates of telephone number changes), screen names, screen name changes (including past screen names and dates of screen name changes), websites, education, work, hometown, and other personal identifiers (including previous and current);

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

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

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

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

f. All "check ins" and other location information;

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

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

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

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

k. All records of Facebook searches performed by the account;

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

m. The length of service (including start date), the types of service utilized by the user, and the means and source of any payments associated with the service (including any credit card or bank account number);

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

o. All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken and also including any identity verification documents sent to Facebook; and

p. Any and all of the above requested records that were deleted by any user or Facebook but are still maintained by Facebook, including the dates of the changes.

Date Range for Search of User ID:

Facebook User ID	Date Range of Search
100004739910411	November 1, 2017, to December 26, 2017

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 1028A and 18 U.S.C. §2339B involving DAIS, including, for the User ID identified on Attachment A, information pertaining to the following matters:

a. Terrorism or a threat to the national security of the United States;

- b. Loyalties to a foreign power;
- c. Weapons, ammunition, tactical equipment, tactical or camouflage clothing, explosives, explosives devices, explosive precursor chemicals, incendiaries, incendiary devices, incendiary chemicals or precursor chemicals and any other hazardous devices or substances deemed relevant to the investigation;
- d. Flags, banners, patches, specifically designed clothing that depicts the symbol of a terrorist groups or terrorist movements;
- e. Forms of identification, journals, and diaries;
- f. Indicia of travel overseas and domestically, including airline tickets, passports, visas, hotel records, and travel itineraries;
- g. Calendars, time schedules, address books, and contact list information;
- h. Financial information to include all financial institution records and account information;
- i. Cellular telephones, smart telephones, computers, electronic data storage devices or media, associated electronic accessories;
- j. Any passwords, personal identification numbers (PINs), or other information necessary to encrypt or decrypt information;
- k. Evidence of geographical location of the user of the identified account at times relevant to the investigation; Global Positioning System (GPS) information and mapping history from any account;
- l. Persons associated with ISIS or involved in terrorist or military-like activities or violent acts overseas or in the United States, including their identities and location and contact information;

- m. Organizations whose purpose, primary or ancillary, is raising, collecting, organizing, distributing, or facilitating funds, goods, personnel, or services for training and fighting overseas or in the United States and *not* in conjunction with the U.S. armed forces;
- n. Hacking or the unauthorized use of any computer or email or social media account;
- o. Evidence indicating how and when the Facebook account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Facebook account owner;
- p. Evidence indicating the Facebook account owner's state of mind as it relates to the crime under investigation;
- q. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s); and
- r. The identity of the person(s) who communicated with the user ID about matters relating to providing material support to terrorist organizations, including records that help reveal their whereabouts.