# UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with email account practical_75@hotmail.com that is stored at premises controlled by Microsoft Corporation.

Case No. 18-M-123 (DEJ)

## 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 Wisconsin:

See 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:

See Attachment B

**YOU ARE COMMANDED** to execute this warrant ON OR BEFORE Aug. 23, 2018 *(not to exceed 14 days)*
☑ in the daytime between 6:00 a.m. and 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 Hon. David E. Jones.
*(United States Magistrate Judge)*

☐ 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: Aug. 9, 2018 11:30 am

*Judge's signature*

City and State: Milwaukee, Wisconsin Hon. David E. Jones, U.S. Magistrate Judge
*Printed Name and Title*

AO 93 (mod. 5/14) Search and Seizure Warrant

**Return**

| Case No: | Date and time warrant executed: | Copy of warrant and inventory left with: |
|---|---|---|
| 18-M-123 (DEJ) | 11/01/2018 ~~10/04/2018~~ 1000am | Microsoft |

Inventory made in the presence of:

SA Scott Manloch

Inventory of the property taken and/or name of any person(s) seized:

Various digital files associated with email.

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the undersigned judge.

Date: 11/1/2018

*Executing officer's signature*

Scott Manloch / Special Agent

*Printed name and title*

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

Date: Nov. 1, 2018

*United States Magistrate Judge*

## ATTACHMENT A

### Property to Be Searched

This warrant applies to information associated with email account practical_75@hotmail.com that is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, an email provider headquartered at 1065 La Avenida, Building 4, Mountain View, California (CA) 94043.

## ATTACHMENT B

### Particular Things to be Seized

**I. Information to be disclosed by Microsoft Corporation (the "Provider")**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider. The Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within ten days of service of this warrant.

## 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. § 2339(b) involving DAIS since March 1, 2017, including, for the account identified on Attachment A, information pertaining to the following matters:

a. Any information in any form that is related to terrorism or a threat the national security of the United States;

b. Evidence of 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. Travel documents and 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, checks, credit or debit cards, automated teller machine cards, public benefit program cards, account information, other financial records, financial instruments and moneys;

i. Money orders, wire transfers, cashier's check receipts, bank statements, passbooks, checkbooks, and check registers pertaining to travel overseas, the Islamic State of Iraq and al-Sham (ISIS), terrorist or military-like activities, or violent acts;

j. Cellular telephones, smart telephones, computers, electronic data storage devices or media, associated electronic accessories;

k. Any information that could be determined to passwords, personal identification numbers (PINs), or other information necessary to encrypt or decrypt information;

l. 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;

m. Secure storage facilities for financial instruments, passports, visas, and identification documents, including safe deposit boxes;

n. 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;

o. 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;

p. Instructions, in any form, relating to explosives, biological weapons, terrorist attacks, or the hacking and other unauthorized use of computers and email and social media accounts; and

q. Hacking or the unauthorized use of any computer or email or social media account.

r. Evidence indicating how and when the 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 account owner;

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

t. 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

u. The identity of the person(s) who communicated with the account about matters relating to providing material support to terrorist organizations, including records that help reveal their whereabouts.