

UNITED STATES DISTRICT COURT

for the
District of Columbia

In the Matter of the Search of

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

Computer Servers and Records of Microsoft Corporation
for Information Associated with the E-Mail Account,

Case: 1:13-mj-00278

Assigned To : Magistrate Judge Deborah A. Robinson

Assign. Date : 4/15/2013

Description: Search and Seizure Warrant

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):
computer servers and records of Microsoft Corporation, located at One Microsoft Way, Redmond, Washington for information associated with the e-mail account [REDACTED]

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

certain property, the disclosure of which is governed by Title 18, U.S.C. Sections 2701 through 2711, namely contents of electronic e-mails and other electronic data more fully described in ATTACHMENT B to this application.

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

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

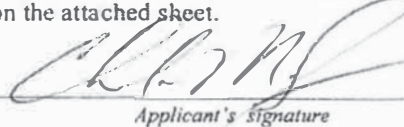
The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 793(d)	Unauthorized disclosure of classified information
18 U.S.C. 793(g)	Conspiracy to commit Unauthorized disclosure of classified information

The application is based on these facts:

See attached affidavit incorporated by reference as if fully restated herein.

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

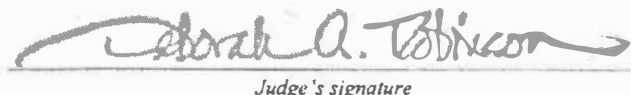

Applicant's signature

Special Agent Christina M. Sun
Printed name and title

Sworn to before me and signed in my presence.

Date: 04/15/2013

City and state: Washington, D.C.


Judge's signature

U.S. Magistrate Judge Deborah A. Robinson
Printed name and title

AFFIDAVIT IN SUPPORT SEARCH WARRANT

I, Christina M. Sun, being first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of an application for a search warrant for information associated with a certain email account that is stored at premises controlled by Microsoft Corporation, an e-mail provider headquartered at One Microsoft Way, Redmond, WA 98052-6399. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft Corporation to disclose to the government copies of the information (including the content of communications) further 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.

2. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") since May 2006. I am currently assigned to the Counterintelligence Division of the FBI's Washington Field Office, where I investigate offenses involving espionage, illegal agents of foreign powers, and unauthorized retention and disclosure of classified information. Before joining the FBI, I was a Manager at BearingPoint, Inc., an international information technology consulting firm from June 2000 through May 2006. At BearingPoint, Inc., I managed various technology infrastructure and operations projects and programs. Throughout my career, I have interviewed many witnesses, collected many types of evidence, and prepared numerous search warrants for both physical and electronic media. Accordingly, I have considerable experience in complex criminal investigations.

3. As a federal agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States. The statements in this affidavit are based in part on information developed in the course of this investigation to date and on my experience and background as a Special Agent of the FBI. The information set forth in this affidavit concerning this investigation is known to me as a result of my own involvement in this investigation or has been provided to me by other law enforcement professionals. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. In addition, where conversations or statements are related herein, they are related in substance and in part except where otherwise indicated.

IDENTIFICATION OF PROPERTY TO BE SEARCHED

4. The property to be searched is subscriber information, transactional records and the content of the email account identified as [REDACTED] maintained on computer systems in the possession, custody, or control of Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399, hereinafter referred to as the SUBJECT ACCOUNT.

STATUTORY AUTHORITY

5. For the reasons set forth below, I believe there is probable cause to conclude that the subscriber information, records and contents of the SUBJECT ACCOUNT contain evidence, fruits, and/or instrumentalities of criminal violations of 18 U.S.C. § 793(d) (Unauthorized Disclosure of National Defense Information) and/or 18 U.S.C. § 793(g) (Conspiracy to Disclose National Defense Information).

6. Based on my training and experience, and discussions with the federal prosecutors assigned to this investigation, I have learned that Title 18, United States Code, Section 793(d)

makes punishable, by up to ten years imprisonment, the willful communication, delivery, or transmission of documents and information related to the national defense to someone not entitled to receive them by one with lawful access or possession of the same. Specifically, Section 793(d) states:

(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years or both.

18 U.S.C. § 793(d). Further, Section 793(g) makes a conspiracy to violate Section 793(d) also a violation of Section 793 and punishable by up to ten years imprisonment. See 18 U.S.C. § 793(g).

7. Based on my training and experience, and discussion with the federal prosecutors assigned to this investigation, I have learned that "classified" information is defined by Executive Order 13526 (Executive Order), as information in any form that: (1) is owned by, produced by or for, or under control of the United States government; (2) falls within one or more of the categories set forth in the Executive Order; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security which includes defense against transnational terrorism. Where such unauthorized disclosure reasonably could be expected to cause "exceptionally grave damage" to the national security, the information is classified as "TOP SECRET."

8. 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 Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

9. This investigation concerns the unauthorized disclosure of classified information connected with a disrupted suicide bomb attack on a U.S.-bound airliner by the Yemen-based terrorist organization Al-Qaeda in the Arabian Peninsula (AQAP) and the recovery by the United States of a bomb in connection with that plot in April 2012 (referred to hereinafter as “the bomb”). Beginning on May 7, 2012, multiple news organizations published articles about the disrupted suicide bomb attack and recovery of the bomb. The lead article was published by the [REDACTED] reporters [REDACTED] on May 7, 2012. It was entitled, “US: CIA Thwarts New al-Qaida Underwear Bomb Plot.” Thereafter [REDACTED] and other media outlets published additional articles and/or broadcast television reports about the disrupted suicide bomb attack and recovery of the bomb (referred to collectively hereinafter as the “Media Reports”).

10. During its investigation, the FBI has learned from Intelligence Community representatives and/or the FBI’s own review of classified documents that the Media Reports contained, in part, information classified up to the TOP SECRET level.

11. Based on my training and experience, I have learned that classified information, of any designation, may be shared only with persons determined by an appropriate United States government official to be eligible for access to such classified information, that is, the individual has received a security clearance, has signed an approved non-disclosure agreement, and

possesses a "need to know" the information in question. If a person is not eligible to receive classified information, classified information may not be disclosed to that person.

12. The FBI's investigation has revealed that the first article about the disrupted suicide bomb attack and recovery of the bomb was published by [REDACTED] at approximately 4:07 p.m. on May 7, 2012. One of the [REDACTED] reporters who wrote that article was [REDACTED]. A search of government databases has revealed that [REDACTED] does not possess, and has never possessed, a security clearance.

13. In connection with the disrupted suicide bomb attack, in late April 2012 the bomb was sent to the FBI Laboratory, in Quantico, Virginia (hereinafter referred to as the "FBI Lab"), for forensic examination by FBI bomb technicians and other forensic examiners and scientists. The FBI's investigation has identified Donald John Sachtleben (SACHTLEBEN) as an FBI consultant who was present at the FBI Lab from May 2, 2012 through May 4, 2012. Review of FBI records has revealed that SACHTLEBEN was born in 1958. SACHTLEBEN became an FBI Special Agent beginning in 1983. In 1990, SACHTLEBEN became an FBI Special Agent Bomb Technician. In that capacity, SACHTLEBEN was certified as an expert in the areas of explosives and hazardous devices. In 1996, SACHTLEBEN became a Supervisory Special Agent and Forensics Examiner in the FBI Explosives Unit located at the FBI Lab. In 2004, SACHTLEBEN became a coordinating forensic examiner for all evidence submitted to the FBI Lab in the aftermath of the 9/11 attacks. In 2007, SACHTLEBEN transferred to the FBI Indianapolis Field Office, where he worked as a bomb technician coordinator for the FBI for Indiana. In September 2008, SACHTLEBEN retired from the FBI.

14. Thereafter, SACHTLEBEN formed Raptor Consulting, LLC, a consulting company providing training and security consulting services to government agencies and private

sector businesses. In 2009, SACHTLEBEN, through Raptor Consulting, LLC, entered into a government contract to provide bomb technician consulting services to the FBI. As of April 2012, SACHTLEBEN was also employed as a Visiting Assistant Professor at Oklahoma State University's (OSU) School of Forensic Sciences. In that capacity, SACHTLEBEN was employed as the Director of Training for Oklahoma State University's Center for Improvised Explosives Research and Training. In April 2012, SACHTLEBEN was a resident of Carmel, Indiana.

15. FBI records reveal that, in April and May 2012, SACHTLEBEN possessed a TOP SECRET security clearance. Over his career at the FBI, SACHTLEBEN signed no less than three Classified Information Nondisclosure Agreements and no less than three Sensitive Compartmented Information Nondisclosure Agreements (together, NDAs) with the United States government. NDAs are legally binding agreements between an individual being granted, or already in possession of, a security clearance, and the United States government, wherein the parties agree that the individual shall never disclose classified information without the authorization of the United States government. The standard form NDA notifies the individual entering into the agreement with the United States government that the unauthorized disclosure of classified information can lead to criminal prosecution, to include a violation of 18 U.S.C. § 793.

16. The FBI's investigation has revealed that SACHTLEBEN traveled from Indianapolis, Indiana, to Tulsa, Oklahoma, on April 18, 2012, to conduct a training of law enforcement officers in his capacity as the Director of Training of OSU's Center for Improvised Explosive Research and Training. The training was conducted between April 24, 2012, and April 27, 2012 at OSU. SACHTLEBEN was joined at the training by at least one of his

colleagues from the FBI Lab who assisted him in the training. On April 26, 2012, while that FBI Lab employee was still in Tulsa with SACHTLEBEN, the FBI Lab employee received an email from his supervisor at the FBI Lab. That email stated that the FBI Lab would imminently be working on a classified, "close hold" case. That FBI Lab employee has denied providing SACHTLEBEN with any information concerning the bomb.

17. The bomb arrived at the FBI Lab for forensic analysis at approximately 9:45 a.m. on April 30, 2012.

18. Two hours later, at approximately 11:33 a.m., the FBI Lab employee who was with SACHTLEBEN at the training in Tulsa, Oklahoma, sent an email to SACHTLEBEN's FBI email account that stated that the FBI Lab's Explosives Unit was "involved in a 24/7 rush case right now for which I am the chemist so my time is limited at the moment."

19. Examination of telephone toll records for a cellular telephone number associated with [REDACTED] reporter [REDACTED] revealed that two hours later, at approximately 1:32 p.m. on April 30, 2012, a call was made from a cellular telephone number for which SACHTLEBEN was the subscriber to a cellular telephone number for which [REDACTED] was the subscriber. That call lasted approximately two minutes and eighteen seconds.

20. At 6:30 p.m. that evening, ABC World News Tonight broadcast a news story which stated, in part, that for the past year U.S. and European officials had warned that AQAP's master bomb-maker, Ibrahim al-Asiri, had been designing surgically implanted body bombs to

¹ As part of the FBI's investigation, authorization was obtained pursuant to 28 C.F.R. § 50.10(d) to issue subpoenas for the telephone toll records for certain media personnel, including for [REDACTED]. Subscriber records confirmed that [REDACTED] was the subscriber for the cellular phone number that had contact with SACHTLEBEN's cellular phone number.

get past airport security, and that there was concern that AQAP may soon try to explode a U.S.-bound aircraft with an explosive hidden inside the bodies of terrorists.

21. Later that evening, beginning at approximately 7:13 p.m., four text messages were exchanged between [REDACTED] cellular phone and SACHTLEBEN's cellular phone. These texts were as follows:

Date	Time	Originating Cellular Phone	Terminating Cellular Phone	Content of Text Message
4/30/2012	7:13 p.m.	[REDACTED]	SACHTLEBEN	Al-Asiri is up to his old tricks. I wonder if ur boys got a hold of a cavity bomb
4/30/2012	7:14 p.m.	[REDACTED]	SACHTLEBEN	:)
4/30/2012	7:15 p.m.	SACHTLEBEN	[REDACTED]	Yikes. Remind me to bring sum purell to the lab
4/30/2012	7:15 p.m.	[REDACTED]	SACHTLEBEN	Not totally sure though

22. Beginning at approximately 9:50 a.m. the following day (May 1, 2012), two more text messages were exchanged between SACHTLEBEN's cellular phone and [REDACTED] cellular phone. These text messages were as follows:

Date	Time	Originating Cellular Phone	Terminating Cellular Phone	Content of Text Message
5/1/2012	9:50 a.m.	SACHTLEBEN	[REDACTED]	Hmm. . . Methinks the 10am news conf may b related
5/1/2012	9:50 a.m.	[REDACTED]	SACHTLEBEN	Ah!

23. At approximately 10:00 a.m. on May 1, 2012, the FBI held a news conference concerning the arrest of five men in Cleveland, Ohio, who were charged with plotting a bomb attack on a bridge in Ohio.

24. Thereafter, SACHTLEBEN's cellular phone sent two text messages to [REDACTED]

[REDACTED] cellular phone. Those texts were as follows:

Date	Time	Originating Cellular Phone	Terminating Cellular Phone	Content of Text Message
5/1/2012	10:04 a.m.	SACHTLEBEN	[REDACTED]	Just abt to take off. ² Will b curious to c coverage when I land at dulles. Hope that tsa doesn't get out the rubber gloves and ky
5/1/2012	12:49 p.m.	SACHTLEBEN	[REDACTED]	Got that one wrong. A lil surprised they r wrkin 24 hr shifts cuz of those mutts. Still mght b sumthin else brewin. Will find out tomorrow

25. FBI computer log-on records reveal that beginning at approximately 9:05 a.m. the next morning (May 2, 2012), SACHTLEBEN's unique electronic computer profile logged into the FBI's classified computer system from a computer terminal located within the FBI Lab in a room directly adjacent to the suite of rooms where the bomb was being examined. SACHTLEBEN's computer profile logged off of the FBI Lab's computer terminal at approximately 10:16 a.m. on May 2, 2012.

26. At approximately 10:25 a.m., SACHTLEBEN's cellular phone placed a two minute and seven second call to [REDACTED]'s cellular phone.

27. Approximately two-and-a-half hours later, [REDACTED] and another [REDACTED] reporter called or sent text messages to multiple United States government officials and stated that [REDACTED] knew the following facts: (1) the United States had intercepted a bomb from Yemen; (2) the FBI was analyzing the bomb; and (3) [REDACTED] believed, but had not confirmed, that the bomb was linked to AQAP's premier bomb-maker, Ibrahim Al-Asiri. During its investigation, the FBI has learned from Intelligence Community representatives and/or the FBI's own review of classified

² The FBI's investigation has revealed that on May 1, 2012, SACHTLEBEN flew from Indianapolis, Indiana, to Dulles International Airport located in Chantilly, Virginia.

documents that the facts the [REDACTED] reporters stated they knew as of May 2, 2012 (namely, (1) and (2) in the immediately preceding sentence) constituted classified information as of that date.

28. Additionally, the FBI's investigation has revealed that United States government officials engaged in an effort to stop or delay publication of the [REDACTED] story concerning the recovery of the bomb. [REDACTED] published its first story concerning the disrupted suicide bomb attack and recovery of the bomb on May 7, 2012.

29. The FBI's investigation has revealed that between May 8, 2012, and May 10, 2012, SACHTLEBEN was in Kansas City, Missouri, conducting a training of law enforcement officers for the FBI's National Improvised Explosive Familiarization program (NIEF). At least two FBI Lab employees who had worked, or were working, on the examination of the bomb were in Kansas City with SACHTLEBEN assisting him with the NIEF training. Both employees have denied providing SACHTLEBEN with any information concerning the bomb.

30. At approximately 2:16 a.m. on May 9, 2012 [REDACTED] published another story concerning the disrupted suicide bomb attack. That story asserted that the bomber in the disrupted suicide bomb plot was working for "Saudi intelligence."

31. Beginning at approximately 7:32 a.m. on the morning of May 9, 2012, five more text messages were exchanged between SACHTLEBEN's cellular phone and [REDACTED] cellular phone. These text messages were as follows:

Date	Time	Originating Cellular Phone	Terminating Cellular Phone	Content of Text Message
5/9/2012	7:32 a.m.	SACHTLEBEN	[REDACTED]	[REDACTED] is pissed this morning after reading ur piece. Guess u got it right.

³ The FBI's investigation has revealed that [REDACTED] was a FBI colleague of SACHTLEBEN who was assigned to the bomb examination team at the FBI Lab. FBI records show that [REDACTED] was in Kansas City, Missouri, assisting SACHTLEBEN in the NIEF training between May 8, 2012, and May 10, 2012.

5/9/2012	7:35 a.m.	[REDACTED]	SACHTLEBEN	Interesting. This whole tale is still very murky. That's for sure. But we were told this device cud be replicated very easily. It was not hard to build.
5/9/2012	8:10 a.m.	SACHTLEBEN	[REDACTED]	They r workin on that notion right now.
5/9/2012	8:35 a.m.	[REDACTED]	SACHTLEBEN	That the device is easy to build?
5/9/2012	9:02 a.m.	SACHTLEBEN	[REDACTED]	They r makin one just to see how they did it. Not sure we r sayin it is easy. Plus we r not mkin it in a mud hut.

32. Thereafter, on May 9, 2012, [REDACTED] published another story concerning the disrupted suicide attack. That story stated that the "FBI is attempting to replicate bomb [sic], trying to determine how destructive the bomb would have been and how easy it would be for AQAP to build another."

33. The FBI's investigation has developed no evidence that SACHTLEBEN was authorized, directly or indirectly, by the United States government to deliver, communicate, or transmit any classified information to [REDACTED] or any other member of the media.

34. To date, apart from SACHTLEBEN, the FBI's investigation has not identified any other individual who worked at the FBI Lab in April and May 2012 who communicated with [REDACTED] during that time period.

35. At this time, the investigation has not revealed any information that SACHTLEBEN was assigned to the examination team responsible for analyzing the bomb upon its arrival at the FBI Lab. FBI email records reveal, however, that SACHTLEBEN sent and/or received communications from multiple individuals at the FBI Lab who were either assigned to

the bomb examination team or who were aware of the FBI Lab's forensic analysis of the bomb, including between April 30, 2012, and May 2, 2012.

36. To date, FBI telephone records reveal that, between April 30, 2012, and May 2, 2012, there were at least seven telephone calls and thirteen text messages exchanged between SACHTLEBEN's cellular telephone and telephone numbers associated with FBI Lab personnel who were either assigned to the bomb examination team or who were aware of the FBI's forensic analysis of the bomb. Other text messages sent from SACHTLEBEN's cellular phone indicate SACHTLEBEN's location in relationship to the FBI Lab in Quantico, Virginia.

37. During the course of its investigation, the FBI learned about two Chase Bank credit cards that were associated with SACHTLEBEN. On March 7, 2013, the United States obtained from Chase Bank customer records for one of those cards indicating that SACHTLEBEN was the primary applicant for the credit card, and that the email address [REDACTED] was associated with the account.

38. On April 4, 2012, the United States obtained subscriber information from Microsoft Corporation for the SUBJECT ACCOUNT. Those subscriber records listed the name Donald Sachtleben in the "User Info" field for the account, and the name [REDACTED] in the "Subscriber Information" field for the account. The investigation has revealed that [REDACTED] is SACHTLEBEN'S wife.

39. On or about March 14, 2013, the United States submitted an application under seal pursuant to 18 U.S.C. § 2703(d), for an Order to Microsoft Corporation to disclose non-content header and footer information for the SUBJECT ACCOUNT. On or about March 14, 2013, United States District Court Magistrate Judge Deborah A. Robinson signed an Order directing Microsoft Corporation to disclose non-content information for the SUBJECT

ACCOUNT within 10 days of the date of the Order. On or about April 4, 2013, Microsoft Corporation delivered the requested records to the FBI (hereinafter "MSN Records"). Review of the MSN Records revealed that approximately 12 emails were sent from the SUBJECT ACCOUNT to the email account [REDACTED] in 2012. Specifically, emails were sent from the SUBJECT ACCOUNT to the email account [REDACTED] once on January 6, 2012, twice on February 16, 2012, once on April 10, 2012, once on April 12, 2012, once on April 13, 2012, once on April 17, 2012, once on April 20, 2012, and three times on April 29, 2012. The following day, April 30, 2012, a phone call and multiple text messages were exchanged between SACHTLEBEN's cellular phone and [REDACTED] cellular phone. See supra ¶¶ 17-19.

40. Further review of the MSN Records indicated that on May 11, 2012, at least one email was sent from the SUBJECT ACCOUNT to FBI email accounts used by FBI Lab personnel who were either assigned to the bomb examination team or who were aware of the FBI's forensic analysis of the bomb.

41. Additionally, review of the MSN Records indicated that the SUBJECT ACCOUNT may contain evidence of SACHTLEBEN's travels and whereabouts during the relevant time period. The MSN Records revealed approximately 18 emails that were exchanged between the SUBJECT ACCOUNT and various hotels, airports, airlines, and car rental companies between April 18, 2012, and May 9, 2012.

42. Based on my training and experience, I believe that the information requested in Attachment B for the SUBJECT ACCOUNT will provide information relevant to the investigation of the unauthorized disclosure at issue, including the content of email and other records related to the SUBJECT ACCOUNT that will establish further links between SACHTLEBEN and [REDACTED] or between SACHTLEBEN and FBI Lab

personnel who were either assigned to the bomb examination team or who were aware of the FBI's forensic analysis of the bomb. Further, the content of those emails and records related to the SUBJECT ACCOUNT may assist the FBI in establishing SACHTLEBEN's location during the relevant time frame, his knowledge of the FBI Lab's analysis of the bomb, his understanding of the sensitivity of that information, and his communications with members of the media.

THE INTERNET, EMAIL, AND EMAIL SERVERS

43. I have received training from the FBI related to computer systems and the use of computers during criminal investigations. Based on my education, training and experience, and information provided to me by other law enforcement agents, I know the following:

- a. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. The term "computer", as used herein, is defined in 18 U.S.C. § 1030(e)(1) and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. A computer user accesses the Internet through a computer network or an Internet Service Provider (ISP).
- b. Email, or electronic mail, is a popular method of sending messages and files between computer users. When a computer user sends an email, it is created on the sender's computer, transmitted to the mail server of the sender's email service providers, then transmitted to the mail server of the recipient's email service provider, and eventually transmitted to the recipient's computer. A server is a computer attached to a dedicated network that serves many users. Copies of emails are usually maintained on the recipient's email server, and in some cases are maintained on the sender's email server.
- c. A server is a computer on a network that manages network resources. Authorized users on the network can store files on the server.
- d. A mail or email server is a computer on a network that works as a virtual post office, i.e., it stores and moves email over the network and into the Internet. When a computer user sends an email, it is created on the sender's computer, transmitted to the email server of the sender's email service providers, then transmitted to the email server of the recipient's

email service provider, and eventually transmitted to the recipient's computer. An email server usually consists of a storage area where email is stored for local users, a set of definable rules which determine how the mail server should react to the destination of a specific message, a database of user accounts that the mail server recognizes and will deal with (or "serve") locally, and communications modules which are the components that actually handle the transfer of the email message to and from other mail servers and email users.

- e. A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, DVDs, flash memory, CD-ROMs, servers and several other types of magnetic or optical media not listed here.
- f. The term "computer systems," as used herein, means any computer, computer server, or storage medium for computer data.

BACKGROUND CONCERNING E-MAIL

44. In my training and experience, I have learned that Microsoft Corporation provides a variety of on-line services, including electronic mail ("e-mail") access, to the public. Microsoft Corporation allows subscribers to obtain e-mail accounts at the domain name msn.com, like the e-mail account listed in Attachment A. In general, an e-mail that is sent to a Microsoft Corporation subscriber is stored in the subscriber's "mail box" on Microsoft Corporation's servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Microsoft Corporation's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Microsoft Corporation's servers for a certain period of time.

45. Subscribers obtain an account by registering with Microsoft Corporation. During the registration process, Microsoft Corporation asks subscribers to provide basic personal information. Therefore, the computers of Microsoft Corporation are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Microsoft Corporation subscribers) and information concerning subscribers and their use of Microsoft Corporation

services, such as account access information, e-mail transaction information, and account application information. 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.

46. A Microsoft Corporation subscriber can also store with the provider 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 Microsoft Corporation. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

47. 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 number). 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.

48. 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 Internet Protocol address ("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.

49. 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.

CONCLUSION

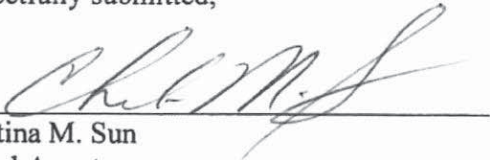
50. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the information, records and content of the SUBJECT ACCOUNT described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

51. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation. Premature disclosure of the contents of this affidavit and

related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,


Christina M. Sun
Special Agent
Federal Bureau of Investigation

APR 15 2013

Subscribed and sworn to before me on April __, 2013:


UNITED STATES MAGISTRATE JUDGE

**DEBORAH A. ROBINSON
U.S. MAGISTRATE JUDGE**

ATTACHMENT A

This warrant applies to information, records and content associated with the following email account:



that is stored at premises or on servers owned, maintained, controlled, or operated by Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399.

ATTACHMENT B
SPECIFIC ITEMS 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, 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 e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- 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 e-mail 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 at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- 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.

II . Information to be seized by the government

All information described above in Section I that constitutes evidence, fruits, and/or instrumentalities of criminal violations of 18 U.S.C. § 793(d) (Unauthorized Disclosure of National Defense Information), and/or 18 U.S.C. § 793(g) (Conspiracy to Disclose National Defense Information), including:

- a. records or information relating to the disclosure or potential disclosure of United States classified, intelligence, or national defense information;
 - b. classified documents, images, records, or information, and any communications relating to any such document, image, record, or information;
 - c. records or information relating to the national defense, including but not limited to documents, maps, plans, diagrams, guides, manuals, and other Department of Defense, United States military, and/or weapons material, sources or methods of intelligence gathering, and foreign intelligence;
 - d. records or information relating to Donald Sachtleben's ("SACHTLEBEN's") whereabouts, schedule, travel, or activities from April 1, 2012, through May 31, 2012;
 - e. all communications to or from SACHTLEBEN from April 1, 2012, through May 31, 2012;
 - f. all communications between, and/or among, SACHTLEBEN and any member of the media, including but not limited to,
-

- g. all communications between SACHTLEBEN and any Federal Bureau of Investigation (FBI) personnel, including but not limited to employees, contractors, subcontractors or any other individuals associated with the FBI;
- h. records or information relating to the disrupted suicide bomb attack on a U.S.-bound airliner by the Yemen-based terrorist organization Al-Qaeda in the Arabian Peninsula (AQAP) and the recovery by the United States of a bomb in connection with that plot in April 2012;
- i. any records or information provided by SACHTLEBEN to any member of the media;
- j. the source(s) or potential source(s) of any records or information provided by SACHTLEBEN to any member of the media;
- k. records or information relating to the state of mind of SACHTLEBEN;
- l. records or information relating to the state of mind of any individuals concerning the communication, disclosure, receipt, or retention of classified, intelligence, or national defense information;
- m. records or information relating to knowledge of laws, rules, regulations and/or procedures prohibiting the unauthorized disclosure of classified, intelligence, or national defense information;
- n. records or information relating to who created, used, owned, controlled or communicated with the SUBJECT ACCOUNT; and
- o. records or information relating to the times and/or locations where the SUBJECT ACCOUNT was used, including Internet Protocol addresses

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of electronic storage and any photographic form.