

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)

Email Account < > that is stored at premises controlled by AOL, Inc.

Case: 1:12-mj-880
Assigned To : Magistrate Judge Alan Kay
Assign. Date : 11/15/2012
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): email account identified by user account < > that is stored by AOL, Inc., located at 22000 AOL Way, Dulles, Virginia and more fully described in ATTACHMENT A to this application

located in the Eastern District of Virginia, 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, United States Code, Sections 2701 through 2711, namely contents of electronic e-mails and other electronic data more fully described in ATTACHMENT A 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:

Table with 2 columns: Code Section, Offense Description. Row 1: 18 U.S.C. § 793, Unauthorized Disclosure of National Defense Information

The application is based on these facts:

see attached affidavit herein incorporated by reference as if fully restated

- ✓ Continued on the attached sheet.
✓ Delayed notice of 90 days (give exact ending date if more than 30 days: 2/15/2013) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Handwritten signature of Craig A. Moringiello

Applicant's signature

Craig A. Moringiello, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: NOV 15 2012

Handwritten signature of Alan Kay

Judge's signature

Alan Kay, United States Magistrate Judge

Printed name and title

City and state: Washington, D.C.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
THAT IS
STORED AT PREMISES CONTROLLED BY
AOL, INC.

Case: 1:12-mj-880
Assigned To : Magistrate Judge Alan Kay
Assign. Date : 11/15/2012
Description: Search And Seizure Warrant

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Craig A. Moringiello, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since June, 2002. I have been assigned to the Counterintelligence Division of the FBI's Washington Field Office since December, 2011. In the course of my duties as a Special Agent, I am responsible for investigating offenses involving espionage, illegal agents of foreign powers, United States trade sanctions, unauthorized retention and disclosure of classified and national defense information, and media leaks in furtherance of national security offenses. As a result of this experience, I am familiar with the tactics, methods, and techniques of particular United States persons who possess, or have possessed a United States government security clearance and may choose to harm the United States by misusing their access to classified information.

2. As a federal agent, I am authorized to investigate violations of 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 provided by the investigation to date and on my experience and background as a Special Agent of the FBI. The information set forth in this affidavit concerning the investigation at issue is known to me as a result of my own involvement in the 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.

3. This affidavit is made in support of an application for a warrant pursuant to 18 U.S.C. § 2703 to compel AOL Inc., which functions as an electronic communications service and remove computing service, and is a provider to electronic communication and remove computing services (hereinafter “AOL” or the “PROVIDER”), located at 22000 AOL Way, Dulles, Virginia, to provide subscriber information, records, and the contents of wire and electronic communications pertaining to the accounts identified as _____@aol.com hereinafter referred to as the SUBJECT ACCOUNT.¹

4. For the reasons set forth below, I believe there is probable cause to conclude that the contents of the wire and electronic communications pertaining to the SUBJECT ACCOUNT, are evidence, fruits and instrumentalities of criminal violations of 18 U.S.C. § 793 (Unauthorized Disclosure of National Defense Information).

5. Based on my training and experience, and discussions with the United States Department of Justice, I have learned that 18 U.S.C. § 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 and with reason to believe that such information could be used to the injury of the United States or to the advantage of any foreign nation.

¹ Because this Court has jurisdiction over the offense under investigation, it may issue the warrant to compel the PROVIDER pursuant to 18 U.S.C. § 2703(a). See 18 U.S.C. § 2703(a) (“A governmental entity may require disclosure by a provider . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation”).

6. The SUBJECT ACCOUNT is an email account. As discussed below, investigation into the SUBJECT ACCOUNT indicates that it was and is used by and is believed to have been associated with the unauthorized disclosure of national defense information.

II. FACTS SUPPORTING PROBABLE CAUSE

7. In June 2012, classified information was published in an article on a United States news organization's website and in print (hereinafter the "June 2012 article A") adapted from a June 2012 book (hereinafter referred to as the "June 2012 book"). The June 2012 article A and the June 2012 book were written by a national news reporter, hereinafter referred to as "Reporter A," who was assigned to cover national security issues in Washington, DC. In June, 2012, two other articles containing national defense information were published on two additional United States news organizations' websites and in print (hereinafter referred to as the "June 2012 article B" and "June 2012 article C"). The June 2012 article B was written by national news reporters hereinafter referred to as "Reporter B1" and "Reporter B2". The June article C was written by a national news reporter hereinafter referred to as "Reporter C."

8. Classified information is defined by Executive Order 13526 and its predecessor orders, 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 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. Where such damage could reasonably result in "exceptionally grave" damage to the national security, the information may be classified as "TOP SECRET." Access to classified information at any level may be further restricted through compartmentalization "SENSITIVE

COMPARTMENTED INFORMATION” (SCI) categories, which further restricts the dissemination and handling of the information.

9. The Intelligence Community owners of the classified information at issue have informed the FBI that the June 2012 article A, the June 2012 book, the June 2012 article B, and the June 2012 article C disclosed national defense information that was classified at the TOP SECRET//SCI Level. Further, they have informed the FBI that the information was not declassified prior to its disclosure in the June 2012 book, the June 2012 article A, the June 2012 article B, and the June 2012 article C. They further informed me that the information disclosed in the book and articles remains classified at the TS/SCI level to this day, its public disclosure has never been lawfully authorized.

10. During the investigation, I learned that a national news reporter, hereinafter referred to as “Reporter D”, published an article with two co-authors, on the website of a national news organization in February 2012, hereinafter referred to as the “February 2012 article,” that contained similar content to the classified national defense information contained in the June 2012 book, the June 2012 article A, the June 2012 article B, and the June 2012 article C.

11. Based on my training and experience, I know 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 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. Reporters A, B1, B2, C and D did not possess a security clearance at any time relevant to the matters under investigation.

12. Following the disclosure of the classified national defense information in the June 2012 book and the June 2012 articles A, B, and C an FBI investigation was initiated to determine the source(s) of the unauthorized disclosures.

13. On or about June 7, 2012, I interviewed an official (hereinafter referred to as "Official A") with a United States intelligence agency (hereinafter referred to as "Agency A") who advised me that on February 13, 2012, this official met with Reporter A. At that meeting, Reporter A outlined certain information he had for the book he was working on, which ultimately was published as the June 2012 book. After the meeting, Official A wrote a classified email notifying the executive management of Agency A that Reporter A possessed classified information.

14.

and

during that time period possessed a security clearance allowing him access to TOP SECRET//SCI information, including TOP SECRET//SCI information that was disclosed in the June 2012 book and articles referenced above.

15. On or about June 15, 2012, I interviewed who told me that he met with Reporter A on two occasions in 2011 and exchanged emails with him in 2012. In the course of their first meeting in 2011 Reporter A's "new book", which was ultimately published as the June 2012 book, was discussed by and Reporter A and the second occasion when they met in 2011 was related to the topic of Reporter A's first book (not the book Reporter A published in 2012). The email exchange between and Reporter A concerned a quote had given Reporter A for the June 2012 book.

is in fact quoted in the June 2012 book and acknowledged to your

affiant that he had given the statement he is quoted as making to Reporter A.

provided affiant with what Reporter A had given him as his (Reporter A's) email address ([Reporter's A first two letters of his first name followed by the first four letters of his last name@[name of national newspaper].com) and a telephone number.

16. I reviewed email records provided from another U.S. Government Agency (hereinafter "Agency B") which contained correspondence between a national security public affairs officer with Agency B (hereinafter "Official B1") and . In June 2012, on the same day that the June 2012 article A was published, sent an email to Official B1 with the subject line "On the record." In the body of the email wrote "What I said on the record was that I would not talk about it. [Reporter A] clearly states that I would not talk about what happened while I was in government and I frankly didn't know (until today of course) what happened after I left. ." Official B1 then forwarded the email to senior U.S. Government officials at Agency B. A senior U.S. Government official also at Agency B (hereinafter "Senior Official B2") stated in reply, "That's not what [Reporter A] told me." Senior Official B2 had repeated contact with Reporter A prior to this email exchange.

17. I have reviewed a document from Agency A's Public Affairs Office which contains telephone numbers and email addresses for Reporter B1, B2, and C which were listed as follows: email address for Reporter B1 ([last name, first initial of Reporter B1]@[domain name of national newspaper].com); Reporter B2 ([last name, first initial of Reporter B2]@[domain name of national newspaper].com); and Reporter C ([first name.last name]@[name of national newspaper].com).

18. I have reviewed records from a different U.S. Government Agency (hereinafter Agency C") which had correspondence between Reporter A and U.S. Government officials.

Reporter A used email address ([Reporter A last name followed by the initials for National Newspaper Name]@gmail.com)

19. On or about August 10, 2012, the PROVIDER advised the FBI that the subscriber for the SUBJECT ACCOUNT was _____ and that the SUBJECT ACCOUNT was created on December 12, 1995.

20. In October, 2012, on application from the United States Attorney for the District of Maryland, this Court issued an order pursuant to 18 U.S.C. § 2703(d) to AOL for the SUBJECT ACCOUNT.

21. On October 17, 2012, pursuant to that order, the PROVIDER produced transactional email information from the SUBJECT ACCOUNT. The data shows the following contact between the SUBJECT ACCOUNT and Reporter A's national newspaper email and gmail account:

DATE	NUMBER OF CONTACTS
August 11, 2011	1 time
August 14, 2011	1 time
November 12, 2011	1 time
November 14, 2011	1 time
November 15, 2011	2 times
November 17, 2011	2 times
February 7, 2012	1 time
July 13, 2012	1 time

22. The data also shows the following contact between the SUBJECT ACCOUNT and Reporter B1's work email account:

MONTH	NUMBER OF CONTACTS
November, 2010	1 time
December, 2010	1 time
March, 2011	2 times
April, 2011	5 times
January, 2012	6 times
March, 2012	5 times
April, 2012	6 times
May, 2012	13 times
June, 2012	5 times

23. The data also shows the following contact between SUBJECT ACCOUNT and Reporter B2's work email account:

MONTH	NUMBER OF CONTACTS
November, 2010	6 times
December, 2010	1 time
January, 2011	1 time
March, 2011	1 time
April, 2011	2 times
May, 2011	3 times

October, 2011	1 time
January, 2012	7 times
March, 2012	1 time
April, 2012	6 times
July, 2012	4 times
October, 2012	10 times

24. The data also shows the following contact between SUBJECT ACCOUNT and Reporter C's work email account:

MONTH	NUMBER OF CONTACTS
May, 2011	1 time
June, 2011	3 times
July, 2011	1 time
August, 2011	3 times
September, 2011	5 times
October, 2011	3 times
February, 2012	5 times
May, 2012	5 times
June, 2012	3 times
September, 2012	1 time

25. The data also shows the following contact between the SUBJECT ACCOUNT and an email account that may be associated with Reporter D's gmail address ([Reporter D's first

initial and last name]@gmail.com) and Reporter D's work email address ([Reporter D's first name.last name]@[national news magazine].com):

MONTH	NUMBER OF CONTACTS
December, 2010	3 times
May, 2011	4 times
June, 2011	4 times
July, 2011	1 time
November, 2011	2 times
March, 2012	6 times

26. From my review of U.S. Government records pertaining to Reporter A's email communications with U.S. Government officials, I have learned that Reporter A sent email to U.S. Government officials asking them to confirm quotes that he intended to use in his articles and books. Specifically, I reviewed several email messages Reporter A sent to U.S. Government officials seeking to confirm specific quotes Reporter A intended to include in the June 2012 book. Additionally, Reporter A also sent emails to U.S. Government officials seeking to arrange meetings and interviews with those government officials, discussing information other government officials had already provided to him, and thanking U.S. Government officials for meeting with him.

27. In October, 2012, the FBI sent a preservation letter to AOL to preserve the SUBJECT ACCOUNT. In general, an e-mail that is sent to an AOL subscriber is stored in the subscriber's "mail box" on AOL servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on AOL's servers indefinitely. Even if the

subscriber deletes the e-mail, it may continue to be available on AOL's servers for a certain period of time.

III. BACKGROUND CONCERNING AOL

28. In my training and experience, I have learned that AOL provides a variety of on-line services, including e-mail access, to the public. AOL allows subscribers to obtain e-mail accounts at the domain name gmail.com, like the SUBJECT ACCOUNT. Subscribers obtain an account by registering with AOL. During the registration process, AOL asks subscribers to provide basic personal information. Therefore, the computers of AOL, Inc. are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for AOL subscribers) and information concerning subscribers and their use of AOL 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.

IV. STORED WIRE AND ELECTRONIC COMMUNICATIONS:

29. 18 U.S.C §§ 2701-2711 is called the "Electronic Communications Privacy Act."
- a. 18 U.S.C. Section 2703(a) provides, in part:
 - i. A government entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication that is in electronic storage in an electronic communications systems for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State Warrant. A government entity may require the disclosure by a provider of electronic communication that has been in electronic storage in an electronic communications systems for more than one hundred eighty days by the means available under subsection (b) of this section.
 - b. 18 U.S.C Section 2703(b) provides, in part:

- i. A government entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection-
 - 1. Without required notice to the subscriber or customer, if the government entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or . . .
 - 2. Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service-
 - a. On behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and
 - b. Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing
- c. The Government may also obtain records and other information pertaining to a subscriber or customer of an electronic communication service or remote computing service by way of a search warrant. 18 U.S.C. Section 2703(c)(1)(A). No notice to the subscriber or customer is required. 18 U.S.C. Section 2703(c)(2).
- d. 18 U.S.C. Section 2711 provides, in part:
 - i. As used in this chapter-(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and (2) the term “remote computing service” means the provision to the public of computer storage or processing services by means of an electronic communication system.
- e. 18 U.S.C. Section 2510 provides, in part:
 - i. (8) “Contents,” when used with respect to any wire, oral or electronic communication, includes any information concerning the substance, purport, or meaning of that communication; ... (14) “electronic communication system” means any wire, radio, electromagnetic, photooptical, or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications; (15) “electronic...communication service” means any service which provides to users thereof the ability to send or receive wire or electronic

communications; ... (17) “electronic storage” means –(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

f. 18 U.S.C. Section 2703 (g) provides in part:

- i. Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber or customer of such service.

V. ITEMS TO BE SEIZED:

30. Based on my training and experience, and the training and experience of other counterespionage agents, I believe that the information requested in Attachment A for the SUBJECT ACCOUNT will provide valuable information regarding the investigation of the June 2012 unauthorized disclosure of national defense information. The contents of the e-mails may help to establish further links between _____ and Reporters A, B1, B2 C and D as well as other members of the media to whom disclosure of national defense information is illegal.

31. Based on the foregoing, I request that the Court issue a search warrant with respect to the PROVIDER in accordance with 18 U.S.C. Section 2703 using the procedures set forth in Attachment A to this search warrant. The PROVIDER will copy all of the files, records, and other documents for the SUBJECT ACCOUNT. Government agents will then review the copied material to search for evidence, fruits and instrumentalities of criminal violations of 18 U.S.C. Section 793. The original production from the PROVIDER will then be sealed.

VI. REQUEST FOR NON-DISCLOSURE BY PROVIDER:

32. Pursuant to 18 U.S.C. Section 27059(b), I request that the Court enter an order commanding the PROVIDER not to notify any other person, including the subscriber of the SUBJECT ACCOUNT, of the existence of the warrant because there is reason to believe that notification of the existence of the warrant will result in: (1) destruction of or tampering of evidence; (2) attempts to influence potential witnesses; or (5) otherwise seriously jeopardize the investigation. The involvement of the SUBJECT ACCOUNT, as set forth above, is not public and I know, based on my training and experience, that subjects of criminal investigations will often destroy digital evidence if the subject learns of an investigation. Additionally, if the PROVIDER or other persons notify anyone that a warrant has been issued on the SUBJECT ACCOUNTS, the targets of this investigation and other persons may further mask their identity and activity and seriously jeopardize the investigation.

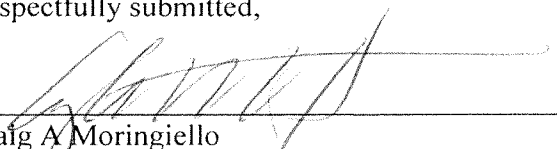
VII. REQUEST FOR SEALING:

33. Because this investigation is continuing and disclosure of some of the details in this affidavit may compromise subsequent investigative measures to be taken in this case may cause the subject to flee, may cause the suspect to destroy evidence and/or may otherwise jeopardize this investigation, I respectfully request this affidavit, and association material seeking this search warrant be sealed until further order of this Court. Finally, I specifically request that the sealing order not prohibit information obtained from this warrant from being shared with other law enforcement and intelligence agencies.

VIII. CONCLUSION

34. Based on the foregoing, there is probable cause to believe that on the computer systems owned, maintained, and/or operated by AOL, Inc. there exists in, and related to, the SUBJECT ACCOUNT, evidence, fruits, and instrumentalities of violations of 18 U.S.C. Section 793 (Unauthorized Disclosure of National Defense Information). By this affidavit and application, I request that the Court issue a search warrant directed to AOL, Inc. allowing agents to seize the content of the SUBJECT ACCOUNT and other related information stored on the AOL, Inc. servers as detailed in Attachment A and following the search procedure also described in Attachment A.

Respectfully submitted,



Craig A. Moringiello
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me

 _____, 2012



ALAN KAY
UNITED STATES MAGISTRATE JUDGE