

UNITED STATES DISTRICT COURT

for the
District of Columbia

In the Matter of the Search of)
(Briefly describe the property to be searched) Case 12-mj-837
or identify the person by name and address) Assigned To Magistrate Judge Robinson Deborah A
Email Account < @gmail.com> that) Assign Date 10/23/2012
is stored at premises controlled by) Description Search and Seizure Warrant
Google, Inc.)

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 Northern District of California (identify the person or describe the property to be searched and give its location): email account identified by user account < @gmail.com> that is stored by Google, Inc., headquartered at 1600 Amphitheatre Parkway, Mountain View, California, and more fully described in ATTACHMENT A to this application

The person or property to be searched, described above, is believed to conceal (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

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before November 6, 2012 (not to exceed 14 days)

[x] in the daytime 6:00 a.m. to 10 p.m. [] at any time in the day or night as I find reasonable 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 United States Magistrate Judge Deborah A. Robinson (name)

[x] 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)

[x] until, the facts justifying, the later specific date of Jan 23, 2013

Date and time issued:

10.53 am

[Handwritten signature]

Judge's signature

City and state: Washington, DC

Deborah A. Robinson, United States Magistrate Judge
Printed name and title

Return		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		
Certification		
<p><i>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</i></p>		
Date:	
 <i>Executing officer's signature</i>	
 <i>Printed name and title</i>	

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
< @GMAIL.COM> THAT IS
STORED AT PREMISES CONTROLLED BY
GOOGLE, INC.

Case 1:12-mj-837
Assigned To Magistrate Judge Robinson, Deborah A
Assign Date 10/23/2012
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 Google Inc., which functions as an electronic communications service and remove computing service, and is a provider to electronic communication and remove computing services (hereinafter “Google” or the “PROVIDER”), located at 1600 Amphitheatre Parkway, Mountain View, California, to provide subscriber information, records, and the contents of wire and electronic communications pertaining to the accounts identified as < @gmail.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.

6. The SUBJECT ACCOUNT is an email account. As discussed below, investigation into the SUBJECT ACCOUNT indicates that it was and is used by James E.

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 . . .”).

Cartwright and is believed to contain evidence related to the unauthorized disclosure of national defense information in at least June 2012.

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, an article by two other national news reporters containing national defense information was published on another United States news organization's websites and in print (hereinafter referred to as the "June 2012 article B"). The June 2012 article B was written by a national news reporter hereinafter referred to as "Reporter B" and another reporter.

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 and the June 2012 article B 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, or the June 2012 article B, it remains classified at the TS/SCI level to this day and its public disclosure has never been lawfully authorized.

10. During the investigation, I learned that a national news reporter, hereinafter referred to as "Reporter C", published an article 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 and the June 2012 Article B.

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, B, and C 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 and B, an FBI investigation was initiated to determine the source(s) of the unauthorized disclosures.

13. Witnesses I have interviewed in this case advised that, to their knowledge, the Intelligence Community owners of the classified information disclosed in the June 2012 book and the June 2012 articles A and B did not authorize Reporters A, B, C or any other members of the press to receive it.

14. On or about June 7, 2012, I interviewed an official 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, the official wrote a classified email notifying the executive management of Agency A that Reporter A possessed classified information.

15. James E. Cartwright is a retired United States Marine Corps four-star general. General Cartwright served as the Vice Chairman of the Joint Chiefs of Staff from 2007-2011 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.

16. On September 1, 2011, General Cartwright executed a Debriefing Acknowledgement on a Special Access Program Indoctrination (SAPI) Agreement. SAPI Agreements are legally binding agreements between an individual being granted, or already in possession, of a security clearance, and the United States Government where in the individual agrees to never disclose classified information without first receiving appropriate authorization. Among other things, the SAPI Agreement states in Paragraph 3: "... I understand that it is my responsibility to consult with appropriate management authorities in the department or agency that last authorized my access to SAPI, whether or not I am still employed or associated with that

Department of Agency. . . I further understand that I am obligated by law and regulation not to disclose any classified information or material in an unauthorized fashion.” Paragraph 6 states “I have been advised that any breach of this agreement may constitute violations of United States criminal laws, including the provisions of Sections 793, 794, 798, and 592, Title 18 United States Code, and of Section 783 in (a), Title 50, United States Code. Nothing in this agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.”

17. On or about July 19, 2012, a former official of the Joint Chiefs of Staff told me that on April 23, 2012 he met with General Cartwright. General Cartwright told the official that he knew Reporter A had another book coming out. General Cartwright told the official that he had advance knowledge of the book and had been asked to review the information in it regarding the classified program. General Cartwright told the official that the information Reporter A had for his book was accurate and nothing could be done to stop the sensitive information it contained from coming out.

18. I have reviewed copies of email correspondence between the Director of Public Affairs for Agency A and Reporter A. On March 10, 2012, Reporter A sent the Director of Public Affairs of Agency A an email from a Google email account. The email address was Reporter A’s name followed by “@gmail.com.” In the email, Reporter A stated “this is my direct gmail account.” I have also reviewed a document from Agency A’s Public Affairs Office which contains telephone numbers and an additional email address for Reporter A issued by the news organization for which he works ([Reporter A last name]@[name of national newspaper].com) and an email address for Reporter B ([last name, first initial of Reporter B]@[domain name of national newspaper].com). The same document also had a telephone number for national news Reporter C. From my review of other U.S. Government records, I

learned of other telephone numbers used by or associated with Reporter A including Reporter A's home telephone number.

19. On or about August 18, 2012, the PROVIDER advised the FBI that the subscriber for the SUBJECT ACCOUNT was James Cartwright, SMS XXX-XXX-9767 and that the SUBJECT ACCOUNT was created on March 26, 2011.

20. In September 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 Google for the SUBJECT ACCOUNT.

21. On October 4, 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 gmail account:

DATE	NUMBER OF CONTACTS
January 15, 2012	4 times
January 17, 2012	1 time
January 18, 2012	4 times
March 9, 2012	2 times
March 13, 2012	3 times
March 14, 2012	4 times
April 6, 2012	3 times
April 7, 2012	1 time
April 9, 2012	3 times

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

MONTH	NUMBER OF CONTACTS
November, 2011	3 times
December, 2011	34 times
January, 2012	14 times
February, 2012	21 times
March, 2012	87 times
April, 2012	19 times
May, 2012	23 times
June, 2012	5 times

23. The data also shows the following contact between the SUBJECT ACCOUNT and an email account that may be associated with Reporter C's gmail address which was listed as Reporter C's first initial and last name@gmail.com:

MONTH	NUMBER OF CONTACTS
November, 2011	15 times
December, 2011	5 times
January, 2012	8 times
February, 2012	28 times

24. On or about August 28, 2012, I received telephone toll records from General Cartwright's Verizon Wireless cellular telephone number XXX-XXX-9767. The records show the following contact between General Cartwright's cellular telephone and telephone numbers associated with Reporter A:

DATE	TIME	FROM	TO	DURATION
01/27/12	5:19 PM	Cartwright Cell	Reporter A Cell #1	2 Min
01/28/12	12:00 PM	Cartwright Cell	Reporter A Cell #1	1 Min
01/28/12	12:02 PM	Reporter A Home	Cartwright A Cell	39 Min
03/09/12	7:04 PM	Cartwright Cell	Reporter A Cell #1	31 Min
04/09/12	1:03 PM	Reporter A Cell#2	Cartwright Cell	2 Min

25. The telephone records also show the following contact between General Cartwright's cellular telephone and telephone numbers associated with Reporter B.

DATE	TIME	FROM	TO	DURATION
09/26/11	3:46 PM	Reporter B Office	Cartwright Cell	15 Min
10/17/11	6:45 PM	Reporter B Office	Cartwright Cell	1 Min
10/25/11	11:02 AM	Reporter B Office	Cartwright Cell	31 Min
01/13/12	10:32 AM	Reporter B Office	Cartwright Cell	6 Min
01/26/12	12:34 PM	Reporter B Cell	Cartwright Cell	1 Min
01/26/12	12:36 PM	Cartwright Cell	Reporter B Cell	38 Min
01/30 /12	5:17 PM	Reporter B Office	Cartwright Cell	18 Min
03/01/12	8:54 AM	Reporter B Cell	Cartwright Cell	1 Min
03/09/12	9:27 AM	Reporter B Cell	Cartwright Cell	1 Min
03/17/12	12:20 PM	Reporter B Cell	Cartwright Cell	1 Min
03/17/12	12:21 PM	Cartwright Cell	Reporter B Cell	1 Min
03/26/12	3:06 PM	Reporter B Office	Cartwright Cell	25 Min
03/27/12	5:54 PM	Reporter B Office	Cartwright Cell	14 Min
04/19/12	4:37 PM	Reporter B Office	Cartwright Cell	41 Min
04/19/12	5:19 PM	Reporter B Office	Cartwright Cell	1 Min
05/07/12	3:09 PM	Reporter B Office	Cartwright Cell	25 Min
05/09/12	5:38 PM	Cartwright Cell	Reporter B Cell	26 Min
05/21/12	5:55 PM	Reporter B Cell	Cartwright Cell	4 Min
06/01/12	11:40 AM	Reporter B Office	Cartwright Cell	1 Min
06/07/12	7:41 AM	Cartwright Cell	Reporter B Cell	29 Min

26. The telephone records also show the following contact between General Cartwright's cellular telephone and a telephone number associated with Reporter C:

DATE	TIME	FROM	TO	DURATION
01/31/12	7:31 AM	Cartwright Cell	Reporter C Office	1 Min
03/22/12	11:01 AM	Reporter C Office	Cartwright Cell	61 Min
05/07/12	4:23 PM	Cartwright Cell	Reporter C Office	14 Min
05/08/12	2:00 PM	Reporter C Office	Cartwright Cell	29 Min

27. 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 emails 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.

28. In June, 2012, the FBI sent a preservation letter to Google, Inc. to preserve the SUBJECT ACCOUNT. In general, an e-mail that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Google's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Google's servers for a certain period of time.

III. BACKGROUND CONCERNING GOOGLE

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

30. 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

31. 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 General Cartwright and Reporters A, B and C, as well as other members of the media to whom disclosure of national defense information is illegal. Further, the content of those communications from General Cartwright may well assist the FBI in establishing the fact of the disclosures and his intent in making them.

32. 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:

33. 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.

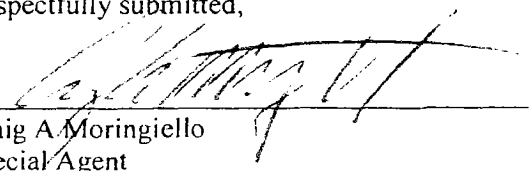
VII. REQUEST FOR SEALING:

34. 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

35. Based on the foregoing, there is probable cause to believe that on the computer systems owned, maintained, and/or operated by Google, 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 Google, Inc. allowing agents to seize the content of the SUBJECT ACCOUNT and other related information stored on the Google, 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 on JCT 23 2012 , 2012



DEBORAH A. ROBINSON
UNITED STATES MAGISTRATE JUDGE

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
< @GMAIL.COM> THAT IS STORED
AT PREMISES CONTROLLED BY GOOGLE,
INC.

Case No. _____

Filed Under Seal

ATTACHMENT A: ITEMS TO BE SEIZED

Pursuant to 18 U.S.C. Section 2703, it is hereby ordered as follows:

I. SERVICE OF WARRANT AND SEARCH PROCEDURE

a. Google, Inc. a provider of electronic communication and remote computing Services, located at 1600 Amphitheatre Drive, Mountain View, California, (hereafter the "PROVIDER") will isolate those accounts and files described in Section II below. Pursuant to 18 U.S.C. Section 2703(g) the presence of an agent is not required for service or execution of this warrant.

b. In order to minimize any disruption of computer service to innocent third parties, the PROVIDER's employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computers account and files described in Section II below, including an exact duplicate of all information stored in the computer account and files described therein.

c. As soon as practicable after service of this warrant, the PROVIDER shall provide the exact duplicate in electronic form of the accounts and files described in Section II below and all information stored in those accounts and files to the following FBI Special Agent:

SA Craig Moringiello
FBI-WFO
601 4th Street NW
Washington, DC 20535
Desk 202-278-8314
Cell 202-384-8314

The PROVIDER shall send the information to the agent via United States mail, and where maintained in electronic form, on CD-ROM or an equivalent electronic medium.

d. The original production from the PROVIDER will be sealed – and preserved for authenticity and chain of custody purposes – until further order of the Court.

e. The PROVIDER shall not notify any other person, including the subscriber of < @gmail.com> (hereinafter “SUBJECT ACCOUNT”) of the existence of the warrant.

f. The U.S. Department of Justice and the Federal Bureau of Investigation shall not be prohibited from sharing information obtained from this warrant with other law enforcement and intelligence agencies, including foreign law enforcement and intelligence agencies, for use in investigation and prosecution.

II. FILES AND ACCOUNTS TO BE COPIED BY THE PROVIDER’S EMPLOYEES

a. All material stored and presently contained in, or on behalf of the SUBJECT ACCOUNT including videos, computer files sent to and received from other websites, received messages, sent messages, deleted messages, and messages maintained in trash or other folders, and any attachments thereto:

b. All existing printouts from original storage of all of the electronic mail described above in Section II(a);

c. All transactional information of all activity of the SUBJECT ACCOUNT described above in Section II(a), including log files, dates, times, methods of connecting, ports, dial-ups, registration Internet Protocol addresses and/or locations;

d. All business records and subscriber information, in any form kept, pertaining to the SUBJECT ACCOUNT described above in Section II(a), including applications, subscribers’ full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers, account numbers, screen names, status of accounts, dates of service, method of payment, telephone numbers, addresses, detailed billing records, and histories and profiles;

e. Any and all Google address books and/or Google instant messenger list

maintained by the account; and

f. All records indicating the account preferences and services available to the subscriber of the SUBJECT ACCOUNT described above in Section II(a).

III. INFORMATION TO BE SEIZED BY LAW ENFORCEMENT PERSONNEL

Items to be seized, which are believed to be evidence and fruits of violations of 18 U.S.C Section 793 (Unauthorized Disclosure of National Defense Information) as follows:

a. The contents of wire and electronic communications, including attachments and stored files, for the SUBJECT ACCOUNT, including videos, computer files sent to and received from other websites, received messages, sent messages, deleted messages, messages maintained in trash or other folders, any attachments thereto, and all existing printouts from original storage of all of the electronic mail described above in Section II(a), that pertain to:

1. records or information related to violations of the aforementioned statute;
2. records or information concerning General James Cartwright's communications and activities on the dates surrounding the publication of the February, 2012 and June 2012 article;
3. records or information related to General James Cartwright's knowledge of rules and/or procedures prohibiting the unauthorized disclosure of classified information;
4. records or information related to General James Cartwright's knowledge of rules and/or procedures regarding communications with the press;
5. records or information related to any disclosure or prospective disclosure of classified information;
6. any classified document, image, record or information, and any communications concerning such documents, images, records, or information
7. any document, image, record or information concerning the national defense, including but not limited to documents, maps, plans, diagrams, guides, manuals, and other Department of

Defense, U.S. military, and/or weapons material, as well as sources and methods of intelligence gathering, and any communications concerning such documents, images, records, or information

8. records or information related to Reporter A, B or C or Reporter A, B, or C's news organizations or any entity or individual affiliated in any way with that organization
9. records or information related to communications with members of the press or any entity or individual affiliated in any way with a press organization;
10. records or information related to the state of mind of any individuals seeking the disclosure or receipt of classified information;
11. records or information related to the subject matter of the February, 2012, and June, 2012 article or the foreign countries referenced in the February 2012 and June 2012 articles;
12. records or information related to the user(s) of the SUBJECT ACCOUNT;
13. records or information related to the associates of General James Cartwright or any other user identified with the SUBJECT ACCOUNT;
14. records or information related to General Cartwright or his associates' schedule of travel or travel documents;
15. records or information related to communications to any foreign person or any person residing in a foreign country; and
16. records and information related to any bank records, checks, credit card bills, account information, and other financial records.

b. All of the records and information described above in Sections II(c), (d), (e), and (f)

including:

1. Account information for the SUBJECT ACCOUNT including:
 - (a) Names and associated email addresses
 - (b) Physical address and location information
 - (c) Records of session times and durations
 - (d) Length of service (including start date) and types of service utilized
 - (e) Telephone or instrument number or other subscribers number or identity, including any temporarily assigned network addresses;
 - (f) The means and source of payment for such service (including any credit card or bank account number); and
 - (g) Internet Protocol addresses used by the subscriber to register the account or otherwise initiate service.
2. User connection logs for the SUBJECT ACCOUNT for any connections to or from the SUBJECT ACCOUNT. User connection logs should include the following:
 - (a) Connection time and date;
 - (b) Disconnect time and date;
 - (c) Method of connection to system (e.g. SLIP, PPP, Shell);
 - (d) Data transfer volume (e.g. bytes);
 - (e) The IP address that was used when the user connected to the service

- (f) Connection information for other systems to which user connected via the SUBJECT ACCOUNT, including:
 - (1) Connection destination;
 - (2) Connection time and date;
 - (3) Disconnect time and date;
 - (4) Method of connection to system (e.g. telnet, ftp, http);
 - (5) Data transfer volume (e.g. bytes);
 - (6) Any other relevant routing information.
- (g) Source or destination of any wire or electronic mail messages sent from or received by the SUBJECT ACCOUNT, and the date, time, and length of message; and
- (h) Any address to which the wire or electronic mail was or is to be forwarded from the SUBJECT ACCOUNT or email address.

ATTACHMENT B

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL RULE
OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google, Inc, and my official title is _____. I am a custodian of records for Google, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of Google, Inc; and
- c. such records were made by Google, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature