

# UNITED STATES DISTRICT COURT

for the  
Eastern District of Virginia

In the Matter of the Search of )  
(Briefly describe the property to be searched )  
or identify the person by name and address) )  
ONE DELL POWEREDGE 2900 SERVER )  
SERIAL NUMBER G842PC1 )

Case No. 1:15-SW-537

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Virginia  
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

SEE ATTACHMENT B

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 September 11, 2015  
(not to exceed 14 days)

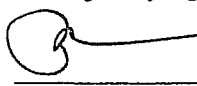
- in the daytime 6:00 a.m. to 10 p.m.       at any time in the day or night as I find reasonable cause has been established.

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 Theresa C. Buchanan  
(name)

- I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)  for \_\_\_\_\_ days (not to exceed 30).  
 until, the facts justifying, the later specific date of \_\_\_\_\_

Date and time issued: 8/25/15

  
Theresa Carroll Buchanan  
United States Magistrate Judge  
Judge's signature

City and state: Alexandria, Virginia

Theresa C. Buchanan, United States Magistrate Judge  
Printed name and title

UNITED STATES DISTRICT COURT

for the Eastern District of Virginia

AUG 28 2015

UNDER SEAL

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

ONE DELL POWEREDGE 2900 SERVER SERIAL NUMBER G842PC1

Case No. 1:15-SW-537

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):

SEE ATTACHMENT A

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

SEE ATTACHMENT B

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. Rows include 18 U.S.C. 793(e) and 793(f) with descriptions of national defense information (NDI) offenses.

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- 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.

Reviewed by AUSA/SAUSA:

[Redacted]

[Redacted Signature]

Applicant's signature

[Redacted Name], FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 08/28/2015

Theresa Carroll Buchanan United States Magistrate Judge

Judge's signature

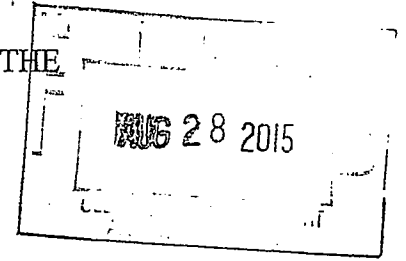
City and state: Alexandria, Virginia

Theresa C. Buchanan, United States Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF                    )  
ONE DELL POWEREDGE 2900 SERVER,            )  
SERIAL NUMBER G842PC1                        )     **UNDER SEAL**  
Case No. 1:15-SW-537

AFFIDAVIT IN SUPPORT OF A SEARCH AND SEIZURE WARRANT

I, [REDACTED], being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. The government is conducting a criminal investigation concerning the improper transmission and storage of classified information on unclassified email systems and servers. The investigation began as a result of a review of emails undertaken by the U.S. Department of State in connection with Freedom of Information Act (FOIA) litigation. During this FOIA review, it was determined that certain emails containing classified information were sent and received on systems unauthorized for the transmission or storage of such information. On or about July 6, 2015, the Inspector General for the Intelligence Community notified the Federal Bureau of Investigation (FBI) of a potential compromise of classified information involving the emails discovered through the FOIA review. After an initial review of the matter, the FBI opened a criminal investigation to, among other things, identify any unauthorized systems which the emails in question have transited, identify any person(s) who may have introduced classified information onto unauthorized systems and all circumstances surrounding such introduction, and identify any person(s) who may have transmitted information over any such systems.

2. The FBI's investigation has established that the emails containing classified

information have been transmitted and stored on multiple forms of electronic media. One of the items identified as having contained such emails is a Dell Poweredge 2900 Server, Serial Number G842PC1 (the "Target Server"), which was used by former Secretary of State Hillary Rodham Clinton ("Clinton") to transmit, receive, and store email for a personal email account or accounts she maintained. As described below, one domain on the Target Server was @clintonemail.com. The Target Server is currently located within the Eastern District of Virginia, as more fully described in Attachment A to this affidavit. There is probable cause to believe that the Target Server contains evidence, contraband, fruits, and/or other items illegally possessed in violation of 18 U.S.C. § 793(e) and (f).

3. I am a Special Agent with the FBI, and have been since July 2010. Prior to my appointment as a Special Agent, I worked as an Intelligence Analyst with the FBI for approximately five years, addressing primarily counterintelligence and counterterrorism matters. As a Special Agent, I have been assigned to the Counterintelligence Division of the FBI's Washington Field Office since November 2010. 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 money laundering in furtherance of national security offenses.

#### SOURCE OF EVIDENCE

4. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation, and information from other FBI personnel. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

## STATUTORY AUTHORITY AND DEFINITIONS

5. Under 18 U.S.C. § 793(e), “[w]hoever having unauthorized possession of, access to, or control over any document . . . 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 do or causes the same “to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it” shall be fined or imprisoned not more than ten years, or both.

6. Under 18 U.S.C. § 793(f), “[w]hoever, being entrusted with or having lawful possession or control of any document . . . or information, relating to the national defense” either “(1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed,” or “(2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer” shall be fined or imprisoned not more than ten years, or both.

7. Under Executive Order 13526, information in any form may be classified if it: (1) is owned by, produced by or for, or is under the control of the United States government; (2) falls within one or more of the categories set forth in the Executive Order [Top Secret, Secret, and Confidential]; 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.

8. Where such unauthorized disclosure could reasonably result in damage to the national security, the information may be classified as "Confidential" and must be properly safeguarded. Where such unauthorized disclosure could reasonably result in "serious" damage to the national security, the information may be classified as "Secret" and must be properly safeguarded. Where such unauthorized disclosure could reasonably result in "exceptionally grave" damage to the national security, the information may be classified as "Top Secret" and must be properly safeguarded.

9. Sensitive Compartmented Information (SCI) means classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems.

10. Special Intelligence, or "SI," is an SCI control system designed to protect technical and intelligence information derived from the monitoring of foreign communications signals by other than the intended recipients. The SI control system protects SI-derived information and information relating to SI activities, capabilities, techniques, processes, and procedures.

11. Classified information may be marked as "Not Releasable to Foreign Nationals/Governments/US Citizens," abbreviated "NOFORN," to indicate information that may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-U.S. citizens without permission of the originator.

12. Classified information may be marked as "Releasable to Five Eyes," abbreviated "REL FVEY," to indicate classified information that is authorized for release to only the United States, Australia, Canada, Great Britain, and New Zealand.

13. Classified information, of any designation, may be shared only with persons

determined by an appropriate United States government official to be eligible for access, and who possess a "need to know." Among other requirements, in order for a person to obtain a security clearance allowing that person access to classified United States government information, that person is required to and must agree to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations. If a person is not eligible to receive classified information, classified information may not be disclosed to that person. In order for a foreign government to receive access to classified information, the originating United States agency must determine that such release is appropriate.

14. Pursuant to Executive Order 13526, classified information contained on automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information must be maintained in a manner that: (1) prevents access by unauthorized persons; and (2) ensures the integrity of the information.

15. 32 C.F.R. Parts 2001 and 2003 regulate the handling of classified information. Specifically, 32 C.F.R. § 2001.43, titled "Storage," regulates the physical protection of classified information. This section prescribes that Secret and Top Secret information "shall be stored in a GSA-approved security container, a vault built to Federal Standard (FED STD) 832, or an open storage area constructed in accordance with § 2001.53." It also requires periodic inspection of the container and the use of an Intrusion Detection System, among other things.

## PROBABLE CAUSE FOR SEARCH

16. Clinton served as the Secretary of State from on or about January 21, 2009 to on or about February 1, 2013. At all times relevant to this affidavit, Clinton and other individuals with whom she corresponded using her @clintonemail.com account(s) had security clearances, as described in Paragraph 13 above.

17. The Target Server was initially set up on or about March 9, 2009. To date, the exact nature and extent of the set-up, configuration, electronic security, back-up systems, third-party vendors with access to the email network, and technological infrastructure surrounding the establishment, maintenance, and use of the Target Server is unknown. In 2013, Platte River Networks, a Denver, Colorado-based information technology firm, took possession of the Target Server. The Target Server was housed at a facility located at 800 Secaucus Road, Secaucus, New Jersey. Prior to Platte River Networks taking possession of the Target Server, the FBI believes the Target Server was housed at Clinton's residence in Chappaqua, New York. The Target Server, regardless of its physical location, was not a device authorized by the United States government to store or transmit classified or national defense information.

18. As a result of a FOIA request, the State Department is currently reviewing approximately 30,490 email communications sent to or from Clinton at the @clintonemail.com domain that resided on the Target Server. The FOIA process implemented by the State Department requires that these emails be reviewed by government agencies for classified information prior to public release. In July 2015, the Inspector General for the Intelligence Community reviewed a sample of approximately 300 emails and found that at least six (6) emails contained classified information, as determined by the relevant original classification authorities. One (1) of the six (6) emails contained information that was determined to be classified at the



Top Secret level. Although not marked as classified, all six (6) emails were determined to contain classified information at the time they were sent to Clinton and received at the @clintonemail.com domain, and the information in five (5) of the emails remains classified today.

19. Through written consent provided by Clinton's personal counsel, Williams & Connolly LLP, the FBI obtained the Target Server as well as physical and electronic copies of the 30,490 emails that Clinton, through her counsel, provided to the State Department for purposes of its FOIA review. Based on representations by Williams & Connolly, the FBI believes the 30,490 electronic email communications were stored on the Target Server, including the six (6) above-referenced emails determined to contain classified information.

20. As an example of one such email determined to contain classified information, on April 10, 2011, a State Department employee sent an email to a State Department email distribution list and three additional State Department employees on the State Department's unclassified email system.<sup>1</sup> One of the individuals then forwarded the email to Clinton's @clintonemail.com account, which, as explained, resided on the Target Server. This email contained information that has since been determined to be classified at the SECRET//SI//NOFORN level when it was sent and is currently classified at the S//REL FVEY level.

21. The U.S. Government's determination that this email contained information classified at the SECRET//SI//NOFORN level at the time it was sent is significant because it means that the unauthorized disclosure of the email could result in "serious" damage to national

---

<sup>1</sup> Like the Target Server, the State Department's unclassified email system is not authorized for the transmission or storage of classified information.

security. This email contains technical and intelligence information derived from the monitoring of foreign communications and therefore contains classified and national defense information. The NOFORN caveat identifies classified intelligence that may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-U.S. citizens.

22. As another example of an email determined to contain classified information, on November 18, 2012, a State Department employee sent an email to five other State Department employees on the State Department's unclassified email system. One of the individuals forwarded the email to five additional State Department employees on the State Department's unclassified email system, one of whom then forwarded the email to Clinton's @clintonemail.com account, which, as explained, resided on the Target Server. This email contained information that has since been determined to be classified at the SECRET//NOFORN level when it was sent and is currently classified at the SECRET//NOFORN level.

23. The U.S. Government's determination that this email contained information classified at the SECRET//NOFORN level at the time it was sent is significant because it means that the unauthorized disclosure of the email could result in "serious" damage to national security. This email contains sensitive sources and methods information and therefore contains classified and national defense information. The NOFORN caveat identifies classified intelligence that may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-U.S. citizens.

24. Following conversations between the Department of Justice and Williams & Connolly, the Department of Justice sent Williams & Connolly and counsel for Platte River Networks a letter on August 7, 2015 confirming counsel's intent to voluntarily produce to the FBI the Target Server and related equipment.

25. On August 10, 2015, Williams & Connolly responded to the Department of Justice's August 7 letter. In this August 10 letter, Williams & Connolly explained that in voluntarily providing to the FBI the Target Server and related equipment, it was doing so only with respect to Clinton's @clintonemail.com account and not with respect to any other accounts that may have been hosted on the Target Server. Williams & Connolly expressed its belief that no such other email accounts or data currently resided on the Target Server, but emphasized that the only consent authority it had with respect to the Target Server related to Clinton's account.

26. On August 12, 2015, Platte River Networks physically turned over the Target Server to the FBI. At the time that Platte River Networks produced the Target Server to the FBI, it gave written consent for the FBI to conduct a search of the Target Server. Upon taking custody of the Target Server in New Jersey, the FBI transported the Target Server to its Operational Technology Division, located at the Engineering Research Facility, Quantico, Virginia.

27. Based upon the consent provided by Williams & Connolly and Platte River Networks to search the Target Server, the FBI conducted a limited, preliminary forensic examination of the Target Server. The preliminary examination revealed that Microsoft Exchange for the domain @clintonemail.com was installed on or about March 9, 2009 and was uninstalled on or about December 3, 2013. Although Microsoft Exchange was uninstalled, deleted files remain on the Target Server and are recoverable in whole or in part. In addition, these files and related logs may provide information about the transmittal of classified information described above.

28. In addition, the FBI's preliminary forensic examination revealed that the Target Server had been configured for two other domains, @presidentclinton.com and @wjcoffice.com.

Due to the uninstallation of Microsoft Exchange from the Target Server, the data from the three relevant domains is comingled and cannot be segregated without a complete forensic analysis and review of the Target Server. As a result, it is not possible to conduct a targeted search of Clinton's @clintonemail.com account(s); rather, the Target Server must be searched as a whole, among other reasons, in order to identify the emails and records that comprise Clinton's @clintonemail.com account(s), pursuant to the procedures specified below.

29. A complete forensic analysis and review will also allow the FBI to determine if there is any evidence of computer intrusions into the Target Server. As discussed above, the FBI believes that classified information was transmitted to and stored on the Target Server. Violations of 18 U.S.C. § 793(e) and/or (f) could have resulted from a computer intrusion of the Target Server, which could have exposed such information to unauthorized persons.

30. Even though Platte River Networks provided consent for the FBI to search the Target Server without limitation, Williams & Connolly limited its consent to Clinton's @clintonemail.com account. For that reason, and also because the data from the three relevant domains is comingled and cannot be segregated without a complete forensic analysis and review, the FBI is seeking a search warrant for the entire Target Server.

31. For the reasons set forth above, I have probable cause to believe that the Target Server contains information classified at the Secret and/or Top Secret level, which was produced by and is owned by the U.S. Government. The Target Server was never authorized for the storage or transmission of classified information. Accordingly, I am seeking the issuance of a warrant to search the Target Server for items described in Attachment B.

## BACKGROUND CONCERNING SERVER HOSTING AND EMAIL HOSTING

32. A server is a computer, connected to other computers through a network, that provides services to other computers. Server hosting companies maintain server computers connected to the Internet. Through a variety of possible arrangements, server hosting companies sell to customers the right to use their server computers, or to use their physical server racks, power, and cooling.

33. In this case, the Target Server hosted the email services for the domain @clintonemail.com. Preliminary forensic analysis indicates that the Target Server previously had been configured for the @presidentclinton.com and @wjcoffice.com domains. Therefore, the Target Server is likely to contain stored electronic communications (including retrieved and unretrieved emails) for at least three domains: @clintonemail.com, @presidentclinton.com, and @wjcoffice.com.

34. Many email servers also provide storage for files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

35. In my training and experience, email servers typically retain certain information about the creation and use of each account on their systems. This information can include the date on which the account was created, dates of use, logon/logoff information, the types of service utilized, the methods used to connect to the account (such as logging into the account via a website or email client), and other log files that reflect usage of the account. In addition, email servers often have records of the Internet Protocol (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 an email account on the Target Server.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

36. As described above and in the Attachments, this application seeks permission to examine the entire Target Server for records that might be stored on it. I submit that there is probable cause to believe those records will be stored on the Target Server, both for the reasons given above and also for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been written to a storage medium, such as a hard drive in the Target Server. Electronic files written to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can sometimes be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file often does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or unallocated space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task.

37. *Forensic evidence.* As further described in the Attachments, this application seeks permission to locate not only computer files that might contain direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the Target Server was used, the purpose of its use, who used it, and when. There is probable cause to believe that examining the Target Server will reveal this forensic electronic evidence because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file. Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Operating systems can record additional information, such as the attachment of additional devices such as USB storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on a computer is evidence of a crime may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the requested warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the



presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

#### SEARCH PROCESS

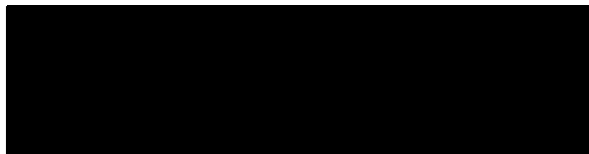
38. To account for the possibility that records containing information that may be subject to attorney-client or other privileges could be maintained on the Target Server, designated FBI personnel who are not, and will not be, actively involved in the criminal investigation will first examine the materials, in consultation with Department of Justice attorneys designated for that purpose (and who likewise are not, and will not be, actively involved in the criminal investigation), and will only release them to the investigative team after it has been ascertained that there is no privileged information or that such information has been removed from the materials. Any information within the scope of this Search Warrant that does contain privileged information will be sealed and not examined by me or anyone participating in the criminal investigation unless and until the privilege is waived or otherwise determined to be inapplicable.

39. Because this warrant seeks only permission to examine the Target Server, which is already in the government's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

#### CONCLUSION


40. Based on the foregoing facts and circumstances, I submit that probable cause exists to believe that evidence, contraband, fruits, and/or other items illegally possessed in violation of 18 U.S.C. § 793(e) and (f) are located on the Target Server. Accordingly, I seek the issuance of a warrant to search the Target Server for evidence, contraband, fruits, or other items

illegally possessed (more particularly described in Attachment B) in violation of 18 U.S.C. § 793(e) and (f).



Special Agent  
Federal Bureau of Investigation

Sworn to and subscribed before me this 28<sup>th</sup> day of August, 2015.

 \_\_\_\_\_  
/s/  
Theresa Carroll Buchanan  
United States Magistrate Judge

Theresa C. Buchanan  
United States Magistrate Judge

ATTACHMENT A

The property to be searched is a Dell Poweredge 2900 Server, Serial Number G842PC1.

Location To Be Searched

The TARGET SERVER is a server computer associated with the @clintonemail.com domain located at the FBI's Operational Technology Division, located at the Engineering Research Facility, Quantico, Virginia 22135.

ATTACHMENT B

Items To Be Seized

All information found on the Target Server that constitutes evidence, contraband, fruits, or other items illegally possessed in violation of 18 U.S.C. § 793(e) and (f), including:

1. Data and information associated with the operation, maintenance, backup, auditing, and security functions of the Target Server including, but not limited to:
  - a. Emails and attachments, in any form;
  - b. User and system files stored on the server, including file fragments and items carved from unallocated space;
  - c. Logs, configuration files, and backups;
  - d. Executable code and scripts;
  - e. Documents and spreadsheets; and
  - f. Network diagrams or architecture;
  
2. Data and information electronically stored on the Target Server associated with Clinton's email account(s) on the domain @clintonemail.com;
  
41. Data and information on the Target Server that might identify the person or persons, who accessed, operated, paid for, or are associated with the Target Server or @clintonemail.com domain, including names, addresses, telephone numbers and other identifiers, email addresses, business information, the length of service (including start date), types of services utilized, means and source of payment for services (including any credit card or bank account number), and information about any domain name registration; and
  
3. Data and information stored on the Target Server that might identify activity related to a computer intrusion, including, but not limited to evidence of malware or viruses, executable code or scripts, log files, audit files, system files, user and account information, IP addresses, computer hardware addresses, intrusion-detection logs, anti-virus logs or anti-malware logs.

UNDER SEAL UNITED STATES DISTRICT COURT  
for the  
COPY Eastern District of Virginia

In the Matter of the Search of )  
(Briefly describe the property to be searched )  
or identify the person by name and address )  
Information Associated With Email Account )  
██████████@Gmail.com That Is Stored At )  
Premises Controlled By Google, Inc. )

Case No. 1:15-SW-578

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):

See Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Attachment B

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 October 1, 2015 (not to exceed 14 days)

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.

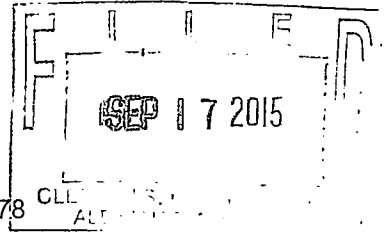
The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge John F. Anderson (name)

I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) for days (not to exceed 30). until, the facts justifying, the later specific date of

Date and time issued: September 17, 2015 3:30 PM Judge's signature

City and state: Alexandria, Virginia The Honorable John F. Anderson Printed name and title

UNITED STATES DISTRICT COURT  
UNDER SEAL for the  
Eastern District of Virginia



In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)  
Information Associated With Email Account  
[Redacted]@Gmail.com That Is Stored At  
Premises Controlled By Google, Inc.

Case No. 1:15-SW-578

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):

See Attachment A

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

See Attachment B

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(e);	Unlawful possession and communication of national defense information (NDI);
18 U.S.C. 793(f)	Unlawful removal or failure to report unlawful removal of NDI

The application is based on these facts:

- 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.

[Redacted Signature]  
Applicant's signature

[Redacted Name], Special Agent, FBI  
Printed name and title

Sworn to before me and signed in my presence.

Date: 09/17/2015

/s/ [Signature]  
John F. Anderson  
United States Magistrate Judge  
Judge's signature

City and state: Alexandria, Virginia

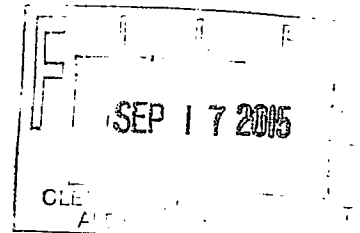
The Honorable John F. Anderson  
Printed name and title

**UNDER SEAL**

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF )  
INFORMATION ASSOCIATED WITH EMAIL )  
ACCOUNT ██████████@GMAIL.COM )  
THAT IS STORED AT PREMISES )  
CONTROLLED BY GOOGLE, INC. )

UNDER SEAL

Case No. 1:15-SW-578

AFFIDAVIT IN SUPPORT OF A SEARCH AND SEIZURE WARRANT

I, ██████████, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. The government is conducting a criminal investigation concerning the improper transmission and storage of classified information on unclassified email systems and servers. The investigation began as a result of a review of emails undertaken by the U.S. Department of State in connection with Freedom of Information Act (FOIA) litigation. During this FOIA review, it was determined that certain emails containing classified information were sent and received on systems unauthorized for the transmission or storage of such information. On or about July 6, 2015, the Inspector General for the Intelligence Community notified the Federal Bureau of Investigation (FBI) of a potential compromise of classified information involving the emails discovered through the FOIA review. After an initial review of the matter, the FBI opened a criminal investigation to, among other things, identify any unauthorized systems which the emails in question have transited, identify any person(s) who may have introduced classified information onto unauthorized systems and all circumstances surrounding such introduction, and identify any person(s) who may have transmitted such information over any such systems.

2. The purpose of this affidavit is to secure a search and seizure warrant for the

Google account [REDACTED], which is associated with the email address [REDACTED]@gmail.com (hereinafter the "SUBJECT ACCOUNT"), within the possession and control of the remote computing service and electronic communication service provider, also referred to as an Internet Service Provider or "ISP," known as Google, Inc. ("Google"), more fully described in Attachment A. There is probable cause to believe that the SUBJECT ACCOUNT contains evidence, contraband, fruits and/or other items illegally possessed in violation of 18 U.S.C. § 793(e) and (f).

3. The search warrant is sought under 18 U.S.C. § 2703(a), (b)(1)(A), and (c)(1)(A) to require Google to disclose to the government records and other information in its possession, pertaining to the subscriber(s) or customer(s) associated with the SUBJECT ACCOUNT, including contents of electronic communications.

4. I am a Special Agent with the FBI, and have been since July 2010. Prior to my appointment as a Special Agent, I worked as an Intelligence Analyst with the FBI for approximately five years, addressing primarily counterintelligence and counterterrorism matters. As a Special Agent, I have been assigned to the Counterintelligence Division of the FBI's Washington Field Office since November 2010. 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 money laundering in furtherance of national security offenses. I have participated in obtaining both Electronic Communications Privacy Act (ECPA) search warrants and process involving email and ISPs.

#### SOURCE OF EVIDENCE

5. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation, and information from other



FBI personnel. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

#### STATUTORY AUTHORITY AND DEFINITIONS

6. Under 18 U.S.C. § 793(e), “[w]hoever having unauthorized possession of, access to, or control over any document . . . 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 do or causes the same “to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it” shall be fined or imprisoned not more than ten years, or both.

7. Under 18 U.S.C. § 793(f), “[w]hoever, being entrusted with or having lawful possession or control of any document . . . or information, relating to the national defense” either “(1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed,” or “(2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer” shall be fined or imprisoned not more than ten years, or both.

8. Under Executive Order 13526, information in any form may be classified if it: (1) is owned by, produced by or for, or is under the control of the United States government; (2) falls within one or more of the categories set forth in the Executive Order [Top Secret, Secret, and

Confidential]; 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.

9. Where such unauthorized disclosure could reasonably result in damage to the national security, the information may be classified as “Confidential” and must be properly safeguarded. Where such unauthorized disclosure could reasonably result in “serious” damage to the national security, the information may be classified as “Secret” and must be properly safeguarded. Where such unauthorized disclosure could reasonably result in “exceptionally grave” damage to the national security, the information may be classified as “Top Secret” and must be properly safeguarded.

10. Sensitive Compartmented Information (SCI) means classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems.

11. Special Intelligence, or “SI,” is an SCI control system designed to protect technical and intelligence information derived from the monitoring of foreign communications signals by other than the intended recipients. The SI control system protects SI-derived information and information relating to SI activities, capabilities, techniques, processes, and procedures.

12. Talent Keyhole, or “TK,” is an SCI control system designed to protect information and activities related to space-based collection of imagery, signals, measurement and signature intelligence, certain products, processing, and exploitation techniques, and the design, acquisition, and operation of reconnaissance satellites.

13. Controlled Imagery, or “IMCON,” is a dissemination caveat used to limit access

to or distribution of imagery information that is classified or otherwise restricted.

14. Classified information may be marked as “Not Releasable to Foreign Nationals/Governments/US Citizens,” abbreviated “NOFORN,” to indicate information that may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-U.S. citizens without permission of the originator.

15. Classified information may be marked as releasable to a specific country abbreviated “REL TO,” to indicate classified information that is authorized for release to one or more countries. “REL TO USA, AUS, CAN, GBR, NZL” identifies information releasable to the United States, Australia, Canada, Great Britain, and New Zealand.

16. Classified information, of any designation, may be shared only with persons determined by an appropriate United States government official to be eligible for access, and who possess a “need to know.” Among other requirements, in order for a person to obtain a security clearance allowing that person access to classified United States government information, that person is required to and must agree to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations. If a person is not eligible to receive classified information, classified information may not be disclosed to that person. In order for a foreign government to receive access to classified information, the originating United States agency must determine that such release is appropriate.

17. Pursuant to Executive Order 13526, classified information contained on automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information must

be maintained in a manner that: (1) prevents access by unauthorized persons; and (2) ensures the integrity of the information.

18. 32 C.F.R. Parts 2001 and 2003 regulate the handling of classified information. Specifically, 32 C.F.R. § 2001.43, titled "Storage," regulates the physical protection of classified information. This section prescribes that Secret and Top Secret information "shall be stored in a GSA-approved security container, a vault built to Federal Standard (FED STD) 832, or an open storage area constructed in accordance with § 2001.53." It also requires periodic inspection of the container and the use of an Intrusion Detection System, among other things.

#### PROBABLE CAUSE FOR SEARCH

19. As a result of a FOIA request, the State Department is currently reviewing approximately 30,490 email communications sent to or from @clintonemail.com, a domain that resided on a server used by former Secretary of State Hillary Rodham Clinton ("Clinton") to transmit, receive, and store email for a personal email account[s] she maintained. The FOIA process implemented by the State Department requires that these emails be reviewed by government agencies for classified information prior to public release. In July 2015, the Inspector General for the Intelligence Community reviewed a sample of approximately 300 emails. It has since been determined by the relevant original classification authorities that at least seven (7) of these emails contained classified information. Two (2) of the seven (7) emails contained information that was determined to be classified at the TOP SECRET level. Although not marked as classified, all seven (7) emails were determined to contain classified information at the time they were sent to Clinton and received at the @clintonemail.com domain, and the information in six (6) of the emails remains classified today.

20. Through written consent provided by Clinton's personal counsel, Williams &

Connolly LLP, the FBI obtained Clinton's server on which the @clintonemail.com domain resided, as well as physical and electronic copies of the 30,490 emails that Clinton, through her counsel, provided to the State Department for purposes of its FOIA review. In its review of these emails, the FBI found a copy of the electronic business card of Jacob "Jake" Sullivan, formerly Secretary Clinton's Deputy Chief of Staff for Policy from January 2009 to February 2011, and Director of Policy Planning from February 2011 to January 2013. Sullivan's electronic business card identified him as an employee of the Department of State through his business address and phone numbers, which are known to be associated with the State Department, and listed his personal email address as [REDACTED]@gmail.com.

21. On July 3, 2009, at 11:42 p.m., a State Department employee sent an email to three State Department email distribution lists and four additional State Department employees on the State Department's unclassified email system. This email contained information that has since been determined to be classified at the TOP SECRET//SI//TK//IMCON/REL TO USA, AUS, CAN, GBR, NZL level when it was sent and remains classified at this level to this date.

22. On July 4, 2009, at 12:13 a.m., the drafter of the July 3 email replied-all to the recipients of the original 11:42 p.m. email to clarify a few points. It appears that one of the recipients of the 12:13 a.m. email then replied-all at 2:03 a.m. At 7:35 a.m., it appears that one of the recipients of the 2:03 a.m. email forwarded the email to three individuals including Jacob Sullivan (and carbon copied a State Department email distribution list and another individual who were recipients of the original July 3 email). The 7:35 a.m. email was forwarded to both Jacob Sullivan's State Department email address and the SUBJECT ACCOUNT. Insofar as Google servers store and retain copies of email communications, the FBI has reason to believe TOP SECRET U.S. government information is being stored in an unauthorized manner.

23. The U.S. government's TOP SECRET//SI//TK//IMCON/REL TO USA, AUS, CAN, GBR, NZL classification of this email is significant insofar as it indicates that its unauthorized disclosure could result in "exceptionally grave" damage to national security. This email includes technical and intelligence information derived from the monitoring of foreign communications and information related to space-based collection of imagery, signals, measurement, and signature intelligence and therefore contains classified and national defense information. The REL TO USA, AUS, CAN, GBR, NZL caveat indicates classified intelligence that cannot be released in any form to any country other than the United States, Australia, Canada, Great Britain, and New Zealand.

24. Pursuant to the FBI's review of the 30,490 emails described above, at least 496 email communications containing the SUBJECT ACCOUNT have been identified. Out of the 496 emails, the FBI has identified several additional emails that it believes contain classified information, but these emails have not undergone a formal classification review.

25. I have probable cause to believe that the SUBJECT ACCOUNT contains classified information, which was produced by and is owned by the U.S. government. Such information is being stored in an unauthorized location and in an unauthorized manner. Accordingly, I am seeking the issuance of a warrant to search the SUBJECT ACCOUNT for items described in Attachment B.

#### BACKGROUND ON EMAIL

26. In my training and experience and based on information obtained from other law enforcement officers, I understand the following about email providers, such as Google:

- a. Google provides a variety of on-line services, including email access, to the public. Google allows subscribers to obtain email accounts at the domain

name gmail.com. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information.

- b. In addition to the account, subscriber, and IP address login/logout (session) information, which can assist in identifying who controls/uses the account and which computers or other devices were used to access the account (and when such access occurred), the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email).
- c. A Google subscriber can also store address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.
- d. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

- e. A subscriber may also store email on Google servers for which there is insufficient storage space in the subscriber's computer or which he does not wish to maintain on his own computer. A search of the email on a subscriber's "home" computer will not necessarily uncover the files, messages, and other information maintained by a subscriber on Google servers.

#### SEARCH PROCEDURE

27. This warrant will be executed in compliance with ECPA. Specifically, the warrant will require Google to disclose to the government a copy of the records and other information (including the content of communications, if any) described in Part I of Attachment B. Upon receipt of such information, the information described in Part III of Attachment B will be subject to seizure by law enforcement.

28. 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. See 18 U.S.C. § 2703(a), (b)(1)(A), and (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).

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

#### CONCLUSION

Based on the foregoing facts and circumstances, I submit that probable cause exists to believe that evidence, contraband, fruits and/or other items illegally possessed in violation of 18 U.S.C. § 793(e) and (f) are located in the SUBJECT ACCOUNT. Accordingly, I seek the issuance of a warrant to search the SUBJECT ACCOUNT for evidence, contraband, fruits,




and/or other items illegally possessed (more particularly described in Attachment B), in violation of 18 U.S.C. § 793(e) and (f).



Special Agent  
Federal Bureau of Investigation

Sworn to and subscribed before me this 17<sup>th</sup> day of September 2015.

                     /s/                        
John F. Anderson  
United States Magistrate Judge  
John F. Anderson  
United States Magistrate Judge

ATTACHMENT A

Property To Be Searched

This warrant applies to information associated with Google account [REDACTED], which is associated with the email address [REDACTED]@gmail.com ("SUBJECT ACCOUNT") that is stored at premises controlled by Google Inc., a company that does business and accepts process at 1600 Amphitheater Parkway, Mountain View, California 94043.

**ATTACHMENT B**

**Particular Things To Be Seized**

**I. Information To Be Disclosed by Google**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to requests made under 18 U.S.C. § 2703(f) on July 28, 2015 and August 18, 2015, Google is required to disclose the following information to the government for the SUBJECT ACCOUNT:

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

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

c. The types of service utilized;

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

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

## **II. Key Word Searches**

Law enforcement personnel will search the contents of email communications provided by Google to identify emails meeting the following criteria, which will be the emails reviewed pursuant to this search warrant:

a. Any email communications sent by the SUBJECT ACCOUNT to a .gov email address or sent to the SUBJECT ACCOUNT from a .gov email address, as well as any emails to or from the SUBJECT ACCOUNT on which a .gov email address was carbon copied or blind carbon copied;

b. Any email communications sent to or from the SUBJECT ACCOUNT containing prior emails from, to, or carbon copying a .gov email address;

c. Any email communications that contain any of the key words from a list of terms used by the FBI in this case. The FBI has developed a list of terms to include key words utilized to locate emails and files related to the improper transmission and storage of classified information on unclassified email systems and servers. The list of terms is subject to modification and is updated as necessary to reflect case developments.

### **III. Information To Be Seized by the Government**

All information described above in Section I that constitutes evidence, contraband, fruits, and/or other items illegally possessed in violation of 18 U.S.C. § 793(e) and (f), those violations occurring from January 2009 through January 2013, including, for the SUBJECT ACCOUNT, information pertaining to the following matters:

- a. Evidence indicating how and when the SUBJECT ACCOUNT was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the offenses under investigation and to the SUBJECT ACCOUNT owner; and
- b. The identity of the person(s) who communicated with the SUBJECT ACCOUNT about matters relating to the offenses under investigation, as described above.

# UNITED STATES DISTRICT COURT

for the  
Eastern District of Virginia

# UNDER SEAL

In the Matter of the Search of )  
(Briefly describe the property to be searched )  
or identify the person by name and address) )  
Information Associated With Email Account )  
[REDACTED]@Gmail.com That Is )  
Stored At Premises Controlled By Google, Inc. )

Case No. 1:16-SW- 331

## 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):

See Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Attachment B

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 July 4, 2016  
(not to exceed 14 days)

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 Michael S. Nachmanoff  
(name)

I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)  for \_\_\_\_\_ days (not to exceed 30).  
 until, the facts justifying, the later specific date of \_\_\_\_\_.

Date and time issued: 6/20/16 @ 3:31 p Michael S. Nachmanoff  
United States Magistrate Judge  
Judge's signature

City and state: Alexandria, Virginia Michael S. Nachmanoff, United States Magistrate Judge  
Printed name and title

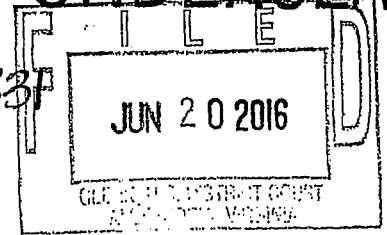
# UNITED STATES DISTRICT COURT

for the  
Eastern District of Virginia

# FILED UNDER SEAL

In the Matter of the Search of  
*(Briefly describe the property to be searched  
or identify the person by name and address)*  
Information Associated With Email Account  
[REDACTED]@Gmail.com That Is  
Stored At Premises Controlled By Google, Inc.

Case No. 1:16-SW-331



## 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)*:

See Attachment A

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

See Attachment B

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:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. 793(e);	Unlawful possession and communication of national defense information (NDI);
18 U.S.C. 793(f)	Unlawful removal or failure to report unlawful removal of NDI

The application is based on these facts:

- 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.

[REDACTED]

*Applicant's signature*

[REDACTED]

, Special Agent, FBI  
*Printed name and title*

Sworn to before me and signed in my presence.

Date: 06/20/2016

/s/ [Signature]  
Michael S. Nachmanoff  
United States Magistrate Judge

*Judge's signature*

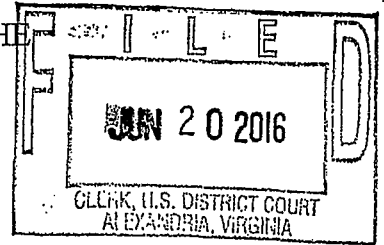
City and state: Alexandria, Virginia

Michael S. Nachmanoff, United States Magistrate Judge  
*Printed name and title*

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division



IN THE MATTER OF THE SEARCH OF )  
INFORMATION ASSOCIATED WITH )  
EMAIL ACCOUNT )  
[REDACTED]@GMAIL.COM )  
THAT IS STORED AT PREMISES )  
CONTROLLED BY GOOGLE, INC. )

UNDER SEAL

Case No. 1:16- 331

AFFIDAVIT IN SUPPORT OF A SEARCH AND SEIZURE WARRANT

I, [REDACTED], being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. The government is conducting a criminal investigation concerning the improper transmission and storage of classified information on unclassified email systems and servers. The investigation began as a result of a review of emails undertaken by the U.S. Department of State (State Department) in connection with Freedom of Information Act (FOIA) litigation. During this FOIA review, it was determined that certain emails containing classified information were sent and received on systems unauthorized for the transmission or storage of such information. On or about July 6, 2015, the Inspector General for the Intelligence Community notified the Federal Bureau of Investigation (FBI) of a potential compromise of classified information involving the emails discovered through the FOIA review. After an initial review of the matter, the FBI opened a criminal investigation to, among other things, identify any unauthorized systems which the emails in question have transited, identify any person(s) who may have introduced classified information onto unauthorized systems and all circumstances surrounding such introduction, identify any person(s) who may have transmitted information



over any such systems, and identify whether classified information has been compromised through computer intrusions or unauthorized access into these systems.

2. The FBI's investigation has established that emails containing classified information have been transmitted and stored on multiple forms of electronic media. One of the items identified as having contained such emails is a server which was used by former Secretary of State Hillary Rodham Clinton (Clinton) to transmit, receive, and store email for a personal email account or accounts she maintained. One domain on that server used by Clinton was @clintonemail.com.

3. The purpose of this affidavit is to secure a search and seizure warrant for the Google account [REDACTED] which is associated with the email address [REDACTED]@gmail.com (hereinafter the "SUBJECT ACCOUNT"), within the possession and control of the remote computing service and electronic communication service provider, also referred to as an Internet Service Provider or "ISP," known as Google, Inc. (Google), more fully described in Attachment A. There is probable cause to believe that the SUBJECT ACCOUNT contains evidence, contraband, fruits and/or other items illegally possessed in violation of 18 U.S.C. § 793(e) and (f).

4. The search warrant is sought under 18 U.S.C. § 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google to disclose to the government records and other information in their possession, pertaining to the subscriber(s) or customer(s) associated with the SUBJECT ACCOUNT, including contents of electronic communications.

5. I am a Special Agent with the FBI, and have been since June 1998. As a Special Agent, I have been assigned to the Criminal, Counterterrorism, and Counterintelligence Divisions of the FBI's Washington Field Office. From 2010 to 2015, I served as a Supervisory

Special Agent in the International Operations Division at FBI Headquarters and in Milan, Italy, where I supported Counterintelligence operations. In January 2015, I was assigned to the Counterintelligence Division in the Washington Field Office as a Supervisory Special Agent 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 money laundering in furtherance of national security offenses.

#### SOURCE OF EVIDENCE

6. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation, and information from other FBI and U.S. Government personnel. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

#### STATUTORY AUTHORITY AND DEFINITIONS

7. Under 18 U.S.C. § 793(e), “[w]hoever having unauthorized possession of, access to, or control over any document . . . 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 do or causes the same “to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it” shall be fined or imprisoned not more than ten years, or both.

8. Under 18 U.S.C. § 793(f), “[w]hoever, being entrusted with or having lawful possession or control of any document . . . or information, relating to the national defense” either

“(1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed,” or  
“(2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer” shall be fined or imprisoned not more than ten years, or both.

9. Under Executive Order 13526, information in any form may be classified if it: (1) is owned by, produced by or for, or is under the control of the United States government; (2) falls within one or more of the categories set forth in the Executive Order [Top Secret, Secret, and Confidential]; 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.

10. Where such unauthorized disclosure could reasonably result in damage to the national security, the information may be classified as “Confidential” and must be properly safeguarded. Where such unauthorized disclosure could reasonably result in serious damage to the national security, the information may be classified as “Secret” and must be properly safeguarded. Where such unauthorized disclosure could reasonably result in exceptionally grave damage to the national security, the information may be classified as “Top Secret” and must be properly safeguarded.

11. Sensitive Compartmented Information (SCI) means classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems.

12. Classified information, of any designation, may be shared only with persons

determined by an appropriate United States government official to be eligible for access, and who possess a “need to know.” Among other requirements, in order for a person to obtain a security clearance allowing that person access to classified United States government information, that person is required to and must agree to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations. If a person is not eligible to receive classified information, classified information may not be disclosed to that person. In order for a foreign government to receive access to classified information, the originating United States agency must determine that such release is appropriate.

13. Pursuant to Executive Order 13526, classified information contained on automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information must be maintained in a manner that: (1) prevents access by unauthorized persons; and (2) ensures the integrity of the information.

14. 32 C.F.R. Parts 2001 and 2003 regulate the handling of classified information. Specifically, 32 C.F.R. § 2001.43, titled “Storage,” regulates the physical protection of classified information. This section prescribes that Secret and Top Secret information “shall be stored in a GSA-approved security container, a vault built to Federal Standard (FED STD) 832, or an open storage area constructed in accordance with § 2001.53.” It also requires periodic inspection of the container and the use of an Intrusion Detection System, among other things.

## PROBABLE CAUSE FOR SEARCH

15. Clinton served as the Secretary of State from on or about January 21, 2009 to on or about February 1, 2013. On or about March 9, 2009, Clinton began using a private email server (Server 1) to transmit, receive, and store email for a personal email account she maintained. One domain on Server 1 was @clintonemail.com. From March 2009 to June 2013, Server 1 was housed at Clinton's residence in Chappaqua, New York.

16. In June 2013, Clinton retained Platte River Networks (PRN), a Denver, Colorado-based information technology firm, to establish and administer a new email server (Server 2) to replace Server 1. On or about June 22, 2013, PRN installed and set up Server 2 at Equinix, a datacenter located in Secaucus, New Jersey. Based upon interviews and a review of the business records produced by PRN pursuant to a grand jury subpoena, the FBI determined that shortly after PRN took control of Server 1 in June 2013, PRN transferred all email accounts and associated data from Server 1 to Server 2. Server 1 and Server 2, regardless of their physical location(s), were not devices authorized by the United States government to store or transmit classified or national defense information.

17. Based upon a records request, Clinton produced to the State Department approximately 30,490 email communications sent to or from Clinton at the @clintonemail.com domain that resided on Server 1 and Server 2. As a result of a FOIA request, the State Department ultimately reviewed these 30,490 emails. The FOIA process implemented by the State Department required that these emails be reviewed by government agencies for classified information prior to public release. In February 2016, the State Department completed its review and determined that 2,115 of the 30,490 emails contain information that is presently classified.

18. The State Department released 2,093 of the emails containing classified

information to the public in redacted form beginning in May 2015 and ending in February 2016. According to the relevant original classification authorities, 2,028 contained information classified as Confidential and 65 contained information classified as Secret. In addition, the State Department determined that 22 emails containing information classified at the Top Secret level, as determined by the relevant original classification authorities, would be withheld in their entirety from public release.

19. The U.S. Government's determination that 2,028 emails contain information classified at the Confidential level is significant because it means that the unauthorized disclosure of those emails could result in damage to national security. The U.S. Government's determination that 65 emails contain information classified at the Secret level is significant because it means that the unauthorized disclosure of those emails could result in serious damage to national security. The U.S. Government's determination that 22 emails contain information classified at the Top Secret level is significant because it means that the unauthorized disclosure of those emails could result in exceptionally grave damage to national security.

20. In or about July 2015, the FBI initiated a criminal investigation into the possible mishandling and compromise of national security information from unauthorized electronic communications systems. As part of the investigation, the FBI has obtained private server equipment and related devices used by Clinton and her staff during her tenure as Secretary of State. The FBI's review of this material identified emails that were later determined by the relevant original classification authorities to contain information classified up to the Top Secret/Sensitive Compartmented Information level.

21. Clinton's personal counsel for purposes of the present investigation, Williams & Connolly LLP, provided written consent to the Department of Justice for the FBI to obtain

Server 1 and Server 2 as well as physical and electronic copies of the 30,490 emails that Clinton, through her counsel, had previously provided to the State Department.

22. Pursuant to the FBI's review of the 30,490 @clintonemail.com emails described above, the FBI determined that a large portion of the emails contained metadata displaying the SUBJECT ACCOUNT. According to subpoena returns from Google, the SUBJECT ACCOUNT is associated with PRN employee Paul Combetta.

23. In a recent interview, Combetta informed the FBI that he used the SUBJECT ACCOUNT to facilitate the transfer of archived Clinton emails to Server 2 from a laptop belonging to a former State Department employee who worked on Clinton's staff. The FBI believes these archived emails included emails from the original set provided to the State Department --- and subsequently to the FBI --- by Williams & Connolly. As noted above, these emails include information that has since been determined to be classified.

24. Based upon an order obtained pursuant to 18 U.S.C. § 2703(d), the FBI determined that 820 @clintonemail.com emails, dated within the time frame October 25, 2010 to December 31, 2010, are currently present in the SUBJECT ACCOUNT. Out of the 820 emails, the FBI identified 57 emails that have been determined by the relevant original classification authorities to contain information currently classified at the Confidential level. The FBI has confirmed that at least one of the 57 emails contained information that, although not marked as such, was classified at the Secret level at the time the email was sent. The original classification authorities did not make a determination as to whether the information in the remaining 56 emails was classified at the time that the emails were sent to or from Clinton at the @clintonemail.com domain. As part of its investigation, the FBI has sought a determination by the relevant original classification authorities as to whether these emails contained classified

information at the time they were sent. That request is currently pending.

25. I have probable cause to believe that the SUBJECT ACCOUNT contains information classified at the Confidential level, which was produced by and is owned by the U.S. Government. Such information is being stored in an unauthorized location and in an unauthorized manner. Accordingly, I am seeking the issuance of a warrant to search the SUBJECT ACCOUNT for items described in Attachment B.

#### BACKGROUND ON EMAIL

26. In my training and experience and based on information obtained from other law enforcement officers, I understand the following about email providers, such as Google:

- a. Google provides a variety of on-line services, including email access, to the public. Google allows subscribers to obtain email accounts at the domain name gmail.com. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information.
- b. In addition to the account, subscriber, and IP address login/logout (session) information, which can assist in identifying who controls/uses the account and which computers or other devices were used to access the account (and when such access occurred), the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email).
- c. A Google subscriber can also store address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books,



contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

- d. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

27. A subscriber may store email, for example, on Google servers for which there is insufficient storage space in the subscriber's computer or which he does not wish to maintain on his own computer. A search of the email on a subscriber's "home" computer will not necessarily uncover the files, messages, and other information maintained by a subscriber on Google servers.

#### SEARCH PROCEDURE

28. This warrant will be executed in compliance with ECPA. Specifically, the warrant will require Google to disclose to the government a copy of the records and other information (including the content of communications, if any) described in Part I of Attachment B. Upon receipt of such information, the information described in Part III of Attachment B will be subject to search by law enforcement.

29. 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. See 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).

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

CONCLUSION

Based on the foregoing facts and circumstances, I submit that probable cause exists to believe that evidence, contraband, fruits and/or other items illegally possessed in violation of 18 U.S.C. § 793(e) and (f) are located in the SUBJECT ACCOUNT. Accordingly, I seek the issuance of a warrant to search the SUBJECT ACCOUNT for evidence, contraband, fruits, and/or other items illegally possessed (more particularly described in Attachment B), in violation of 18 U.S.C. § 793(e) and (f).

  
Supervisory Special Agent  
Federal Bureau of Investigation

Sworn to and subscribed before me this 21<sup>st</sup> day of June, 2016.

\_\_\_\_\_/s/\_\_\_\_\_  
Michael S. Nachmanoff  
United States Magistrate Judge

\_\_\_\_\_  
Michael S. Nachmanoff  
United States Magistrate Judge

ATTACHMENT A

Property To Be Searched

This warrant applies to information associated with Google account [REDACTED], which is associated with the email address [REDACTED]@gmail.com ("SUBJECT ACCOUNT") that is stored at premises controlled by Google Inc., a company that does business and accepts process at 1600 Amphitheater Parkway, Mountain View, California 94043.

ATTACHMENT B

Particular Things To Be Seized

I. Information To Be Disclosed by Google

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to requests made under 18 U.S.C. § 2703(f) on February 22, 2015 and June 3, 2016, Google is required to disclose the following information to the government for the SUBJECT ACCOUNT:

- a. The contents of all emails associated with the SUBJECT ACCOUNT, including stored or preserved copies of emails sent to and from the SUBJECT ACCOUNT, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the SUBJECT ACCOUNT, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;

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

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

## II. Key Word Searches

Law enforcement personnel will search the contents of email communications, for the time period October 25, 2010 to December 31, 2010, provided by Google to identify emails meeting the following criteria, which will be the emails reviewed pursuant to this search warrant:

a. Any email communications sent by the SUBJECT ACCOUNT to a .gov email address or sent to the SUBJECT ACCOUNT from a .gov email address, as well as any emails to or from the SUBJECT ACCOUNT on which a .gov email address was carbon copied or blind carbon copied;

b. Any email communications sent to or from the SUBJECT ACCOUNT containing prior emails from, to, or carbon copying a .gov email address;

c. Any email communications sent to or from the SUBJECT ACCOUNT containing prior emails from, to, or carbon copying a @clintonemail.com email address;

d. Any email communications that contain any of the key words from a list of terms used by the FBI in this case. The FBI has developed a list of terms to include key words utilized to locate emails and files related to the improper transmission and storage of classified

information on unclassified email systems and servers. The list of terms is subject to modification and is updated as necessary to reflect case developments.

### III. Information To Be Seized by the Government

All information described above in Section I that constitutes evidence, contraband, fruits, and/or other items illegally possessed in violation of 18 U.S.C. § 793(e) and (f), those violations occurring from October 25, 2010 to December 31, 2010, including, for the SUBJECT ACCOUNT, information pertaining to the following matters:

- a. Evidence indicating how and when the SUBJECT ACCOUNT was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the offenses under investigation and to the SUBJECT ACCOUNT owner;
- b. The identity of the person(s) who communicated with the SUBJECT ACCOUNT about matters relating to the offenses under investigation, as described above.

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

MAR 18 2016

\_\_\_\_\_  
)  
IN RE APPLICATION OF THE )  
UNITED STATES OF AMERICA FOR )  
AN ORDER PURSUANT TO )  
18 U.S.C. § 2703(d) TO GOOGLE, INC., )  
AN INTERNET SERVICE PROVIDER )

Misc. No. 1:16-ec-365

**Filed Under Seal**

APPLICATION OF THE UNITED STATES  
FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)

The United States of America, moving by and through its undersigned counsel, respectfully submits under seal this *ex parte* application for an Order pursuant to 18 U.S.C. § 2703(d). The proposed Order would require Google, Inc., an Internet Service Provider located in Mountain View, CA, to disclose certain records and other information pertaining to the email account [REDACTED]@gmail.com. The records and other information to be disclosed are described in Attachment A to the proposed Order. In support of this application, the United States asserts:

LEGAL BACKGROUND

1. Google, Inc. is a provider of an electronic communications service, as defined in 18 U.S.C. § 2510(15), and/or a remote computing service, as defined in 18 U.S.C. § 2711(2). Accordingly, the United States may use a court order issued under § 2703(d) to require Google, Inc. to disclose the items described in Part II of Attachment A. *See* 18 U.S.C. § 2703(c)(2) (Part II.A of Attachment A); 18 U.S.C. § 2703(c)(1) (Part II.B of Attachment A).

2. This Court has jurisdiction to issue the proposed Order because it is “a court of competent jurisdiction,” as defined in 18 U.S.C. § 2711. *See* 18 U.S.C. § 2703(d). Specifically,

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

3. A court order under § 2703(d) “shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d). Accordingly, the next section of this application sets forth specific and articulable facts showing that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation.

#### THE RELEVANT FACTS

4. The government is conducting a criminal investigation concerning the improper transmission and storage of classified information on unclassified email systems and servers, in violation of Title 18, United States Code, Sections 793(e) and (f). The investigation began as a result of a review of emails undertaken by the U.S. Department of State in connection with Freedom of Information Act (FOIA) litigation. During this FOIA review, it was determined that certain emails containing classified information were sent and received on systems unauthorized for the transmission or storage of such information. On or about July 6, 2015, the Inspector General for the Intelligence Community notified the Federal Bureau of Investigation (FBI) of a potential compromise of classified information involving the emails discovered through the FOIA review. After an initial review of the matter, the FBI opened a criminal investigation to, among other things, identify any unauthorized systems which the emails in question have transited, identify any person(s) who may have introduced classified information onto



unauthorized systems and all circumstances surrounding such introduction, and identify any person(s) who may have transmitted such information over any such systems.

5. The FBI's investigation has established that the emails containing classified information have been transmitted and stored on multiple forms of electronic media. One of the items identified as having contained such emails is a server which was used by former Secretary of State Hillary Rodham Clinton ("Clinton") to transmit, receive, and store email for a personal email account or accounts she maintained. One domain on that server used by Clinton was @clintonemail.com.

6. Clinton's personal counsel, Williams & Connolly, LLP, voluntarily produced to the FBI, in a PST file,<sup>1</sup> over 30,000 emails sent to or from the @clintonemail.com domain, some of which have been confirmed to include information classified by the United States Government. During a review of these emails, the FBI discovered a large portion of emails carrying metadata displaying the email address [REDACTED]@gmail.com ("Subject Account"). According to subpoena returns from Google, the Subject Account is associated with Paul Combetta, who is an employee of Platte River Networks ("PRN"), a Denver, Colorado-based information technology firm that managed a server for Clinton beginning in June 2013.

7. In a recent interview, Combetta informed the FBI that he used the Subject Account to facilitate the transfer of Clinton archived emails to a PRN exchange server from a laptop belonging to a State Department staffer for the former Secretary. The FBI believes these archived emails included emails from the original dataset provided to the FBI by Williams & Connolly. In addition, as indicated above, the Subject Account appears in the metadata of the @clintonemail.com emails provided to the FBI by Williams & Connolly, which includes

---

<sup>1</sup> A PST (Personal Storage Table) file, often designated as .pst, is used to store Microsoft Outlook email messages and other data items on a local computer.

confirmed classified emails.

8. Based on the FBI's investigation, there is reason to believe that the Subject Account contains evidence related to the unlawful storage and transmission of classified information from the beginning of Clinton's tenure as Secretary of State on January 21, 2009, to the present.

#### REQUEST FOR ORDER

9. The facts set forth in the previous section show that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation. Specifically, a review of these items for the time period January 21, 2009 to the present will help the FBI determine if any @clintonemail.com emails, including confirmed classified emails, from Clinton's tenure at the State Department, reside within the Subject Account. Accordingly, the United States requests that Google, Inc. be directed to produce all items described in Part II of Attachment A to the proposed Order.

10. The United States further requests that the Order require Google, Inc. not to notify any person, including the subscribers or customers of the account(s) listed in Part I of Attachment A, of the existence of the Order until further order of the Court. *See* 18 U.S.C. § 2705(b). This Court has authority under 18 U.S.C. § 2705(b) to issue "an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order." *Id.* In this case, such an order would be appropriate because the requested Order relates to an ongoing criminal investigation that is neither public nor known to all of the subjects of the investigation, and its

disclosure may alert subjects to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the requested Order will seriously jeopardize the investigation, including by giving subjects an opportunity to destroy or tamper with evidence, or otherwise seriously jeopardize an ongoing investigation. *See* 18 U.S.C. § 2705(b)(3), (5). Because much of the evidence in this investigation is stored electronically, if alerted to the investigation, subjects could destroy that evidence, including information saved to personal computers.

11. The United States further requests that the Court order that this application and any resulting order be sealed until further order of the Court. As explained above, these documents discuss an ongoing criminal investigation that is neither public nor known to all of the subjects of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

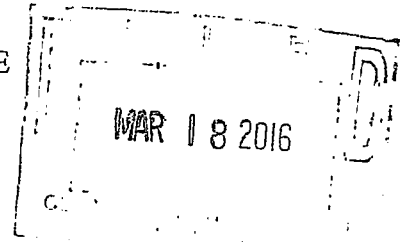
Dana J. Boente  
United States Attorney

By:

Assistant United States Attorney

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



\_\_\_\_\_  
)  
IN RE APPLICATION OF THE )  
UNITED STATES OF AMERICA FOR )  
AN ORDER PURSUANT TO )  
18 U.S.C. § 2703(d) TO GOOGLE, INC., )  
AN INTERNET SERVICE PROVIDER )

Misc. No. 1:16-ec-365

**Filed Under Seal**

ORDER

The United States has submitted an application pursuant to 18 U.S.C. § 2703(d), requesting that the Court issue an Order requiring Google, Inc., an electronic communications service provider and/or a remote computing service located in Mountain View, CA, to disclose the records and other information described in Attachment A to this Order.

The Court finds that the United States has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

The Court determines that there is reason to believe that notification of the existence of this Order will seriously jeopardize the ongoing investigation, including by giving subjects an opportunity to destroy or tamper with evidence, or otherwise seriously jeopardize an ongoing investigation. *See* 18 U.S.C. § 2705(b)(3), (5).

IT IS THEREFORE ORDERED, pursuant to 18 U.S.C. § 2703(d), that Google, Inc. shall, within ten days of the date of this Order, disclose to the United States the records and other information described in Attachment A to this Order.

IT IS FURTHER ORDERED that Google, Inc. shall not disclose the existence of the application of the United States, or the existence of this Order of the Court, to the subscriber(s) of the account listed in Attachment A, or to any other person, unless and until otherwise authorized to do so by the Court, except that Google, Inc. may disclose this Order to an attorney for Google, Inc. for the purpose of receiving legal advice.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court.

\_\_\_\_\_/s/ JFA  
John F. Anderson  
United States Magistrate Judge  
John F. Anderson  
United States Magistrate Judge

Date: MARCH 18, 2016

At Alexandria, Virginia

A TRUE COPY, TESTE:  
CLERK, U.S. DISTRICT COURT

BY Marian J. [Signature]  
DEPUTY CLERK

## ATTACHMENT A

### I. The Account(s)

The Order applies to certain records and information associated with the following email account: [REDACTED]@gmail.com.

### II. Records and Other Information to Be Disclosed

Google, Inc. is required to disclose the following records and other information, if available, to the United States for each account or identifier listed in Part I of this Attachment ("Account"), for the time period from January 21, 2009 to the present:

- A. The following information about the customers or subscribers of the Account:
  - 1. Names (including subscriber names, user names, and screen names);
  - 2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
  - 3. Local and long distance telephone connection records;
  - 4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
  - 5. Length of service (including start date) and types of service utilized;
  - 6. Telephone or instrument numbers (including MAC addresses);
  - 7. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
  - 8. Means and source of payment for such service (including any credit card or bank account number) and billing records.
  
- B. All records and other information (not including the contents of communications) relating to the Account, including:
  - 1. Records of user activity for each connection made to or from the Account, including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; and source and destination Internet Protocol addresses;
  
  - 2. Information about each communication sent or received by the Account, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers).

**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

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

\_\_\_\_\_  
IN RE APPLICATION OF THE )  
UNITED STATES OF AMERICA FOR )  
AN ORDER PURSUANT TO )  
18 U.S.C. § 2703(d) TO GOOGLE, INC., )  
AN INTERNET SERVICE PROVIDER )

Misc. No. 1:16-ec-727

**Filed Under Seal**

APPLICATION OF THE UNITED STATES  
FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)

The United States of America, moving by and through its undersigned counsel, respectfully submits under seal this *ex parte* application for an Order pursuant to 18 U.S.C. § 2703(d). The proposed Order would require Google, Inc., an Internet Service Provider located in Mountain View, CA, to disclose certain records and other information pertaining to email account [REDACTED]@gmail.com. The records and other information to be disclosed are described in Attachment A to the proposed Order. In support of this application, the United States asserts:

LEGAL BACKGROUND

1. Google, Inc. is a provider of an electronic communications service, as defined in 18 U.S.C. § 2510(15), and/or a remote computing service, as defined in 18 U.S.C. § 2711(2). Accordingly, the United States may use a court order issued under § 2703(d) to require Google, Inc. to disclose the items described in Part II of Attachment A. *See* 18 U.S.C. § 2703(c)(2) (Part II.A of Attachment A); 18 U.S.C. § 2703(c)(1) (Part II.B of Attachment A).

2. This Court has jurisdiction to issue the proposed Order because it is “a court of competent jurisdiction,” as defined in 18 U.S.C. § 2711. *See* 18 U.S.C. § 2703(d). Specifically,



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

3. A court order under § 2703(d) “shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d). Accordingly, the next section of this application sets forth specific and articulable facts showing that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation.

#### THE RELEVANT FACTS

4. The government is conducting a criminal investigation concerning the improper transmission and storage of classified information on unclassified email systems and servers, in violation of Title 18, United States Code, Sections 793(e) and (f). The investigation began as a result of a review of emails undertaken by the U.S. Department of State in connection with Freedom of Information Act (FOIA) litigation. During this FOIA review, it was determined that certain emails containing classified information were sent and received on systems unauthorized for the transmission or storage of such information. On or about July 6, 2015, the Inspector General for the Intelligence Community notified the Federal Bureau of Investigation (FBI) of a potential compromise of classified information involving the emails discovered through the FOIA review. After an initial review of the matter, the FBI opened a criminal investigation to, among other things, identify any unauthorized systems which the emails in question have transited, identify any person(s) who may have introduced classified information onto

unauthorized systems and all circumstances surrounding such introduction, and identify any person(s) who may have transmitted such information over any such systems.

5. From January 21, 2009 to March 1, 2013, [REDACTED] was employed at the U.S. Department of State, first as Senior Advisor to Secretary of State Hillary Rodham Clinton, and later as Deputy Assistant Secretary of State. During this time, [REDACTED] is known to have maintained a personal email account, [REDACTED]@gmail.com (“Subject Account”), in addition to any official Department of State accounts he may have used. The Subject Account was not authorized for the transmission or storage of classified information.

6. The investigation has revealed that on or about March 21, 2009, an email was sent from the Subject Account that the CIA has determined, in a subsequent classification review, to be classified at the SECRET//NOFORN<sup>1</sup> level at the time the email was sent.

7. Based on the FBI’s investigation, there is reason to believe that the Subject Account contains evidence related to the unlawful transmission and storage of classified information on unclassified email systems and servers during [REDACTED] tenure at the U.S. Department of State.

#### REQUEST FOR ORDER

8. The facts set forth in the previous section show that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation. Specifically, a review of these items will help the FBI determine if the aforementioned email still resides within the Subject Account maintained by [REDACTED] and whether there are other records connecting email accounts

---

<sup>1</sup> Classified information may be marked as “Not Releasable to Foreign Nationals/Governments/US Citizens,” abbreviated “NOFORN,” to indicate information that may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-U.S. citizens without permission of the originator.

associated with the improper transmission and storage of classified information to the Subject Account. Accordingly, the United States requests that Google, Inc. be directed to produce all items described in Part II of Attachment A to the proposed Order.

9. The United States further requests that the Order require Google, Inc. not to notify any person, including the subscribers or customers of the account(s) listed in Part I of Attachment A, of the existence of the Order until further order of the Court. *See* 18 U.S.C. § 2705(b). This Court has authority under 18 U.S.C. § 2705(b) to issue “an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order.” *Id.* In this case, such an order would be appropriate because the requested Order relates to an ongoing criminal investigation involving email evidence that is not known to all of the subjects of the investigation, and its disclosure may alert subjects to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the requested Order will seriously jeopardize the investigation, including by giving subjects an opportunity to destroy or tamper with evidence, or otherwise seriously jeopardize an ongoing investigation. *See* 18 U.S.C. § 2705(b)(3), (5). Because much of the evidence in this investigation is stored electronically, if alerted to the investigation, subjects could destroy that evidence, including information saved to personal computers.

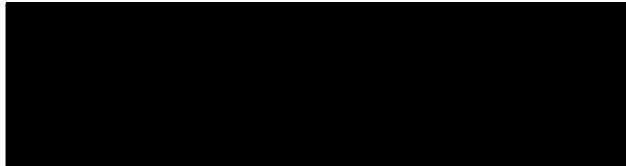
10. The United States further requests that the Court order that this application and any resulting order be sealed until further order of the Court. As explained above, these documents discuss an ongoing criminal investigation that is neither public nor known to all of

the subjects of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

Dana J. Boente  
United States Attorney

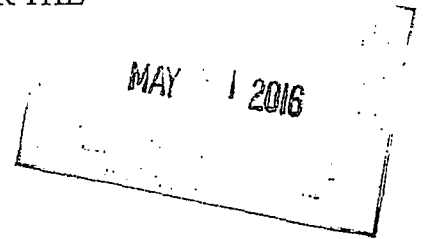
By:



Assistant United States Attorney

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



\_\_\_\_\_  
)  
IN RE APPLICATION OF THE )  
UNITED STATES OF AMERICA FOR )  
AN ORDER PURSUANT TO )  
18 U.S.C. § 2703(d) TO GOOGLE, INC., )  
AN INTERNET SERVICE PROVIDER )

Misc. No. 1:16-ec- 727

**Filed Under Seal**

ORDER

The United States has submitted an application pursuant to 18 U.S.C. § 2703(d), requesting that the Court issue an Order requiring Google, Inc., an electronic communications service provider and/or a remote computing service located in Mountain View, CA, to disclose the records and other information described in Attachment A to this Order.


The Court finds that the United States has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

The Court determines that there is reason to believe that notification of the existence of this Order will seriously jeopardize the ongoing investigation, including by giving subjects an opportunity to destroy or tamper with evidence, or otherwise seriously jeopardize an ongoing investigation. *See* 18 U.S.C. § 2705(b)(3), (5).

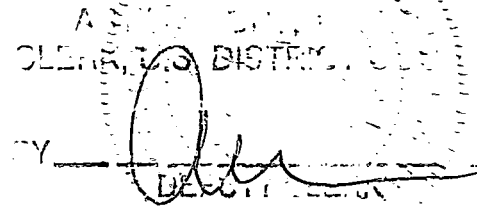
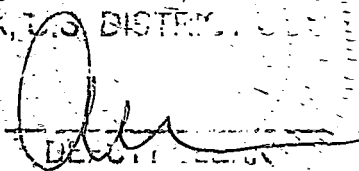
IT IS THEREFORE ORDERED, pursuant to 18 U.S.C. § 2703(d), that Google, Inc. shall, within ten days of the date of this Order, disclose to the United States the records and other information described in Attachment A to this Order.

IT IS FURTHER ORDERED that Google, Inc. shall not disclose the existence of the application of the United States, or the existence of this Order of the Court, to the subscriber(s) of the account listed in Attachment A, or to any other person, unless and until otherwise authorized to do so by the Court, except that Google, Inc. may disclose this Order to an attorney for Google, Inc. for the purpose of receiving legal advice.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court.

  
\_\_\_\_\_  
/s/  
Theresa Carroll Buchanan  
United States Magistrate Judge  
\_\_\_\_\_  
Theresa Carroll Buchanan  
United States Magistrate Judge

Date: 5/31/16  
At Alexandria, Virginia

  
CLERK, U.S. DISTRICT COURT  
BY 

## ATTACHMENT A

### I. The Account(s)

The Order applies to certain records and information associated with the following email account: [REDACTED]@gmail.com.

### II. Records and Other Information to Be Disclosed

Google, Inc. is required to disclose the following records and other information, if available, to the United States for each account or identifier listed in Part I of this Attachment ("Account"), for the time period from January 21, 2009 to March 1, 2013:

- A. The following information about the customers or subscribers of the Account:
  - 1. Names (including subscriber names, user names, and screen names);
  - 2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
  - 3. Local and long distance telephone connection records;
  - 4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
  - 5. Length of service (including start date) and types of service utilized;
  - 6. Telephone or instrument numbers (including MAC addresses);
  - 7. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
  - 8. Means and source of payment for such service (including any credit card or bank account number) and billing records.
  
- B. All records and other information (not including the contents of communications) relating to the Account, including:
  - 1. Records of user activity for each connection made to or from the Account, including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; and source and destination Internet Protocol addresses;
  - 2. Information about each communication sent or received by the Account, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers).

**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



IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

MAY 31 2016

\_\_\_\_\_  
)  
IN RE APPLICATION OF THE )  
UNITED STATES OF AMERICA FOR )  
AN ORDER PURSUANT TO )  
18 U.S.C. § 2703(d) TO GOOGLE, INC., )  
AN INTERNET SERVICE PROVIDER )

Misc. No. 1:16-ec-728

**Filed Under Seal**

APPLICATION OF THE UNITED STATES  
FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)

The United States of America, moving by and through its undersigned counsel, respectfully submits under seal this *ex parte* application for an Order pursuant to 18 U.S.C. § 2703(d). The proposed Order would require Google, Inc., an Internet Service Provider located in Mountain View, CA, to disclose certain records and other information pertaining to email account [REDACTED]@gmail.com. The records and other information to be disclosed are described in Attachment A to the proposed Order. In support of this application, the United States asserts:

LEGAL BACKGROUND

1. Google, Inc. is a provider of an electronic communications service, as defined in 18 U.S.C. § 2510(15), and/or a remote computing service, as defined in 18 U.S.C. § 2711(2). Accordingly, the United States may use a court order issued under § 2703(d) to require Google, Inc. to disclose the items described in Part II of Attachment A. *See* 18 U.S.C. § 2703(c)(2) (Part II.A of Attachment A); 18 U.S.C. § 2703(c)(1) (Part II.B of Attachment A).
2. This Court has jurisdiction to issue the proposed Order because it is “a court of competent jurisdiction,” as defined in 18 U.S.C. § 2711. *See* 18 U.S.C. § 2703(d). Specifically,

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

3. A court order under § 2703(d) “shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d). Accordingly, the next section of this application sets forth specific and articulable facts showing that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation.

#### THE RELEVANT FACTS

4. The government is conducting a criminal investigation concerning the improper transmission and storage of classified information on unclassified email systems and servers, in violation of Title 18, United States Code, Sections 793(e) and (f). The investigation began as a result of a review of emails undertaken by the U.S. Department of State in connection with Freedom of Information Act (FOIA) litigation. During this FOIA review, it was determined that certain emails containing classified information were sent and received on systems unauthorized for the transmission or storage of such information. On or about July 6, 2015, the Inspector General for the Intelligence Community notified the Federal Bureau of Investigation (FBI) of a potential compromise of classified information involving the emails discovered through the FOIA review. After an initial review of the matter, the FBI opened a criminal investigation to, among other things, identify any unauthorized systems which the emails in question have transited, identify any person(s) who may have introduced classified information onto

unauthorized systems and all circumstances surrounding such introduction, and identify any person(s) who may have transmitted such information over any such systems.

5. In the course of this investigation, the FBI learned that on or about March 12, 2011, a classified email was sent from the private, non-secure account [REDACTED]@gmail.com ("Subject Account"). According to the email's signature block, [REDACTED] is the user of the Subject Account. [REDACTED] is believed to reside in Japan, based on his Japan-based telephone number and physical address. A search of relevant databases reveals no U.S. Government security clearances for this individual. Furthermore, the Subject Account was not authorized for the transmission or storage of classified information.

6. The National Geospatial-Intelligence Agency (NGA) has determined, in a subsequent classification review, that this March 12, 2011 email sent from the Subject Account was classified at the SECRET//NOFORN<sup>1</sup> level at the time the email was sent.

7. Once the March 12, 2011 email was sent from the Subject Account, it transited through two private, non-secure email accounts before being forwarded to the private gmail account of Cheryl Mills, who at this time was employed at the U.S. Department of State as Counselor and Chief of Staff to Secretary of State Hillary Rodham Clinton. The email was then forwarded from Mills' gmail account to her Department of State account, and from there it was forwarded to Secretary Clinton's private email account.

8. Based on the FBI's investigation, there is reason to believe that the Subject Account contains evidence related to the unlawful transmission and storage of classified information on unclassified email systems and servers.

---

<sup>1</sup> Classified information may be marked as "Not Releasable to Foreign Nationals/Governments/US Citizens," abbreviated "NOFORN," to indicate information that may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-U.S. citizens without permission of the originator.

## REQUEST FOR ORDER

9. The facts set forth in the previous section show that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation. Specifically, a review of these items for the time period February 12, 2011 to April 12, 2011 will help the FBI determine if emails believed to contain classified information still reside within the Subject Account and whether there are other records connecting email accounts associated with the improper transmission and storage of classified information to the Subject Account. Accordingly, the United States requests that Google, Inc. be directed to produce all items described in Part II of Attachment A to the proposed Order.

10. The United States further requests that the Order require Google, Inc. not to notify any person, including the subscribers or customers of the account(s) listed in Part I of Attachment A, of the existence of the Order until further order of the Court. *See* 18 U.S.C. § 2705(b). This Court has authority under 18 U.S.C. § 2705(b) to issue “an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order.” *Id.* In this case, such an order would be appropriate because the requested Order relates to an ongoing criminal investigation involving email evidence that is not known to all of the subjects of the investigation, and its disclosure may alert subjects to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the requested Order will seriously jeopardize the investigation, including by giving subjects an opportunity to destroy or tamper with evidence, or otherwise seriously jeopardize an ongoing investigation. *See* 18 U.S.C. §

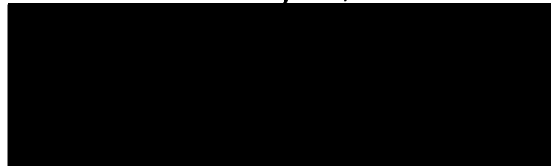
2705(b)(3), (5). Because much of the evidence in this investigation is stored electronically, if alerted to the investigation, subjects could destroy that evidence, including information saved to personal computers.

11. The United States further requests that the Court order that this application and any resulting order be sealed until further order of the Court. As explained above, these documents discuss an ongoing criminal investigation that is neither public nor known to all of the subjects of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

Dana J. Boente  
United States Attorney

By:

A large black rectangular redaction box covering the signature of the Assistant United States Attorney.

Assistant United States Attorney

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

MAY 1 2016

\_\_\_\_\_)  
IN RE APPLICATION OF THE )  
UNITED STATES OF AMERICA FOR )  
AN ORDER PURSUANT TO )  
18 U.S.C. § 2703(d) TO GOOGLE, INC., )  
AN INTERNET SERVICE PROVIDER )

Misc. No. 1:16-ec- 728

**Filed Under Seal**

ORDER

The United States has submitted an application pursuant to 18 U.S.C. § 2703(d), requesting that the Court issue an Order requiring Google, Inc., an electronic communications service provider and/or a remote computing service located in Mountain View, CA, to disclose the records and other information described in Attachment A to this Order.


The Court finds that the United States has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

The Court determines that there is reason to believe that notification of the existence of this Order will seriously jeopardize the ongoing investigation, including by giving subjects an opportunity to destroy or tamper with evidence, or otherwise seriously jeopardize an ongoing investigation. *See* 18 U.S.C. § 2705(b)(3), (5).


IT IS THEREFORE ORDERED, pursuant to 18 U.S.C. § 2703(d), that Google, Inc. shall, within ten days of the date of this Order, disclose to the United States the records and other information described in Attachment A to this Order.

IT IS FURTHER ORDERED that Google, Inc. shall not disclose the existence of the application of the United States, or the existence of this Order of the Court, to the subscriber(s) of the account listed in Attachment A, or to any other person, unless and until otherwise authorized to do so by the Court, except that Google, Inc. may disclose this Order to an attorney for Google, Inc. for the purpose of receiving legal advice.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court.

  
\_\_\_\_\_  
/s/  
Theresa Carroll Buchanan  
United States Magistrate Judge  
\_\_\_\_\_  
Theresa Carroll Buchanan  
United States Magistrate Judge

Date: 5/31/16  
At Alexandria, Virginia

ALEXANDRIA DISTRICT COURT  
CLERK, U.S. DISTRICT COURT  
  
\_\_\_\_\_  
CLERK, U.S. DISTRICT COURT

## ATTACHMENT A

### I. The Account(s)

The Order applies to certain records and information associated with the following email account: [REDACTED]@gmail.com.

### II. Records and Other Information to Be Disclosed

Google, Inc. is required to disclose the following records and other information, if available, to the United States for each account or identifier listed in Part I of this Attachment ("Account"), for the time period from February 12, 2011 to April 12, 2011:

- A. The following information about the customers or subscribers of the Account:
  - 1. Names (including subscriber names, user names, and screen names);
  - 2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
  - 3. Local and long distance telephone connection records;
  - 4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
  - 5. Length of service (including start date) and types of service utilized;
  - 6. Telephone or instrument numbers (including MAC addresses);
  - 7. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
  - 8. Means and source of payment for such service (including any credit card or bank account number) and billing records.
  
- B. All records and other information (not including the contents of communications) relating to the Account, including:
  - 1. Records of user activity for each connection made to or from the Account, including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; and source and destination Internet Protocol addresses;
  
  - 2. Information about each communication sent or received by the Account, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers).



**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

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

MAY 31 2016

\_\_\_\_\_  
)  
IN RE APPLICATION OF THE )  
UNITED STATES OF AMERICA FOR )  
AN ORDER PURSUANT TO )  
18 U.S.C. § 2703(d) TO GOOGLE, INC., )  
AN INTERNET SERVICE PROVIDER )

Misc. No. 1:16-ec- 729

**Filed Under Seal**

APPLICATION OF THE UNITED STATES  
FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)

The United States of America, moving by and through its undersigned counsel, respectfully submits under seal this *ex parte* application for an Order pursuant to 18 U.S.C. § 2703(d). The proposed Order would require Google, Inc., an Internet Service Provider located in Mountain View, CA, to disclose certain records and other information pertaining to email account [REDACTED]@gmail.com. The records and other information to be disclosed are described in Attachment A to the proposed Order. In support of this application, the United States asserts:

LEGAL BACKGROUND

1. Google, Inc. is a provider of an electronic communications service, as defined in 18 U.S.C. § 2510(15), and/or a remote computing service, as defined in 18 U.S.C. § 2711(2). Accordingly, the United States may use a court order issued under § 2703(d) to require Google, Inc. to disclose the items described in Part II of Attachment A. *See* 18 U.S.C. § 2703(c)(2) (Part II.A of Attachment A); 18 U.S.C. § 2703(c)(1) (Part II.B of Attachment A).

2. This Court has jurisdiction to issue the proposed Order because it is “a court of competent jurisdiction,” as defined in 18 U.S.C. § 2711. *See* 18 U.S.C. § 2703(d). Specifically,

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

3. A court order under § 2703(d) “shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d). Accordingly, the next section of this application sets forth specific and articulable facts showing that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation.

#### THE RELEVANT FACTS

4. The government is conducting a criminal investigation concerning the improper transmission and storage of classified information on unclassified email systems and servers, in violation of Title 18, United States Code, Sections 793(e) and (f). The investigation began as a result of a review of emails undertaken by the U.S. Department of State in connection with Freedom of Information Act (FOIA) litigation. During this FOIA review, it was determined that certain emails containing classified information were sent and received on systems unauthorized for the transmission or storage of such information. On or about July 6, 2015, the Inspector General for the Intelligence Community notified the Federal Bureau of Investigation (FBI) of a potential compromise of classified information involving the emails discovered through the FOIA review. After an initial review of the matter, the FBI opened a criminal investigation to, among other things, identify any unauthorized systems which the emails in question have transited, identify any person(s) who may have introduced classified information onto

unauthorized systems and all circumstances surrounding such introduction, and identify any person(s) who may have transmitted such information over any such systems.

5. From January 21, 2009 to March 1, 2013, Cheryl Mills was employed at the U.S. Department of State as Counselor and Chief of Staff to Secretary of State Hillary Rodham Clinton. During this time, Mills is known to have maintained a personal email account, [REDACTED]@gmail.com ("Subject Account"), in addition to any official Department of State accounts she may have used. The Subject Account was not authorized for the transmission or storage of classified information. Pursuant to the FBI's investigation of State Department emails that were transmitted and stored on personal email accounts and servers, at least 911 email communications containing the Subject Account have been identified. Out of the 911 emails, the FBI has identified seven emails containing classified information and approximately 208 additional emails that it believes contain classified information, but which have not yet undergone a formal classification review.

6. For example, the investigation has revealed that on or about March 12, 2011, an email was sent from the Subject Account that the National Geospatial-Intelligence Agency (NGA) has determined, in a subsequent classification review, to be classified at the SECRET//NOFORN<sup>1</sup> level at the time the email was sent.

7. Based on the FBI's investigation, there is reason to believe that the Subject Account contains evidence related to the unlawful transmission and storage of classified information on unclassified email systems and servers during Cheryl Mills' tenure at the U.S. Department of State.

---

<sup>1</sup> Classified information may be marked as "Not Releasable to Foreign Nationals/Governments/US Citizens," abbreviated "NOFORN," to indicate information that may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-U.S. citizens without permission of the originator.

## REQUEST FOR ORDER

8. The facts set forth in the previous section show that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation. Specifically, a review of these items will help the FBI determine if emails believed to contain classified information still reside within the Subject Account maintained by Cheryl Mills and whether there are other records connecting email accounts associated with the improper transmission and storage of classified information to the Subject Account. Accordingly, the United States requests that Google, Inc. be directed to produce all items described in Part II of Attachment A to the proposed Order.

9. The United States further requests that the Order require Google, Inc. not to notify any person, including the subscribers or customers of the account(s) listed in Part I of Attachment A, of the existence of the Order until further order of the Court. *See* 18 U.S.C. § 2705(b). This Court has authority under 18 U.S.C. § 2705(b) to issue “an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order.” *Id.* In this case, such an order would be appropriate because the requested Order relates to an ongoing criminal investigation involving email evidence that is not known to all of the subjects of the investigation, and its disclosure may alert subjects to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the requested Order will seriously jeopardize the investigation, including by giving subjects an opportunity to destroy or tamper with evidence, or otherwise seriously jeopardize an ongoing investigation. *See* 18 U.S.C. § 2705(b)(3), (5). Because much of the evidence in this investigation is stored electronically, if

alerted to the investigation, subjects could destroy that evidence, including information saved to personal computers.

10. The United States further requests that the Court order that this application and any resulting order be sealed until further order of the Court. As explained above, these documents discuss an ongoing criminal investigation that is neither public nor known to all of the subjects of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

Dana J. Boente  
United States Attorney

By:

A large black rectangular redaction box covers the signature and name of the Assistant United States Attorney. The text "Assistant United States Attorney" is visible at the bottom of the redacted area.

Assistant United States Attorney

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

MAY 11 2015

\_\_\_\_\_)  
IN RE APPLICATION OF THE )  
UNITED STATES OF AMERICA FOR )  
AN ORDER PURSUANT TO )  
18 U.S.C. § 2703(d) TO GOOGLE, INC., )  
AN INTERNET SERVICE PROVIDER )

Misc. No. 1:16-ec- 729

**Filed Under Seal**

ORDER

The United States has submitted an application pursuant to 18 U.S.C. § 2703(d), requesting that the Court issue an Order requiring Google, Inc., an electronic communications service provider and/or a remote computing service located in Mountain View, CA, to disclose the records and other information described in Attachment A to this Order.

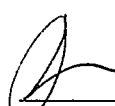
The Court finds that the United States has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

The Court determines that there is reason to believe that notification of the existence of this Order will seriously jeopardize the ongoing investigation, including by giving subjects an opportunity to destroy or tamper with evidence, or otherwise seriously jeopardize an ongoing investigation. *See* 18 U.S.C. § 2705(b)(3), (5).

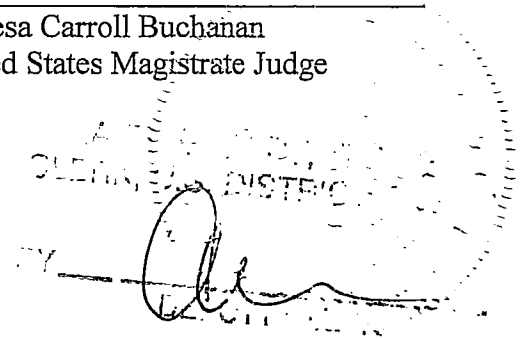
IT IS THEREFORE ORDERED, pursuant to 18 U.S.C. § 2703(d), that Google, Inc. shall, within ten days of the date of this Order, disclose to the United States the records and other information described in Attachment A to this Order.

IT IS FURTHER ORDERED that Google, Inc. shall not disclose the existence of the application of the United States, or the existence of this Order of the Court, to the subscriber(s) of the account listed in Attachment A, or to any other person, unless and until otherwise authorized to do so by the Court, except that Google, Inc. may disclose this Order to an attorney for Google, Inc. for the purpose of receiving legal advice.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court.

 \_\_\_\_\_ /s/  
Theresa Carroll Buchanan  
United States Magistrate Judge  
Theresa Carroll Buchanan  
United States Magistrate Judge

Date: 5/31/16  
At Alexandria, Virginia





## ATTACHMENT A

### I. The Account(s)

The Order applies to certain records and information associated with the following email account: [REDACTED]@gmail.com.

### II. Records and Other Information to Be Disclosed

Google, Inc. is required to disclose the following records and other information, if available, to the United States for each account or identifier listed in Part I of this Attachment ("Account"), for the time period from January 21, 2009 to March 1, 2013:

- A. The following information about the customers or subscribers of the Account:
  - 1. Names (including subscriber names, user names, and screen names);
  - 2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
  - 3. Local and long distance telephone connection records;
  - 4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
  - 5. Length of service (including start date) and types of service utilized;
  - 6. Telephone or instrument numbers (including MAC addresses);
  - 7. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
  - 8. Means and source of payment for such service (including any credit card or bank account number) and billing records.
  
- B. All records and other information (not including the contents of communications) relating to the Account, including:
  - 1. Records of user activity for each connection made to or from the Account, including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; and source and destination Internet Protocol addresses;
  
  - 2. Information about each communication sent or received by the Account, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers).

**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

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

FEB 18 2016

\_\_\_\_\_  
)  
IN RE APPLICATION OF THE )  
UNITED STATES OF AMERICA FOR )  
AN ORDER PURSUANT TO )  
18 U.S.C. § 2703(d) TO YAHOO, INC., )  
AN INTERNET SERVICE PROVIDER )

Misc. No. 1:16-ec-209

**Filed Under Seal**

APPLICATION OF THE UNITED STATES  
FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)

The United States of America, moving by and through its undersigned counsel, respectfully submits under seal this *ex parte* application for an Order pursuant to 18 U.S.C. § 2703(d). The proposed Order would require Yahoo, Inc., an Internet Service Provider located in Sunnyvale, CA, to disclose certain records and other information pertaining to email account [REDACTED]@yahoo.com. The records and other information to be disclosed are described in Attachment A to the proposed Order. In support of this application, the United States asserts:

LEGAL BACKGROUND

1. Yahoo, Inc. is a provider of an electronic communications service, as defined in 18 U.S.C. § 2510(15), and/or a remote computing service, as defined in 18 U.S.C. § 2711(2). Accordingly, the United States may use a court order issued under § 2703(d) to require Yahoo, Inc. to disclose the items described in Part II of Attachment A. *See* 18 U.S.C. § 2703(c)(2) (Part II.A of Attachment A); 18 U.S.C. § 2703(c)(1) (Part II.B of Attachment A).

2. This Court has jurisdiction to issue the proposed Order because it is “a court of competent jurisdiction,” as defined in 18 U.S.C. § 2711. *See* 18 U.S.C. § 2703(d). Specifically,

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

3. A court order under § 2703(d) “shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d). Accordingly, the next section of this application sets forth specific and articulable facts showing that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation.

#### THE RELEVANT FACTS

4. The government is conducting a criminal investigation concerning the improper transmission and storage of classified information on unclassified email systems and servers, in violation of Title 18, United States Code, Sections 793(e) and (f). The investigation began as a result of a review of emails undertaken by the U.S. Department of State in connection with Freedom of Information Act (FOIA) litigation. During this FOIA review, it was determined that certain emails containing classified information were sent and received on systems unauthorized for the transmission or storage of such information. On or about July 6, 2015, the Inspector General for the Intelligence Community notified the Federal Bureau of Investigation (FBI) of a potential compromise of classified information involving the emails discovered through the FOIA review. After an initial review of the matter, the FBI opened a criminal investigation to, among other things, identify any unauthorized systems which the emails in question have transited, identify any person(s) who may have introduced classified information onto

unauthorized systems and all circumstances surrounding such introduction, and identify any person(s) who may have transmitted such information over any such systems.

5. From January 21, 2009 to March 1, 2013, Huma Abedin was employed at the U.S. Department of State as Deputy Chief of Staff to Secretary of State Hillary Rodham Clinton. During this time, Abedin is known to have maintained a personal email account, [REDACTED]@yahoo.com ("Subject Account"), in addition to her official unclassified Department of State OpenNet account.

6. The investigation has revealed that on or about October 4, 2009, at 11:06 p.m., an email was forwarded from Abedin's OpenNet account to the Subject Account. The forwarded email included a Word document entitled, "DRAFT 10-4" that Abedin received from a State Department employee that same day. The Word document contained no classification portion markings, headers, or footers.

7. On or about October 5, 2009, at 12:35 p.m., the text from this Word document, with slight edits and reformatted to State Department letterhead, was sent from a State Department employee on SIPRNet, a classified email system, to Cheryl Mills, Counselor and Chief of Staff to Secretary Clinton. The Word document's title was "MEMORANDUM TO THE NATIONAL SECURITY ADVISOR" and was marked as being classified SECRET//NOFORN.<sup>1</sup> The first page of the Word document cited that the contents of the document were classified by "Secretary of State Hillary Rodman Clinton" and listed a declassification date of October 5, 2019.

---

<sup>1</sup> Classified information may be marked as "Not Releasable to Foreign Nationals/Governments/US Citizens," abbreviated "NOFORN," to indicate information that may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-U.S. citizens without permission of the originator.

8. Based on the FBI's investigation, there is reason to believe that the Subject Account contains evidence related to the unlawful transmission and storage of classified information on unclassified email systems and servers during Huma Abedin's tenure at the U.S. Department of State.

#### REQUEST FOR ORDER

9. The facts set forth in the previous section show that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation. Specifically, a review of these items will help the FBI determine if the aforementioned email, containing the classified Word document, still resides within the Subject Account maintained by Huma Abedin and whether there are other records connecting email accounts associated with the improper transmission and storage of classified information to the Subject Account. Accordingly, the United States requests that Yahoo, Inc. be directed to produce all items described in Part II of Attachment A to the proposed Order.

10. The United States further requests that the Order require Yahoo, Inc. not to notify any person, including the subscribers or customers of the account(s) listed in Part I of Attachment A, of the existence of the Order until further order of the Court. *See* 18 U.S.C. § 2705(b). This Court has authority under 18 U.S.C. § 2705(b) to issue "an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order." *Id.* In this case, such an order would be appropriate because the requested Order relates to an ongoing criminal investigation that is neither public nor known to all of the subjects of the investigation, and its

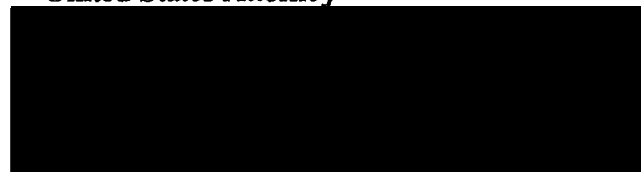
disclosure may alert subjects to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the requested Order will seriously jeopardize the investigation, including by giving subjects an opportunity to destroy or tamper with evidence, or otherwise seriously jeopardize an ongoing investigation. *See* 18 U.S.C. § 2705(b)(3), (5). Because much of the evidence in this investigation is stored electronically, if alerted to the investigation, subjects could destroy that evidence, including information saved to personal computers.

11. The United States further requests that the Court order that this application and any resulting order be sealed until further order of the Court. As explained above, these documents discuss an ongoing criminal investigation that is neither public nor known to all of the subjects of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

Dana J. Boente  
United States Attorney

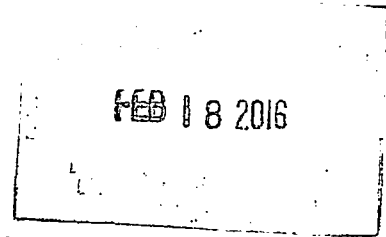
By:



Assistant United States Attorney

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



\_\_\_\_\_  
)  
IN RE APPLICATION OF THE )  
UNITED STATES OF AMERICA FOR )  
AN ORDER PURSUANT TO )  
18 U.S.C. § 2703(d) TO YAHOO, INC., )  
AN INTERNET SERVICE PROVIDER )

Misc. No. 1:16-ec-209

**Filed Under Seal**

ORDER

The United States has submitted an application pursuant to 18 U.S.C. § 2703(d), requesting that the Court issue an Order requiring Yahoo, Inc., an electronic communications service provider and/or a remote computing service located in Sunnyvale, CA, to disclose the records and other information described in Attachment A to this Order.

The Court finds that the United States has offered specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation.

The Court determines that there is reason to believe that notification of the existence of this Order will seriously jeopardize the ongoing investigation, including by giving subjects an opportunity to destroy or tamper with evidence, or otherwise seriously jeopardize an ongoing investigation. *See* 18 U.S.C. § 2705(b)(3), (5).

IT IS THEREFORE ORDERED, pursuant to 18 U.S.C. § 2703(d), that Yahoo, Inc. shall, within ten days of the date of this Order, disclose to the United States the records and other information described in Attachment A to this Order.



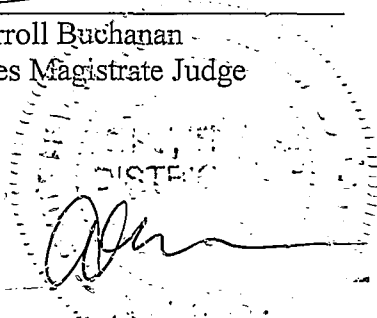
IT IS FURTHER ORDERED that Yahoo, Inc. shall not disclose the existence of the application of the United States, or the existence of this Order of the Court, to the subscriber(s) of the account listed in Attachment A, or to any other person, unless and until otherwise authorized to do so by the Court, except that Yahoo, Inc. may disclose this Order to an attorney for Yahoo, Inc. for the purpose of receiving legal advice.

IT IS FURTHER ORDERED that the application and this Order are sealed until otherwise ordered by the Court.

/s/  
\_\_\_\_\_  
Theresa Carroll Buchanan  
United States Magistrate Judge

\_\_\_\_\_

Theresa Carroll Buchanan  
United States Magistrate Judge



Date: 2/18/16  
\_\_\_\_\_  
At Alexandria, Virginia

## ATTACHMENT A

### I. The Account(s)

The Order applies to certain records and information associated with the following email account: [REDACTED]@yahoo.com.

### II. Records and Other Information to Be Disclosed

Yahoo, Inc. is required to disclose the following records and other information, if available, to the United States for each account or identifier listed in Part I of this Attachment ("Account"), for the time period from January 21, 2009 to March 1, 2013:

- A. The following information about the customers or subscribers of the Account:
1. Names (including subscriber names, user names, and screen names);
  2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
  3. Local and long distance telephone connection records;
  4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
  5. Length of service (including start date) and types of service utilized;
  6. Telephone or instrument numbers (including MAC addresses);
  7. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
  8. Means and source of payment for such service (including any credit card or bank account number) and billing records.
- B. All records and other information (not including the contents of communications) relating to the Account, including:
1. Records of user activity for each connection made to or from the Account, including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; and source and destination Internet Protocol addresses;
  2. Information about each communication sent or received by the Account, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers).

**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 Yahoo, Inc., and my official title is \_\_\_\_\_. I am a custodian of records for Yahoo, 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 Yahoo, 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 Yahoo, Inc.; and
- c. such records were made by Yahoo, 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