

UNITED STATES DISTRICT COURT

for the

District of Columbia

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

INFORMATION ASSOCIATED WITH THE GOOGLE
 ACCOUNT [REDACTED]

Case: 1:18-sc-01518
 Assigned To : Howell, Beryl A.
 Assign. Date : 5/4/2018
 Description: Search & Seizure Warrant

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.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized):*

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before May 18, 2018 *(not to exceed 14 days)*
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Beryl A. Howell
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of

Date and time issued: 5/4/2018 at 3:17 PM

Beryl A. Howell
Judge's signature

City and state: Washington, DC

Hon. Beryl A. Howell, Chief U.S. District Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

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

Certification

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

Date: _____

*Executing officer's signature*_____
Printed name and title

FILED

MAY - 4 2018

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Clerk, U.S. District & Bankruptcy
Courts for the District of Columbia

**IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
THE GOOGLE ACCOUNT**
[REDACTED]

Case: 1:18-sc-01518
Assigned To : Howell, Beryl A.
Assign. Date : 5/4/2018
Description: Search & Seizure Warrant

ORDER

The United States has filed a motion to seal the above-captioned warrant and related documents, including the application and affidavit in support thereof (collectively the "Warrant"), and to require Google LLC, an electronic communication and/or remote computing services with headquarters in Mountain View, California, not to disclose the existence or contents of the Warrant pursuant to 18 U.S.C. § 2705(b).

The Court finds that the United States has established that a compelling governmental interest exists to justify the requested sealing, and that there is reason to believe that notification of the existence of the Warrant will seriously jeopardize the investigation, including by giving the targets an opportunity to flee from prosecution, destroy or tamper with evidence, and intimidate witnesses. *See* 18 U.S.C. § 2705(b)(2)-(5).

IT IS THEREFORE ORDERED that the motion is hereby **GRANTED**, and that the warrant, the application and affidavit in support thereof, all attachments thereto and other related materials, the instant motion to seal, and this Order be **SEALED** until further order of the Court; and

IT IS FURTHER ORDERED that, pursuant to 18 U.S.C. § 2705(b), Google and its employees shall not disclose the existence or content of the Warrant to any other person (except attorneys for Google for the purpose of receiving legal advice) for a period of one year unless otherwise ordered by the Court.



THE HONORABLE BERYL A. HOWELL
CHIEF UNITED STATES DISTRICT JUDGE

5/4/2018
Date

UNITED STATES DISTRICT COURT

for the
District of Columbia

FILED

MAY - 4 2018

Clerk, U.S. District & Bankruptcy
Courts for the District of ColumbiaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)INFORMATION ASSOCIATED WITH THE GOOGLE
ACCOUNT [REDACTED]

Case: 1:18-sc-01518

Assigned To : Howell, Beryl A.

Assign. Date : 5/4/2018

Description: Search & Seizure Warrant

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

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
18 U.S.C. § 2
et al.

Offense Description
aiding and abetting
see attached affidavit

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:

Aaron Zelinsky (Special Counsel's Office)



Applicant's signature

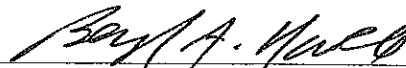
Andrew Mitchell, Supervisory Special Agent, FBI.

Printed name and title

Sworn to before me and signed in my presence.

Date:

5/4/2018



Judge's signature

City and state: Washington, D.C.

Hon. Beryl A. Howell, Chief U.S. District Judge

Printed name and title

FILED

MAY - 4 2018

Clerk, U.S. District & Bankruptcy
Courts for the District of Columbia

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
THE GOOGLE ACCOUNT
[REDACTED]

Case: 1:18-sc-01518
Assigned To : Howell, Beryl A.
Assign. Date : 5/4/2018
Description: Search & Seizure Warrant

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

I, Andrew Mitchell, having been first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of an application for a search warrant for information associated with the following Google Account: [REDACTED] (hereafter the "**Target Account 1**"), that is stored at premises owned, maintained, controlled or operated by Google, Inc., a social networking company headquartered in Mountain View, California ("Google"). The information to be searched is described in the following paragraphs and in Attachments A and B. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Attachment A. Upon receipt of the information described in Attachment A, government-authorized persons will review that information to locate the items described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since 2011. As a Special Agent of the FBI, I have received training and experience in investigating criminal and national security matters.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended

to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the Target Accounts contain communications relevant to violations of 18 U.S.C. § 2 (aiding and abetting), 18 U.S.C. § 3 (accessory after the fact), 18 U.S.C. § 4 (misprision of a felony), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1001 (making a false statement); 18 U.S.C. § 1651 (perjury); 18 U.S.C. § 1030 (unauthorized access of a protected computer); 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1349 (attempt and conspiracy to commit wire fraud), , and 52 U.S.C. § 30121 (foreign contribution ban) (the “Subject Offenses”).¹

5. As set forth below, in May 2016, Jerome CORSI provided contact information for [REDACTED] to Roger STONE. In July 2016, [REDACTED] also told STONE that he needed to meet with then-candidate Trump “alone.” In August 2016, [REDACTED] told STONE that there was an “OCTOBER SURPRISE COMING” and that Trump, “[i]s going to be defeated unless we intervene. We have critical intel.” In that same time period, STONE communicated directly via Twitter with WikiLeaks, Julian ASSANGE, and Guccifer 2.0. On July 25, 2016, STONE emailed instructions to Jerome CORSI to “Get to Assange” in person at the Ecuadorian Embassy and “get pending WikiLeaks emails[.]” On August 2, 2016, CORSI emailed STONE back that, “Word is friend in embassy plans 2 more dumps. One shortly after I’m back. 2nd in Oct. Impact planned to be very damaging.” On August 20, 2016, CORSI told STONE that they needed to meet with [REDACTED] to determine “what if anything Israel plans to do in Oct.”

¹ Federal law prohibits a foreign national from making, directly or indirectly, an expenditure or independent expenditure in connection with federal elections. 52 U.S.C. § 30121(a)(1)(C); *see also id.* § 30101(9) & (17) (defining the terms “expenditure” and “independent expenditure”).

[REDACTED] (the Target Account) is [REDACTED] Google Account, which [REDACTED] used to communicate with STONE and CORSI.

JURISDICTION

6. 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. *Id.* §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States (including a magistrate judge of such a court) . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). The offense conduct included activities in Washington, D.C., as detailed below, including in paragraph 8.

PROBABLE CAUSE

A. U.S. Intelligence Community (USIC) Assessment of Russian Government-Backed Hacking Activity during the 2016 Presidential Election

7. On October 7, 2016, the U.S. Department of Homeland Security and the Office of the Director of National Intelligence released a joint statement of an intelligence assessment of Russian activities and intentions during the 2016 presidential election. In the report, the USIC assessed the following, with emphasis added:

8. The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e mails from US persons and institutions, including from US political organizations. The recent disclosures of alleged hacked e mails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts. These thefts and disclosures are intended to interfere with the US election process. Such activity is not new to Moscow—the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to

influence public opinion there. We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities.

9. On January 6, 2017, the USIC released a declassified version of an intelligence assessment of Russian activities and intentions during the 2016 presidential election entitled, "Assessing Russian Activities and Intentions in Recent US Elections." In the report, the USIC assessed the following:

10. [] Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate [former] Secretary [of State Hillary] Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump."

11. The USIC also described, at a high level, some of the techniques that the Russian government employed during its interference. The USIC summarized the efforts as a "Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or 'trolls.'"

12. With respect to "cyber activity," the USIC assessed that "Russia's intelligence services conducted cyber operations against targets associated with the 2016 US presidential election, including targets associated with both major US political parties." Further, "[i]n July 2015, Russian intelligence gained access to Democratic National Committee (DNC) networks and maintained that access until at least June 2016." The USIC attributed these cyber activities to the Russian GRU, also known as the Main Intelligence Directorate: "GRU operations resulted in the compromise of the personal e-mail accounts of Democratic Party officials and political

figures. By May, the GRU had exfiltrated large volumes of data from the DNC.” The GRU is the foreign military intelligence agency of the Russian Ministry of Defense, and is Russia’s largest foreign intelligence agency.

13. With respect to the release of stolen materials, the USIC assessed “with high confidence that the GRU used the Guccifer 2.0 persona, DCLeaks.com, and WikiLeaks to release US victim data obtained in cyber operations publicly and in exclusives to media outlets.”

14. Guccifer 2.0, who claimed to be an independent Romanian hacker, made multiple contradictory statements and false claims about his identity throughout the election.

B. Roger Stone’s Public Interactions with Guccifer 2.0 and WikiLeaks.

15. Roger Stone is a self-employed political strategist/consultant and has been actively involved in U.S. politics since 1975. Stone worked on the presidential campaign of Donald J. Trump (the “Campaign”) until he was fired in August 2015. Although Stone had no official relationship with the Campaign thereafter, Stone maintained his support for Trump and continued to make media appearances in support of Trump’s presidential campaign. On August 7, 2017, Chief Judge Beryl A. Howell issued a search warrant for the Twitter account @RogerJStoneJr.

16. On June 14, 2016, news reports indicated that the computer systems of the DNC had been hacked. On June 15, 2016, Guccifer 2.0 publicly claimed responsibility for the DNC hack. Shortly thereafter, Guccifer 2.0 began releasing the hacked documents, including a June, 21, 2016 release of hacked documents.

17. On July 22, 2016, WikiLeaks published approximately 20,000 emails stolen from the DNC.

18. On August 5, 2016, Roger Stone published an article on Breitbart.com entitled, "Dear Hillary: DNC Hack Solved, So Now Stop Blaming Russia." Stone wrote: "It doesn't seem to be the Russians that hacked the DNC, but instead a hacker who goes by the name of Guccifer 2.0." Stone embedded publicly available Tweets from Guccifer 2.0 in the article and wrote: "Here's Guccifer 2.0's website. Have a look and you'll see he explains who he is and why he did the hack of the DNC." Stone also stated: "Guccifer 2.0 made a fateful and wise decision. He went to WikiLeaks with the DNC files and the rest is history. Now the world would see for themselves how the Democrats had rigged the game."

19. On August 8, 2016, Stone addressed the Southwest Broward Republican Organization. During his speech, he was asked about a statement by WikiLeaks founder Julian Assange to Russia Today (RT) several days earlier about an upcoming "October Surprise" aimed at the Hillary Clinton presidential campaign. Specifically, Stone was asked: "With regard to the October surprise, what would be your forecast on that given what Julian Assange has intimated he's going to do?" Stone responded: "Well, it could be a number of things. I actually have communicated with Assange. I believe the next tranche of his documents pertain to the Clinton Foundation but there's no telling what the October surprise may be." A few days later, Stone clarified that while he was not personally in touch with Assange, he had a close friend who served as an intermediary.

20. On August 12, 2016, Guccifer 2.0 publicly tweeted: "@RogerJStoneJr thanks that u believe in the real #Guccifer2." That same day, Guccifer 2.0 released the personal cellphone numbers and email addresses from the files of the Democratic Congressional Campaign Committee (DCCC).

21. On August 13, 2016, Stone posted a tweet using @RogerJStoneJr calling Guccifer 2.0 a “HERO” after Guccifer 2.0 had been banned from Twitter. The next day, Guccifer 2.0’s Twitter account was reinstated.

22. On August 17, 2016, Guccifer 2.0 publicly tweeted, “@RogerJStoneJr paying you back.” Guccifer also sent a private message to @RogerJStoneJr stating “i’m pleased to say u r great man. please tell me if I can help u anyhow. it would be a great pleasure to me.”

23. On August 18, 2016, Paul Manafort, Stone’s longtime friend and associate, resigned as Chairman of the Campaign. Contemporary press reports at the time indicated that Manafort had worked with a Washington D.C.-based lobbying firms to influence U.S. policy toward Ukraine.

24. On August 21, 2016, using @RogerJStoneJR, Stone directed a tweet at John Podesta, Hillary Clinton’s presidential campaign manager, stating: “Trust me, it will soon the [sic] Podesta’s time in the barrel. #CrookedHillary.” In a C-SPAN interview that same day, Stone reiterated that because of the work of a “‘mutual acquaintance’ of both his and [Assange], the public [could] expect to see much more from the exiled whistleblower in the form of strategically-dumped Clinton email batches.” He added: “Well, first of all, I think Julian Assange is a hero... I think he’s taking on the deep state, both Republican and Democrat. I believe that he is in possession of all of those emails that Huma Abedin and Cheryl Mills, the Clinton aides, believe they deleted. That and a lot more. These are like the Watergate tapes.”

25. On September 16, 2016 Stone said in a radio interview with Boston Herald Radio that he expected WikiLeaks to “drop a payload of new documents on a weekly basis fairly soon. And that of course will answer the question of exactly what was erased on that email server.”

26. On Saturday, October 1, 2016, using @RogerJStoneJr, Stone Tweeted, “Wednesday @HillaryClinton is done. #WikiLeaks.”

27. On Sunday, October 2, 2016, MSNBC Morning Joe producer Jesse Rodriguez tweeted regarding an announcement Julian Assange had scheduled for the next day from the balcony of the Ecuadoran Embassy in London. On the day of the Assange announcement – which was part of WikiLeaks’ 10-year anniversary celebration – Stone told Infowars that his intermediary described this release as the “mother load.” On Tuesday, October 4, 2016, Stone used @RogerJStoneJr to tweet: “Payload coming. #Lockthemup.”

28. On Friday, October 7, 2016, at approximately 4:03 P.M., the Washington Post published an article containing a recorded conversation from a 2005 Access Hollywood shoot in which Mr. Trump had made a series of lewd remarks.

29. Approximately a half hour later, at 4:32 P.M., WikiLeaks sent a Tweet reading “RELEASE: The Podesta Emails #HillaryClinton #Podesta #imWithHer” and containing a link to approximately 2,050 emails that had been hacked from John Podesta’s personal email account.

30. WikiLeaks continued to release John Podesta’s hacked emails throughout October 10-21, 2016. On October 12, 2016, John Podesta – referring back to Stone’s August 21, 2016 C-SPAN and Twitter references – argued publicly that “[it is] a reasonable assumption to - or at least a reasonable conclusion - that [Stone] had advanced warning [of the release of his emails] and the Trump campaign had advanced warning about what Assange was going to do. I think there’s at least a reasonable belief that [Assange] may have passed this information on to [Stone].” Commenting to the Miami Herald, Stone responded: “I have never met or spoken with Assange, we have a mutual friend who’s traveled to London several times, and everything I know is through that channel of communications. I’m not implying I have any influence with

him or that I have advanced knowledge of the specifics of what he is going to do. I do believe he has all of the e-mails that Huma Abedin and Cheryl Mills, the Clinton aides, thought were deleted. I hear that through my emissary.”

31. On March 27, 2017, CNN reported that a representative of WikiLeaks, writing from an email address associated with WikiLeaks, denied that there was any backchannel communication during the Campaign between Stone and WikiLeaks. The same article quoted Stone as stating: “Since I never communicated with WikiLeaks, I guess I must be innocent of charges I knew about the hacking of Podesta's email (speculation and conjecture) and the timing or scope of their subsequent disclosures. So I am clairvoyant or just a good guesser because the limited things I did predict (Oct disclosures) all came true.”

C. Roger Stone's Private Twitter Direct Messages with WikiLeaks and Julian Assange.

32. On October 13, 2016, while WikiLeaks was in the midst of releasing the hacked Podesta emails, @RogerJStoneJr sent a private direct message to the Twitter account @wikileaks. This account is the official Twitter account of WikiLeaks and has been described as such by numerous news reports. The message read: “Since I was all over national TV, cable and print defending WikiLeaks and assange against the claim that you are Russian agents and debunking the false charges of sexual assault as trumped up bs you may want to rexamine the strategy of attacking me- cordially R.”

33. Less than an hour later, @wikileaks responded by direct message: “We appreciate that. However, the false claims of association are being used by the democrats to undermine the impact of our publications. Don't go there if you don't want us to correct you.”

34. On October 16, 2016, @RogerJStoneJr sent a direct message to @wikileaks: "Ha! The more you \"correct\" me the more people think you're lying. Your operation leaks like a sieve. You need to figure out who your friends are."

35. On November 9, 2016, one day after the presidential election, @wikileaks sent a direct message to @RogerJStoneJr containing a single word: "Happy?" @wikileaks immediately followed up with another message less than a minute later: "We are now more free to communicate."

36. In addition, @RogerJStoneJr also exchanged direct messages with Julian Assange, the founder of WikiLeaks. For example, on June 4, 2017, @RogerJStoneJr directly messaged @JulianAssange, an address associated with Julian Assange in numerous public reports, stating: "Still nonsense. As a journalist it doesn't matter where you get information only that it is accurate and authentic. The New York Times printed the Pentagon Papers which were indisputably stolen from the government and the courts ruled it was legal to do so and refused to issue an order restraining the paper from publishing additional articles. If the US government moves on you I will bring down the entire house of cards. With the trumped-up sexual assault charges dropped I don't know of any crime you need to be pardoned for - best regards. R." That same day, @JulianAssange responded: "Between CIA and DoJ they're doing quite a lot. On the DoJ side that's coming most strongly from those obsessed with taking down Trump trying to squeeze us into a deal."

37. On Saturday, June 10, 2017, @RogerJStoneJr sent a direct message to @wikileaks, reading: "I am doing everything possible to address the issues at the highest level of Government. Fed treatment of you and WikiLeaks is an outrage. Must be circumspect in this forum as experience demonstrates it is monitored. Best regards R."

D. [REDACTED] Emails with Stone and Corsi

39. On September 11, 2017, Chief Judge Beryl A. Howell of the District of Columbia issued a search warrant for STONE's [REDACTED] address, [REDACTED]. On October 17, 2017, Chief Judge Beryl A. Howell issued a search warrant for STONE's [REDACTED] address, [REDACTED]. On March 14, 2018, Chief Judge Beryl A. Howell issued a search warrant for STONE's iCloud account. On April 23, 2018, Chief Judge Beryl A. Howell signed an order pursuant to 18 U.S.C. §2703(d) for the **Target Accounts**. Information recovered pursuant to those search warrants and orders indicated the following:

40. On or about February 2 and February 3, 2016, [REDACTED] using **Target Account 1**, sent two emails to [REDACTED], an email address associated with [REDACTED]
[REDACTED]

[REDACTED]

41. On or about February 5, 2016, [REDACTED] received two emails on Target Account 1 from an account associated with [REDACTED]

42. On or about April 6, 2016, CORSI and [REDACTED] (on Target Account 1) exchanged seven emails. On or about April 7, CORSI email [REDACTED] on Target Account 1. On or about April 8, 2016, [REDACTED] emailed CORSI. On or about April 10, [REDACTED] and CORSI exchanged two emails. On or about April 18, 2016, CORSI sent [REDACTED] an email.

43. On or about May 1, 2016, CORSI emailed [REDACTED] (on Target Account 1) three times and [REDACTED] sent him two responses. On or about May 2, 2017, [REDACTED] (on Target Account 1) emailed CORSI.

44. On or about May 17, 2016, STONE emailed Jerome CORSI, "send me [REDACTED] e-mail address." CORSI wrote back, "Roger[,] [REDACTED] (Target Account 1) also seems to work as [REDACTED] 4

45. That same day, STONE emailed [REDACTED] at Target Account 1. STONE wrote that he would have to move "our meeting to Wednesday. I am uncomfortable meeting without Jerry." As described further below, it appears that "Jerry" is Jerome CORSI. STONE and [REDACTED] exchanged additional emails about setting up dinner, and [REDACTED] emailed back, "RS[,] Confirming dinner Wednesday at 7PM at Club 21, JC included."

46. On or about that same day, May 17, 2016, [REDACTED] on Target Account 1, emailed CORSI.

47. On or about June 3, 2016, CORSI emailed [REDACTED] on Target Account 1.

E. [REDACTED] Stone, and Corsi's Text Messages about "October Surprise" and "Critical Intel."

⁴ The period in a [REDACTED] email account is not read as a character. Therefore, [REDACTED] and [REDACTED] are the same account.

48. On or about May 17, 2016, [REDACTED] messaged STONE, "Hi Roger, I hope all is well. Our dinner tonight for 7PM is confirmed. I arrive at 4PM. Please suggest a good restaurant that has privacy. Thank you. See you soon, [REDACTED]" STONE responded, "See e-mail."

49. On or about May 19, 2016, [REDACTED] messaged STONE, "Hi Roger, It Was Great Seeing You Again Last Night At Dinner. Did You Talk To Trump This Morning? Any News? Thank You. Best, [REDACTED]" STONE responded, "Contact made – interrupted – mood good." [REDACTED] and STONE continued to text about arranging a meeting with then-candidate Trump.

50. On or about June 21, 2016, [REDACTED] messaged STONE, "RS: Secret | Cabinet Minister [REDACTED] in NYC Sat. June 25. Available for DJT meeting. [REDACTED]" According to publicly-available information, during this time [REDACTED] was a Minister without portfolio in the [REDACTED] cabinet dealing with issues concerning defense and foreign affairs.

51. On or about June 25, 2016, [REDACTED] messaged Stone, "Roger, Minister left. Sends greetings from PM.⁵ When am I meeting DJT? Should I stay or leave Sunday as planned? Hope you are well. [REDACTED]"

52. On or about June 26, 2016, STONE messaged [REDACTED] "I am better but turn out to have been poisoned. Completely out of action for 3 days-apologize to Minister for me. I would not leave as we hope to schedule the meeting mon or tues."

53. On or about June 28, 2016, [REDACTED] messaged STONE, "RETURNING TO DC AFTER URGENT CONSULTATIONS WITH PM IN ROME.MUST MEET WITH YOU WED. EVE AND WITH DJ TRUMP THURSDAY IN NYC. [REDACTED]"

⁵ Based on [REDACTED] statements here and below, I believe "PM" refers to the [REDACTED] Prime Minister.

54. On or about Jun 29, 2016, STONE responded, "Monday meeting collapsed after DJT cleared his schedule to deal with the money crisis. I am waiting the new schedule. Will try for Thursday."

55. On or about June 30, 2016, STONE messaged [REDACTED] "Revised – meeting now 1pm July 6."

56. On or about July 1, 2016, [REDACTED] wrote back, "Thank you my friend . I will plan to be back in NYC on July 5th for the meeting with DJT on the 6th at 1pm. THAY YOU ROGER." STONE responded, "Sorry this took so long. R."

57. On July 5, 2016, [REDACTED] messaged STONE, "Roger, I am here, ready for the meeting with DJ Trump at 1PM tomorrow. Let's you and I meet at 10.30AM at the St. Regis Lobby. Thank you. [REDACTED]"

58. On July 6, 2016, [REDACTED] messaged STONE, "At St Regis With Lt General. Waiting For You Thank You. [REDACTED]" STONE wrote back, "[REDACTED] - I am down with a nasty cold and too ill to travel- I have arranged for Jerri to take u in at 1 rather than lose the appointment – please connect with Jerri – Let me know how the meeting goes .DJT expecting u. R" Based on STONE's contacts and emails described above, investigators believe that the "Jerri" referenced in the message refers to Jerome CORSI.

59. [REDACTED] wrote back, "Thank U Very Much[.] I Have To Meet Trump Alone After A Brief Introduction by Jerry Thanks Roger." STONE wrote back, "As long as u get the meeting – I am very sorry I cannot attend – have a high fever and no voice."

60. On July 8, 2016, ^{2016 ACM} [REDACTED] messaged STONE, "Hi Roger. Have you rescheduled the meeting with DJT? The PM is putting pressure for a quick decision. Thank you for all your help! [REDACTED]"

61. On or about July 8, 2016, STONE wrote back, "T not in NYC again before the convention. I have pneumonia and may be hospitalized later today. I can get this back on track post convention when I can attend. Sorry about the fiasco last week, however you can't just bring the General without tell me – R."

62. On or about July 25, 2016, STONE sent an email from his [REDACTED] Account to Jerome CORSI with the subject line, "Get to Assange." The body of the message read: "Get to Assange [a]t Ecuadorian Embassy in London and get pending WikiLeaks emails...they deal with Foundation, allegedly."

63. On or about July 29, 2016, [REDACTED] sent a messaged to STONE, "HI ROGER, I HOPE YOU ARE WELL. HAVE YOU SET UP A NEW MEETING WITH TRUMP? I PLAN TO BE BACK IN THE US NEXT WEEK. PLEASE ADVISE. THANK YOU. [REDACTED]"

64. On or about July 31, 2016, STONE emailed CORSI with the subject line, "Call me MON." The body of the email read: "[REDACTED] should see Assange[.] [REDACTED] should find Bernie [S]anders brother who called Bill a Rapist – turn him for Trump[.] [REDACTED] should find [REDACTED] or more proof of Bill getting kicked out."

65. On or about August 2, 2016 (approximately 19 days before STONE publicly tweeted about "Podesta's time in the barrel"), CORSI emailed the STONE, "Word is friend in embassy plans 2 more dumps. One shortly after I'm back. 2nd in Oct. Impact planned to be very damaging . . . Time to let more than Podesta to be exposed as in bed w enemy if they are not ready to drop HRC. That appears to be the game hackers are now about. Would not hurt to start suggesting HRC old, memory bad, has stroke -- neither he nor she well. I expect that much of next dump focus, setting stage for Foundation debacle." Investigators believe that CORSI's

reference to a “friend in embassy [who] plans 2 more dumps” refers to Julian ASSANGE, the founder of WikiLeaks, who resided in Ecuador’s London Embassy in 2016.

66. On or about August 9, 2016, [REDACTED] messaged STONE, “Roger-As per PM we have one last shot before moving on. Can you deliver? History will not forgive us. TRUMP IN FREE FALL. OCTOBER SURPRISE COMING ! [REDACTED]

67. On or about August 12, 2016, [REDACTED] messaged STONE, “Roger, hello from Jerusalem. Any progress? He is going to be defeated unless we intervene. We have critical intell. The key is in your hands! Back in the US next week. How is your Pneumonia? Thank you. [REDACTED] STONE replied, “I am well. Matters complicated. Pondering. R.” [REDACTED] wrote back, “Thank You.” No additional messages appear in STONE’s iCloud between STONE and [REDACTED] until October 30, 2016.

68. As described above, on October 7, 2016, WikiLeaks began releasing the emails hacked from John Podesta’s account.

69. On October 26, 2016, [REDACTED] emailed [REDACTED] on the Target Account. On or about October 27, 2016, [REDACTED] emailed [REDACTED] three times on the Target Account.

70. On October 30, 2016, [REDACTED] messaged STONE: “Roger, you are doing a great job !!! I am in NY-met with DJT and helping. Victory is in sight. HK says hello. Thanks, [REDACTED]

71. On Thursday, November 3, 2016, [REDACTED] messaged STONE: “Roger, European country ready to release secret tapes to DESTROY objective. Can we meet ASAP? 4 star General will join. [REDACTED]” STONE responded, “Yes let’s talk thurs.” [REDACTED] wrote back, “Must meet in NYC Thursday AM.”

72. On or about November 7, 2016, [REDACTED] messaged STONE, "ROGER,JERRY- SORRY, BUT DUE TO AN UNEXPECTED EMERGENCY I HAVE TO CANCEL TODAY'S MEETING AT 9. THANKS [REDACTED] . . . HAVING a TIA. Early Stroke." STONE responded, "Take care of yourself." [REDACTED] wrote back, "Tnaks Xou RGer. Blury Virson." STONE replied, "You can't die until after we elect Donald."

F. Stone's HPSCI Testimony and Subsequent Conversations

73. According to publicly-available reporting, Stone testified before the House Permanent Select Intelligence Committee (HPSCI) on September 26, 2017. STONE released his prepared remarks to the media. In his remarks, Stone stated that he had learned Assange was in possession of the DNC emails via Twitter, and that he asked a "journalist" to "independently confirm this report." Stone stated his "intermediary" had "assured me that WikiLeaks would release this information in October and continued to assure me of this throughout the balance of August and all of September." Stone denied knowledge in advance of Podesta's emails being hacked. Accordingly to publicly-available news reports, Stone subsequently informed HPSCI that his intermediary was Randy Credico, an American radio host.

74. On or about November 24, 2017, Credico texted Stone, "I told you to watch his Tweets in October not before that I knew nothing about the DNC stuff. I just followed his Tweets." Stone responded, "U never said anything about the DNC but it was August." Credico replied, "It was not August because I didn't interview him or meet him until August 26th."

75. Credico and Stone continued to exchange messages, and on December 1, 2017, Credico wrote: "I don't know why you had to lie and say you had a back Channel now I had to give all of my forensic evidence to the FBI today what a headache. You could have just told him the truth that you didn't have a back channel they now know that I was not in London until

September of this year. You had no back-channel and you could have just told the truth. You want me to cover you for perjury now.”⁶ Stone responded, “What the fuck is your problem? Neither of us has done anything wrong or illegal. You got the best press of your life and you can get away with asserting for 5th amendment rights if u don’t want talk about[.] And if you turned over anything to the FBI you’re a fool.” Credico replied, “You open yourself up to six counts of perjury. But I’m sure that wasn’t sworn testimony so you’re probably clear... You should go back in a minute your testimony and tell them the truth ... You need to amend your testimony before I testify on the 15th.” Stone wrote, “If you testify you’re a fool. Because of tromp [sic] I could never get away with a certain [sic] my Fifth Amendment rights but you can. I guarantee you you are the one who gets indicted for perjury if you’re stupid enough to testify.” Stone and Credico continued to correspond, and according to publicly available news reports, on December 13, 2017, Credico asserted his Fifth Amendment right not to testify before the HPSCI.

76. On January 25, 2018, Credico texted Stone, “You lied to the house Intel committee. But you’ll get off because you’re friends with Trump so don’t worry. I have all the forensic evidence. I was not a ba[ck] Channel and I have all those emails from September of 2016 to prove it.”

INFORMATION REGARDING GOOGLE

77. Google provides numerous free services to the users with a Google profile. Some of services include, Gmail, Google Talk, Google Wallet, Google+, Google Drive, Google+ Photos, and YouTube. Gmail is a web based email service. Google Talk is an instant messaging service that provides both text and voice communication. Google Talk conversation logs are saved to a “Chats” area in the user’s Gmail account. Google+ is a social networking service. Google Drive is a file storage and synchronization service which provides users with cloud

⁶ Contrary to his statement, Credico had not provided any information to the FBI.

storage, file sharing, and collaborative editing. Google+ Photos (formerly known as Picasa Web Albums) is an image hosting and sharing web service that allows users with a Google account to store and share images for free. YouTube is a free video sharing website that allows users upload, view and share videos. Google also retains a record of searches conducted by the user, as well as location data for the use of some of the services described above. All of these services may record information uploaded, inputted, or gathered from the user.

CONCLUSION

78. Based on the forgoing, I request that the Court issue the proposed search warrant.

REQUEST FOR SEALING

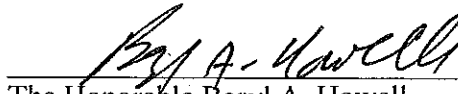
79. I further request that the Court order that all papers in support of this application, including the application, affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,



Andrew T. Mitchell
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on this 4th day of May, 2018.

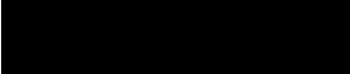


The Honorable Beryl A. Howell
Chief United States District Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Google account

 hat is stored at premises owned, maintained, controlled, or operated by Google, Inc., a business with offices located at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

ATTACHMENT B

Particular Things to be Seized

I. Files and Accounts to be produced by Google, Inc. between January 1, 2016 and the Present.

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Inc. including any messages, records, files, logs, images, videos, or information that have been deleted but are still available to Google or have been preserved pursuant to a preservation request under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all e-mails, attachments and chat messages stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination e-mails sent addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;¹

b. All existing printouts from original storage of all of the electronic mail described above in Section I.A. above;

c. All internet search data including all queries and location data;

d. All transactional information of all activity of the account described above in Section I.A, including log files, dates, times, methods of connecting, ports, dial ups, and/or locations;

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

f. All records or other information regarding the identification of the account described above in Section I.A, to include application, 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 types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, all screen names associated with subscribers and/or accounts, all account names associated with the subscriber, methods of connecting, log files, means and source of payment (including any credit or bank account number), and detailed billing records;

g. All records indicating the services available to subscribers of the electronic mail address described above in Section I.A.;

h. Google+ subscriber information, circle information, including name of circle and

¹ This Search warrant applies on to email sent, received, or drafted on or after May 26, 2017.

members, contents of posts, comments, and photos, to include date and timestamp;

- i. Google Drive files created, accessed or owned by the account;
- j. YouTube subscriber information, private videos and files, private messages, and comments;
- k. Google+ Photos contents to include all images, videos and other files, and associated upload/download date and timestamp;
- l. Google Talk and Google Hangouts conversation logs associated with the account.

II. Information to be Seized by Law Enforcement Personnel

a. Any and all records that relate in any way to the account described in Attachment A which is evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2 (aiding and abetting), 18 U.S.C. § 3 (accessory after the fact), 18 U.S.C. § 4 (misprision of a felony), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1001 (making a false statement); 18 U.S.C. § 1651 (perjury); 18 U.S.C. § 1030 (unauthorized access of a protected computer); 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1349 (attempt and conspiracy to commit wire fraud), , and 52 U.S.C. § 30121 (foreign contribution ban) from Jan 1, 2015 to the present, including:

All records, information, documents or tangible materials that relate in any way to communications with foreign government officials or agents of a foreign power, or discussions with others regarding those actions, or plans or attempts at undertaking such actions:

b. All images, messages, communications, calendar entries, search terms, and contacts, including any and all preparatory steps taken in furtherance of these crimes;

c. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts;

d. Evidence of the times the account was used;

e. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;

f. Passwords and encryption keys, and other access information that may be necessary to access the account and other associated accounts;

g. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;

h. All existing printouts from original storage which concern the categories identified in subsection II.A; and

i. All "address books" or other lists of contacts.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
THE GOOGLE ACCOUNT
[REDACTED]

Case: 1:18-sc-01518
Assigned To : Howell, Beryl A.
Assign. Date : 5/4/2018
Description: Search & Seizure Warrant

**MOTION TO SEAL WARRANT AND RELATED DOCUMENTS
AND TO REQUIRE NON-DISCLOSURE UNDER 18 U.S.C. § 2705(B)**

The United States of America, moving by and through its undersigned counsel, respectfully moves the Court for an Order placing the above-captioned warrant and the application and affidavit in support thereof (collectively herein the “Warrant”) under seal, and precluding the provider from notifying any person of the Warrant pursuant to 18 U.S.C. § 2705(b). In regard to non-disclosure, the proposed Order would direct Google LLC, an electronic communication and/or remote computing services provider with headquarters in Mountain View, California, not to notify any other person (except attorneys for Google for the purpose of receiving legal advice) of the existence or content of the Warrant for a period of one year unless otherwise ordered of the Court.

JURISDICTION AND LEGAL BACKGROUND

1. The Court has the inherent power to seal court filings when appropriate, including the Warrant. *United States v. Hubbard*, 650 F.2d 293, 315–16 (D.C. Cir. 1980) (citing *Nixon v. Warner Communications, Inc.*, 435 U.S. 589, 598 (1978)). The Court may also seal the Warrant to prevent serious jeopardy to an ongoing criminal investigation when, as in the present case, such jeopardy creates a compelling governmental interest in preserving the confidentiality of the Warrant. *See Washington Post v. Robinson*, 935 F.2d 282, 287–89 (D.C. Cir. 1991).

2. In addition, this Court has jurisdiction to issue the requested order because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 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). As discussed fully below, acts or omissions in furtherance of the offense under investigation occurred within Washington, D.C. *See* 18 U.S.C. § 3237. [REDACTED]

[REDACTED]

[REDACTED]

3. Further, the Court has authority to require non-disclosure of the Warrant under 18 U.S.C. § 2705(b). Google provides an “electronic communications service,” as defined in 18 U.S.C. § 2510(15), and/or “remote computing service,” as defined in 18 U.S.C. § 2711(2). The Stored Communications Act (“SCA”), 18 U.S.C. §§ 2701–2712, governs how Google may be compelled to supply communications and other records using a subpoena, court order, or search warrant. Specifically, Section 2703(c)(2) authorizes the Government to obtain certain basic “subscriber information” using a subpoena, Section 2703(d) allows the Government to obtain other “non-content” information using a court order, and Section 2703(a)–(b)(1)(A) allows the Government to obtain contents of communications using a search warrant. *See* 18 U.S.C. § 2703.

4. The SCA does not set forth any obligation for providers to notify subscribers about subpoenas, court orders, or search warrants under Section 2703. However, many have voluntarily adopted policies of notifying subscribers about such legal requests. Accordingly, when necessary, Section 2705(b) of the SCA enables the Government to obtain a court order to preclude such notification. In relevant part, Section 2705(b) provides as follows:¹

(b) Preclusion of notice to subject of governmental access. — A governmental entity acting under section 2703 . . . may apply to a court for 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

¹ Section 2705(b) contains additional requirements for legal process obtained pursuant to 18 U.S.C. § 2703(b)(1)(B), but the Government does not seek to use the proposed Order for any legal process under that provision.

deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in —

- (1) endangering the life or physical safety of an individual;
- (2) flight from prosecution;
- (3) destruction of or tampering with evidence;
- (4) intimidation of potential witnesses; or
- (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

18 U.S.C. § 2705(b). The United States District Court for the District of Columbia has made clear that a nondisclosure order under Section 2705(b) must be issued once the Government makes the requisite showing about potential consequences of notification:

The explicit terms of section 2705(b) make clear that if a courts [sic] finds that there is reason to believe that notifying the customer or subscriber of the court order or subpoena may lead to one of the deleterious outcomes listed under § 2705(b), the court must enter an order commanding a service provider to delay notice to a customer for a period of time that the court determines is appropriate. Once the government makes the required showing under § 2705(b), the court is required to issue the non-disclosure order.

In re Application for Order of Nondisclosure Pursuant to 18 U.S.C. § 2705(b) for Grand Jury Subpoena #GJ2014031422765, 41 F. Supp. 3d 1, 5 (D.D.C. 2014).

5. Accordingly, this motion to seal sets forth facts showing reasonable grounds to command Google not to notify any other person (except attorneys for Google for the purpose of receiving legal advice) of the existence of the Warrant for a period of one year unless otherwise ordered by the Court.

FACTS SUPPORTING SEALING AND NON-DISCLOSURE

6. At the present time, law enforcement officers of the FBI are conducting an investigation into violations related to 18 U.S.C. § 2 (aiding and abetting), 18 U.S.C. § 3 (accessory

after the fact), 18 U.S.C. § 4 (misprision of a felony), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1030 (unauthorized access of a protected computer); 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1349 (attempt and conspiracy to commit wire fraud), and 52 U.S.C. § 30121 (foreign contribution ban) arising out of the conduct of various unknown persons that operated and controlled the subject accounts. It does not appear that these individuals are currently aware of the nature and scope of the ongoing FBI investigation.

REQUEST FOR SEALING AND NON-DISCLOSURE

7. In this matter, the government requests that the Warrant be sealed until further order of the Court and that Google and its employees be directed not to notify any other person of the existence or content of the Warrant (except attorneys for Google for the purpose of receiving legal advice) for a period of one year unless otherwise ordered by the Court. Such an order is appropriate because the Warrant relates to an ongoing criminal investigation, the full scope of which is neither public nor known to the targets of the investigation, and its disclosure may alert these targets to the ongoing investigation and its scope. Once alerted to this investigation, potential targets would be immediately prompted to destroy or conceal incriminating evidence, alter their operational tactics to avoid future detection, and otherwise take steps to undermine the investigation and avoid future prosecution. In particular, given that they are known to use electronic communication and remote computing services, the potential target could quickly and easily destroy or encrypt digital evidence relating to their criminal activity.

8. Given the complex and sensitive nature of the criminal activity under investigation, and also given that the criminal scheme may be ongoing, the Government anticipates that this confidential investigation will continue for the next year or longer. However, should circumstances

change such that court-ordered nondisclosure under Section 2705(b) becomes no longer needed, the Government will notify the Court and seek appropriate relief.

9. There is, therefore, reason to believe that notification of the existence of the Warrant will seriously jeopardize the investigation, including by giving the targets an opportunity to flee from prosecution, destroy or tamper with evidence, and intimidate witnesses. *See* 18 U.S.C. § 2705(b)(2)–(5). Because of such potential jeopardy to the investigation, there also exists a compelling governmental interest in confidentiality to justify the government’s sealing request. *See Robinson*, 935 F.2d at 287–89.

10. Based on prior dealings with Google, the United States is aware that, absent a court order under Section 2705(b) commanding Google not to notify anyone about a legal request, it is Google’s policy and practice, upon receipt of a warrant seeking the contents of electronically stored wire or electronic communications for a certain account, to notify the subscriber or customer of the existence of the warrant prior to producing the material sought.

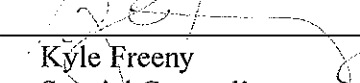
WHEREFORE, for all the foregoing reasons, the government respectfully requests that the above-captioned warrant, the application and affidavit in support thereof, and all attachments thereto and other related materials be placed under seal, and furthermore, that the Court command Google not to notify any other person of the existence or contents of the above-captioned warrant

(except attorneys for Google for the purpose of receiving legal advice) for a period of one year
unless otherwise ordered by the Court.

Respectfully submitted,

ROBERT S. MUELLER, III
Special Counsel

Dated: 5/4/18

By: 
Kyle Freney
Special Counsel's
Office (202) 616-0800