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

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 [redacted]

Case: 1:17-mj-00760
Assigned To : Howell, Beryl A.
Assign. Date : 10/17/2017
Description: Search and 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 October 31, 2017 *(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: 10/17/2017 at 10:45 A.M. Beryl A. Howell
Judge's signature

City and state: Washington, DC Hon. Beryl A. Howell, Chief U.S. District Judge
Printed name and title

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with the following Google account:

[redacted]

that 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

Particular Things to be Seized

I. Files and Accounts to be produced by Google, Inc. between January 1, 2015 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;

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 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.

06 (Rev. 04/10) Application for a Search Warrant

FILED

OCT 17 2017

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
(Briefly describe the property to be searched or identify the person by name and address)
INFORMATION ASSOCIATED WITH [redacted]

Case: 1:17-mj-00760
Assigned To : Howell, Beryl A.
Assign. Date : 10/17/2017
Description: Search and Seizure Warrant

APPLICATION FOR A SEARCH WARRANT

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

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.

This warrant is sought pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A).

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. § 1030	Fraud and Related Activities in Connection with Computers Agents
18 U.S.C. § 2	Aiding and Abetting
22 U.S.C. § 371	Conspiracy to Commit an Offense Against the United States

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.

Amy Anderson
Applicant's signature

Reviewed by AUSA/SAUSA:

Aaron Zelinsky (ASC)

Amy Anderson, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 10/17/2017

Beryl A. Howell
Judge's signature

City and state: Washington, D.C.

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

FILED

OCT 17 2017

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

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
[redacted]

Case: 1:17-mj-00760
Assigned To : Howell, Beryl A.
Assign. Date : 10/17/2017
Description: Search and Seizure Warrant

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Amy Anderson, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the email account [redacted] (hereafter the "**Target Account**"), that 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. The information to be disclosed by Google and searched by the government 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).

2. I am a Special Agent with Federal Bureau of Investigation ("FBI") assigned to FBI Headquarters working directly with the Special Counsel's Office. I have been a Special Agent with the FBI since 2010. Since then, I have conducted national security investigations of foreign intelligence services, espionage, and counter proliferation matters. I have training and experience related to espionage and foreign intelligence services national security investigations. I have conducted and participated in various investigations involving multiple threat countries as well as national security threats and applicable criminal violations.

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 Account** contains communications relevant to violations of 18 U.S.C. § 1030 (fraud and related activities in connection with computers), 18 U.S.C. § 2 (aiding and abetting), and 18 U.S.C. § 371 (conspiracy to commit an offense against the United States).

5. As set forth below, Roger STONE communicated directly via Twitter with WikiLeaks, Julian Assange, and Guccifer 2.0, a Twitter account used by Russian intelligence to disseminate hacked information. STONE, using his [redacted] Account, also emailed instructions to Jerome CORSI to "Get to Assange" in person at the Ecuadorian Embassy and "get pending WikiLeaks emails[.]" CORSI emailed STONE back on his [redacted] Account that it was "Time to let more than Podesta to be exposed" (before any of Podesta's were leaked). After Podesta's emails were leaked, CORSI emailed STONE "talking points" about Podesta to the **Target Account**. CORSI also emailed the **Target Account** to convey information "from a very trusted source" regarding Julian ASSANGE, WikiLeaks, and potential future disclosures. In addition, STONE used the **Target Account** to continue conversations via email that he began on Twitter and forwarded emails, including at least one related to WikiLeaks, from his [redacted] account to the **Target Account**.

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 7.

PROBABLE CAUSE

A. The 2016 Email Hack and Russia's Use of "Guccifer 2.0" and WikiLeaks to Disseminate Hacked Information.

7. According to the public and unclassified intelligence report conducted by the United States Intelligence Community, the Russian military intelligence (General Staff Main Intelligence Directorate or "GRU") probably began cyber operations aimed at the U.S. election by March 2016. The GRU operations resulted in the compromise of the personal e-mail accounts of Democratic National Committee (DNC) and other Democratic Party officials and political figures. By May 2016, the GRU had exfiltrated large volumes of data from the DNC. The DNC headquarters is located at 430 South Capitol Street SE, Washington, D.C. 20003.

8. The public and unclassified intelligence report assessed that the GRU used a Twitter account, "Guccifer 2.0," as well as the websitesDCLeaks.com, and WikiLeaks to release U.S. victim data obtained in the cyber operations publicly and in exclusives to media outlets. Guccifer 2.0, who claimed to be an independent Romanian hacker, made multiple contradictory statements and false claims about his likely Russian identity throughout the election. Press reporting suggests more than one person claiming to be Guccifer 2.0 interacted with journalists.

B. Roger Stone's Publicly Disclosed Interactions with Guccifer 2.0 and WikiLeaks.

9. 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.

10. As discussed further below, Stone made a number of public references to WikiLeaks and its release of DNC-related emails. Stone has also stated that he was in contact via Twitter with Guccifer 2.0.

11. 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.

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

13. 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."

14. 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.

15. 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).

16. 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.

17. On August 14, 2016, Stone sent a private message on Twitter using @RogerJStoneJr to Guccifer 2.0, stating he was "delighted" to see the user's Twitter handle reinstated after having been suspended.[1]

18. On August 15, 2016, Guccifer 2.0 replied to Stone at @RogerJStoneJr, stating: "wow. thank u for writing back, and thank u for an article about me!!! did you find anything interesting in the docs I posted."

---

[1] These messages were released by Stone on March 10, 2017, as described further below in paragraph ~~28.~~ 29 AEA

19. On August 16, 2016, Stone sent a private message using @RogerJStoneJr asking Guccifer to retweet an article he had written regarding the 'rigg[ing]' of the 2016 presidential elections.

20. 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."

21. 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 working with a Washington D.C.-based lobbying firms to influence U.S. policy toward Ukraine.

22. 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."

23. 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."

24. On Saturday, October 1, 2016, using @RogerJStoneJr, Stone Tweeted, "Wednesday @ HillaryClinton is done. #WikiLeaks."

25. On Sunday, October 2, 2016, MSNBC Morning Joe producer Jesse Rodriquez 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."

26. 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.

27. Approximately a half hour later, at 4:32 P.M., WikiLeaks send 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.

28. 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."

29. On March 10, 2017, Stone spoke with *The Washington Times* and acknowledged he had been in contact with Guccifer 2.0 using @RogerJStoneJr. Stone publicly stated that he had been in contact with Guccifer 2.0 regarding the DNC hack, and that he had used Twitter's private message system to do so. Stone provided a copy of the private messages to *The Washington Times*.

30. 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.

31. On August 7, 2017, Chief Judge Beryl A. Howell issued a search warrant for the Twitter account @RogerJStoneJr. Contrary to Stone's representation to CNN that he "never communicated with WikiLeaks," Stone in fact communicated via private direct messaging with WikiLeaks during the Campaign. Stone also used the @RogerJStoneJr Twitter account's private direct messaging system to communicate directly with Julian Assange since at least June 2017.

32. For example, 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 has also recently 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. Roger Stone's Emails Regarding WikiLeaks, Julian Assange, Russia, and John Podesta

38. On September 11, 2017, Chief Judge Beryl A. Howell of the District of Columbia issued a search warrant for STONE's [redacted] address, [redacted] (the "[redacted] Account"). Emails recovered pursuant to that search warrant indicated the following:

39. On July 25, 2016, STONE sent an email from his [redacted] Account to JEROME CORSI, an author and political commentator, 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."

40. On or about August 2, 2016 (approximately 19 days before STONE publicly tweeted about "Podesta's time in the barrel"), CORSI emailed the [redacted] Account, "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." Based on my training, experience, and review of materials in this case, it appears 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.

41. On or about August 16, 2016, CORSI emailed the **Target Account** link to a piece CORSI had written about STONE titled, "Trump Adviser: WikiLeaks Plotting Email Dump to Derail Hillary."

42. On or about August 31, 2016, CORSI emailed the [redacted] Account: "Did you get the Podesta writeup." STONE replied "yes."

43. On or about September 6, 2016, CORSI emailed the [redacted] Account: "Roger[,] Is NY Post going to use the Pedesta [sic] stuff?"

44. On or about October 4, 2016 STONE forwarded an email from his [redacted] Account to the **Target Account** with the subject line "Comment on WikiLeaks?" The email, from a reporter, asked STONE for any comment on the "lack of an 'October surprise' release from WikiLeaks today?"

45. On or about October 7, 2016, WikiLeaks began releasing the Podesta emails.

46. On or about October 12, 2016, the same day on which Podesta accused STONE of having advance knowledge of the publication of his emails, CORSI emailed STONE on both the **Target Account** and the [redacted] Account, with a subject line "Podesta talking points." Attached to the email was a file labeled, "ROGER STONE podesta talking points Oct 12 2016.docx." The "talking points" included the statement that, "Podesta is at the heart of a Russian-government money laundering operation that benefits financially Podesta personally and the Clintons through the Clinton Foundation." CORSI followed up several minutes later with another email to the

Target Account and the [redacted] Account titled, "Podesta talking points," with the text "sent a second time just to be sure you go it." STONE emailed CORSI back via the [redacted] Account, "Got them and used them."

47. On or about October 17, 2016, CORSI emailed the **Target Account** and the [redacted] Account with the subject, "Fwd: ASSANGE…URGENT…" CORSI wrote, "From a very trusted source," and forwarded an email with the header information stripped out, showing only the body text. The email read, "Yes[.] I figured this. Assange is threatening Kerry, Ecuador and U.K. He will drop the goods on them if they move to extradite him. My guess is that he has a set of dead man files that include Hillary. It's what they used to call a 'Mexican stand off[.]' Only hope is that if Trump speaks out to save him[.] Otherwise he'd dead anyway, once he's dropped what he has. If HRC wins, Assange can kiss his life away. Interesting gambit Assange has to play out. He's called Podesta's bluff and raised him the election."

48. On or about January 7, 2017, [redacted] emailed the **Target Account**, the [redacted] Account, CORSI, and [redacted] with the subject line, "in case you need his mail……" Attached to the message was a scan of a business card for John Podesta. Several hours later, [redacted] replied to all recipients, including the **Target Account**, "Ha… maybe he wants to go phishing with us?"

49. I know from my training and experience that the term "phishing" is used to refer to the practice of sending emails purporting to be from a reputable party in order to induce individuals to reveal personal information, including passwords. Public reports indicate that Podesta's emails were obtaining through a "phishing" scheme.

E. Roger Stone's Use of the Target Account to Continue Conversations Begun on Twitter Direct Message.

50. STONE has also used **Target Account** to continue conversations began via Twitter direct message. For example, on August 18, 2016, an individual sent @RogerJStoneJr a direct message asking "know where to send information to" regarding "Presidential polls and why cycle favors Trump." Stone responded: "[**Target Account**]."

51. On August 19, 2017, an individual sent a direct message to @RogerJStoneJr concerning an offer for "$500 for a 30 minute phone call," stating that "My audience would be fascinated by discussion." The individual then direct messages Stone, "Hi Roger! I'm striking out with your rep. Hoping we can swing something this week. My offer still stands." @RogerJStoneJr wrote back: "Email me direct **[Target Account]**."

BACKGROUND CONCERNING GOOGLE

52. 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 storage, file sharing, and collaborative editing. Google+ Photos (formerly knowns 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.

53. In my training and experience, in addition to information such as search history can help to show the state of mind of an individual at the time the search was made, as well as the individuals potential advance knowledge of events, as they search to see if the anticipated event has occurred. Individuals who communicate via Gmail also often use other Google products, including Google Talk, to communicate, and Google Drive to store or transfer, open, or edit files.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

54. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) associated with the account in Attachment A and particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachments B, government-authorized persons will review that information to locate the items described in Section II of Attachments B. The items identified in Attachments A and B will also be screened by reviewers not on the prosecution team to identify and filter out privileged material.

CONCLUSION

55. STONE instructed CORSI via the [redacted] Account to "Get to Assange" at the Ecuadorian Embassy regarding upcoming leaks, and CORSI emailed Stone on the [redacted] Account that it was "Time to let more than Podesta to be exposed as in bed w enemy if they are not ready to drop HRC." CORSI later emailed STONE "talking points" about Podesta to the **Target Account**, and also emailed the **Target Account** to convey information "from a very trusted source" regarding ASSANGE, WikiLeaks, and potential disclosure. STONE also used

the **Target Account** to continue conversations via email that he began on Twitter and forwarded emails related to WikiLeaks from the [redacted] Account to the **Target Account**. There is therefore probable cause to believe that evidence of the DNC hack and the hacking of other emails associated with the 2016 election will be found in the information associated with the **Target Account**.

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

57. 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.

REQUEST FOR SEALING

58. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation, the full nature and extent of which is not known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

Amy Anderson
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on this 17th day of October, 2017.

The Honorable Beryl A. Howell
Chief United States District Judge

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with the following Google account:

[redacted]

that 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

Particular Things to be Seized

I. Files and Accounts to be produced by Google, Inc. between January 1, 2015 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;

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 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 accounts described in Attachment A which consists of evidence, fruits, or instrumentalities of violations of 18 U.S.C.§ 1030 (fraud and related activities in connection with computers), 18 U.S.C. § 2 (aiding and abetting), and 18 U.S.C. § 371 (conspiracy to commit an offense against the United States), for the period January 2015 to the present, including:

All records, information, documents or tangible materials that relate in any way to communications regarding hacking, release of hacked material, communications with persons or entities associated with WikiLeaks, including but not limited to Julian Assange;

b. All images, messages, communications, calendar entries, search terms, and contacts, including any and all preparatory steps taken in furtherance of the above-listed offenses;

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.