

**FILED**

## UNITED STATES DISTRICT COURT

NOV - 6 2017

for the  
District of ColumbiaClerk, U.S. District & Bankruptcy  
Courts 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 TWITTER  
 ACCOUNTS [REDACTED]

Case: 1:17-mj-00821  
 Assigned To : Howell, Beryl A.  
 Assign. Date : 11/6/2017  
 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:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 1030	Fraud and Related Activities in Connection with Computers
18 U.S.C. § 371, § 2	Conspiracy Against the United States, Aiding and Abetting
50 U.S.C. § 30121	Foreign Contribution Ban

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 (ASC)

  
 Applicant's signature

Amy Anderson, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 11/6/2017

City and state: Washington, D.C.

  
 Judge's signature

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

Printed name and title

**FILED**

**NOV - 6 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 THE  
TWITTER ACCOUNT [REDACTED] AND  
[REDACTED]

Case: 1:17-mj-00821

Assigned To : Howell, Beryl A.

Assign. Date : 11/6/2017

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 Twitter Accounts [REDACTED] (hereafter "**Target Account 1**") and [REDACTED] (hereafter "**Target Account 2**"), that is stored at premises owned, maintained, controlled, or operated by Twitter, a social-networking company headquartered in San Francisco, CA. The information to be disclosed by Twitter 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") 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, foreign intelligence services, and 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 certain individuals with whom the **Target Accounts** were in communication have committed violations of 18 U.S.C. § 1030 (fraud and related activities in connection with computers), 50 U.S.C. § 30121 (foreign contribution ban), 18 U.S.C. § 2 (aiding and abetting), 18 U.S.C. § 371 (conspiracy to commit an offense against the United States), and that communications related to these violations will be found on the **Target Accounts**. There is therefore probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

5. As detailed further below, from on or about June 22, 2016, through at least on or about July 17, 2016, **Target Account 1**, belonging to WikiLeaks, exchanged numerous direct messages concerning hacked information with Guccifer 2.0, which was a Twitter account used by the Russian Government to release data obtained through hacking accounts of U.S. users. **Target Account 1** also sent direct messages via Twitter concerning a “guessed” password for the website “[REDACTED]” to [REDACTED] **Target Account 2** belongs to Julian Assange, the founder of WikiLeaks. Beginning no later than on or about July 2016, former Campaign adviser Roger Stone was in contact with Assange via an intermediary regarding upcoming leaks of hacked information obtained by WikiLeaks. In addition, Assange, using **Target Account 2**, communicated directly with Stone beginning no later than on or about April 7, 2017. Stone stated to **Target Account 2** that he was “doing everything possible to address the issues [related

to WikiLeaks] at the highest level of Government,” and that he and **Target Account 2** “must be circumspect in this forum as experience demonstrates it is monitored.”

### 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 in paragraph 9.

### PROBABLE CAUSE

#### **A. Background on the Target Accounts, Julian Assange, and Roger Stone.**

7. **Target Account 1** is the public account of WikiLeaks. As detailed further below, it frequently has been used to release hacked information, including during the 2016 election. **Target Account 2** is the public account of Julian Assange. **Target Account 2** has over 500,000 followers, but only follows one account, **Target Account 1**. **Target Account 2** frequently tweets information related to WikiLeaks and tags **Target Account 1**.

8. Julian Assange is the founder of WikiLeaks. According to the publicly-accessible profile of **Target Account 2**, Assange currently is the “Publisher @WikiLeaks [**Target Account 1**].” **Target Account 2**’s profile contains a link to the website “IamWikiLeaks.org/donate.” According to publicly-available press reporting, Assange began hacking secure computer systems when he sixteen years old, in 1987. On or about December 1996, Assange pled guilty in Australia to twenty-five charges related to hacking secure computer systems. In 2006, Assange and others established WikiLeaks, and he previously described himself as WikiLeaks’s Editor-



in-Chief. Assange has stated in public interviews that he is deeply involved in running WikiLeaks. Referring to the DNC emails, Assange stated in an August, 2017 interview that, “We had quite some difficulties to overcome, in terms of the technical aspects, and making sure we were comfortable with the forensics,” and that “You have to get close and interact with it, then you start to get a feel.” Assange indicated that only a small number of people, including himself, worked on the release of the DNC emails. Assange stated in August 2016 to a news organization that, “We are working around the clock. We have received quite a lot of material.”

9. Roger Stone is a self-employed political strategist/consultant and has been actively involved in U.S. politics since 1975. Stone officially worked on the presidential campaign of Donald J. Trump (the “Campaign”) until 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. After Stone’s public departure from the Campaign, Stone continued to correspond with individuals related to the Campaign, including Paul Manafort (who worked for a time as Campaign manager), Rick Gates (a campaign adviser), and Jason Miller (Campaign spokesman). As discussed further below, Stone made a number of public references to WikiLeaks, Julian Assange, and the release of DNC-related emails.

**B. The DNC Email Hack and Russia’s Use of “Guccifer 2.0” and WikiLeaks to Disseminate Hacked Information.**

10. According to the public and unclassified intelligence report prepared by the United States Intelligence Community, Russian intelligence gained access to the Democratic National Committee (DNC) networks in July 2015 and maintained that access until at least June 2016. By March 2016, the Russian military intelligence (General Staff Main Intelligence

Directorate or “GRU”) probably began cyber operations aimed at the U.S. election. The GRU operations resulted in the compromise of personal e-mail accounts within the DNC and other Democratic Party officials and political figures. By in or about 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.

11. The public and unclassified intelligence report assessed that:

- a. The GRU used a Twitter account, “Guccifer 2.0” and the website DCLeaks.com to release the U.S. victim data obtained in cyber operations publicly and in exclusives to media outlets and relayed material to WikiLeaks.
- b. 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.
- c. Content that was taken from e-mail accounts targeted by the GRU in March 2016 appeared on DCLeaks.com starting in June 2016.
- d. The GRU relayed material it acquired from the DNC and senior Democratic officials to WikiLeaks. WikiLeaks was mostly likely chosen because of its self-proclaimed reputation for authenticity. Disclosures through WikiLeaks did not contain any evident forgeries.
- e. The Kremlin’s principal international propaganda outlet RT (formerly Russia Today) has actively collaborated with WikiLeaks. RT’s editor-in-chief visited WikiLeaks founder Julian Assange at the Ecuadorian Embassy in London in August 2013, where they discussed renewing his broadcast contract with RT, according to Russian and Western media. Russian media has subsequently announced that RT had



become “the only Russian media company” to partner with WikiLeaks and had received access to “new leaks of secret information.”

f. On or about August 6, 2016, RT published an English-language video called “Julian Assange Special: Do WikiLeaks Have the E-Mail That’ll Put Clinton in Prison?” and an exclusive interview with Assange entitled “Clinton and ISIS Funded by the Same Money.”

12. On or about June 14, 2016, the Washington Post reported that “Russian government hackers” had penetrated the DNC computer network and stole opposition research on Donald J. Trump. The Kremlin’s spokesman denied any Russian involvement in the hack.

13. On or about June 15, 2016, Guccifer 2.0 claimed responsibility for the DNC hack and began posting hacked documents.

14. As detailed further below, on or about June 22, 2016, Guccifer 2.0 and **Target Account 1** initiated communication via Twitter private messaging regarding the transfer and release of hacked information, including the hacked email accounts related to the DNC.

15. On or about July 22, 2016, WikiLeaks published about 20,000 emails stolen from the DNC. Using **Target Account 1**, WikiLeaks publicly tweeted: “WikiLeaks releases thousands of documents about Clinton and internal deliberations” and linked to a Washington Post article and [www.wikileaks.org/dnc-emails/](http://www.wikileaks.org/dnc-emails/).

16. On or about August 12, 2016, Guccifer 2.0 released personal cellphone numbers and email addresses from the files of the Democratic Congressional Campaign Committee (DCCC).

17. On or about August 21, 2016, Roger Stone directed a publicly-available 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."

18. On or about September 13, 2016, **Target Account 1** tweeted a public message stating, "678.4 MB of new 'DNC documents' from @Guccifer\_2," with a link to a publicly available file.

19. 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.

20. Approximately a half hour later, at 4:32 P.M., **Target Account 1** sent out 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. WikiLeaks, via **Target Account 1**, continued to release John Podesta's hacked emails throughout October 10-14, 2016.

### **C. Communications Between the Target Account 1 and Guccifer 2.0**

21. On July 7, 2017 Magistrate Judge Maria-Elena James of the Northern District of California issued a search warrant for the Twitter Account associated with Guccifer 2.0. The communications obtained from the account are detailed further below.



22. On or about June 22, 2016, WikiLeaks sent Guccifer 2.0 sent a direct message (DM) stating “Do you have secure communications?” **Target Account 1** stated, “Send any new material here for us to review and it will have a much higher impact than what you are doing. No other media will release the full material.” Guccifer 2.0 replied, “what can u suggest for a secure connection? Soft, keys, etc? I’m ready to cooperate with you, but I need to know what’s in your archive 80gb? Are there only HRC emails? Or some other docs? Are there any DNC docs? If it’s not secret when you are going to release it?” **Target Account 1** wrote back, “You can send us a message in a .txt file here,” and attached a web link. Guccifer 2.0 responded, “do you have GPG?” I know from my training and experience that “GPG” refers to a program for exchanged encrypted information.

23. On or about June 24, 2016, Guccifer 2.0 wrote to **Target Account 1**, “How can we chat? Do u have jabber or something like that?” I know from my training and experience that “Jabber” is an instant messaging service. **Target Account 1** wrote back, “Yes, we have everything. We’ve been busy celebrating Brexit. You can also email an encrypted message to office@wikileaks.org. They key is here.”<sup>1</sup> A web link was attached to the message. I know from my training and experience that an encryption “key” is a string of information created for scrambling and unscrambling data.

24. On or about June 27, 2016, Guccifer 2.0 wrote to **Target Account 1**, “Hi, [I]’ve just sent you an email with a text message encrypted and an open key.” **Target Account 1** wrote back, “Thanks.” Guccifer 2.0 replied, “waiting for ur response. I send u some interesting piece.”

---

<sup>1</sup>**Target Account 1** sent each sentence as a separate message, though close in time. These messages have been consolidated into a single quote for ease of reading. The same is done below with other close in time messages.

25. On or about July 4, 2016, Guccifer 2.0 wrote to **Target Account 1**, “hi there, check up r email, waiting for [r]epley.”

26. On or about July 6, 2016, Guccifer 2.0 wrote to **Target Account 1**, “have u received my parcel?” **Target Account 1** responded, “Not unless it was very recent. [we haven’t checked in 24h].”<sup>2</sup> Guccifer 2.0 replied, “I sent it yesterday, an archive of about 1 gb. via [website link]. [A]nd check your email.” **Target Account 1** wrote back, “Wil[l] check, thanks.” Guccifer 2.0 responded, “let me know the results.” **Target Account 1** wrote back, “Please don’t make anything you send to us public. It’s a lot of work to go through it and the impact is severely reduced if we are not the first to publish.” Guccifer 2.0 replied, “agreed. How much time will it take?” **Target Account 1** responded, “likely sometime today.” Guccifer 2.0 wrote back, “will u announce a publication? and what about 3 docs [I] sent u earlier?” **Target Account 1** responded, “I don’t believe we received them. Nothing on ‘Brexit’ for example.” Guccifer 2.0 wrote back, “wow. have you checked ur mail?” **Target Account 1** replied, “At least not as of 4 days ago. . . . For security reasons mail cannot be checked for some hours.” Guccifer 2.0 wrote back, “fuck, [I] sent 4 docs on brexit on jun 29, an archive in gpg[.] ur submission form is too fucking slow, [I] spent the whole day uploading 1 gb.” I know from my training and experience that the term “gb” is an abbreviation for “gigabyte,” a unit of measurement of information stored on a computer.

27. **Target Account 1** wrote back, “We can arrange servers 100x as fast. The speed restrictions are to anonymise the path. Just ask for custom fast upload point in an email.” Guccifer 2.0 wrote, “will u be able to check ur email?” **Target Account 1** responded, “We’re best with very large data sets. e.g. 200gb. these prove themselves since they’re too big to fake.”

---

<sup>2</sup> The brackets appear in the original message.



Guccifer 2.0 responded, “or shall I send brexit docs via submission once again?” **Target Account 1** responded, “to be safe, send via [web link].”

28. On or about that same day, Guccifer 2.0 wrote, “can u confirm u received dnc emails?” **Target Account 1** wrote back several messages later, “for security reasons we can’t confirm what we’ve received here. e.g., in case your account has been taken over by us intelligence and is probing to see what we have.” Guccifer 2.0 responded, “then send me an encrypted email.” **Target Account 1** wrote back, “we can do that. but the security people are in another time zone so it will need to wait some hours.” **Target Account 1** wrote, “what do you think about the FBI’s failure to charge? To our mind the clinton foundation investigation has always been the more serious. we would be very interested in all the emails/docs from there. She set up quite a lot of front companies. e.g in sweden.” Guccifer 2.0 responded, “ok, [I]’ll be waiting for confirmation. [A]s for investigation, they have everything settled, or else I don’t know how to explain that they found a hundred classified docs but fail to charge her.” **Target Account 1** responded, “She’s too powerful to charge at least without something stronger. [A]s far as we know, the investigation into the clinton foundation remains open[.] [W]e hear the FBI are unhappy with Loretta Lynch over meeting Bill, because he’s a target in that investigation.”

29. On or about that same day, Guccifer 2.0 wrote to **Target Account 1**, “[D]o you have any info about marcel lazar? There’ve been a lot of rumors of late.” “Marcel Lazar” is the name of a Romanian Hacker who used the pseudonym “Guccifer,” and who pled guilty on May 25, 2016 in the Eastern District of Virginia to hacking the personal accounts of a variety of victims, including a former U.S. president. According to publicly available reporting, in May 2016, Lazar also claimed to have hacked the email served belonging to then-candidate Clinton. Lazar stated, “For me, it was easy . . . easy for me, for everybody.” Lazar’s claims have not been

substantiated, and the undersigned is not aware of evidence indicating Lazar accomplished the hack.

30. **Target Account 1** wrote back, "the death? [A] fake story." **Target Account 1** messaged: "His 2013 screen shots of Max Blumenthal's inbox prove that Hillary secretly deleted at least one email about Libya that was meant to be handed over to Congress. So we were very interested in his co-operation with the FBI." Guccifer 2.0 wrote back, "some dirty games behind the scenes [I] believe[.] Can you send me an email now?" **Target Account 1** wrote back, "No; we have not been able to activate the people who handle it. Still trying." Guccifer 2.0 replied, "what about tor submission? [W]ill u receive a doc now?" **Target Account 1** replied, "We will get everything sent on [weblink]." [A]s long as you see \"upload succseful\" at the end. [I]f you have anything hillary related we want it in the next tweeo [sic] days prefable [sic] because the DNC is approaching and she will solidify bernie supporters behind her after." Guccifer 2.0 responded, "ok. I see."

31. **Target Account 1** wrote, "[W]e think the public interest is greatest now and in early october." Guccifer 2.0 responded, "do u think a lot of people will attend bernie fans rally in philly? Will it affect the dnc anyhow?" **Target Account 1** wrote, "bernie is trying to make his own faction leading up to the DNC. [S]o he can push for concessions (positions/policies) or, at the outside, if hillary has a stroke, is arrested etc, he can take over the nomination. [T]he question is this: can bernies supporters+staff keep their coherency until then (and after). [O]r will they dis[s]olve into hillary's camp? [P]resently many of them are looking to damage hilary [sic] inorder [sic] to increase their unity and bargaining power at the DNC. Doubt one rally is going to be that significant in the bigger scheme. [I]t seems many of them will vote for hillary just to prevent trump from winning."



32. On or about that same day, Guccifer 2.0 sent **Target Account 1** a message reading, "sent brexit docs successfully." **Target Account 1** responded, "(:)))". **Target Account 1** wrote back, "we think trump has only about a 25% chance of winning against hillary so conflict between bernie and hillary is interesting." Guccifer 2.0 responded, "so it is." **Target Account 1** wrote, "also, it's important to consider what type of president hillary might be. If bernie and trump retain their groups past 2016 in significant number, then they are a restraining force on hillary."

33. On or about July 7, 2016, **Target Account 1** wrote, "All good?" Guccifer 2.0 responded, "yeah, what about u? is smth wrong?" I know from my training and experience that "smth" is used as an abbreviation for "something." **Target Account 1** wrote back, "No. All good." Guccifer 2.0 wrote back, "are working with the emails [I] sent u? [C]heck ur email. [I] sent u a check archive from another email box. fuck, mail undelivered. [D]o you have another way to receive large volumes of data? [B]esides for tor submission form?"

34. On or about July 11, 2016, Guccifer 2.0 wrote to **Target Account 1**, "sent it via ur submission. check it."

35. On or about July 13, 2016, Guccifer 2.0 wrote, "r u there?" On or about July 14, 2016, Guccifer 2.0 wrote, "ping. Check ur email. sent u a link to a big archive and a pass." **Target Account 1** replied, "great, thanks; can't check until tomorrow though."

36. On or about July 17, 2016, Guccifer 2.0 wrote, "what bout now?" On or about July 18, 2016, **Target Account 1** responded, "have the 1Gb or so archive." Guccifer 2.0 responded, "have u managed to extract the files?" **Target Account 1** responded, "yes. turkey coup has delayed us a couple of days. [O]therwise all ready[.]" Guccifer 2.0 responded, "so when r u about to make a release?" **Target Account 1** wrote back, "this week. [D]o you have

any bigger datasets? [D]id you get our fast transfer details?" Guccifer 2.0 wrote back, "i'll check it. did u send it via email? **Target Account 1** responded, "yes." Guccifer 2.0 replied, "to [web link]. [I] got nothing." **Target Account 1** wrote, "check your other mail? this was over a week ago." Guccifer 2.0 wrote back, "oh, that one, yeah, [I] got it."

37. On or about July 18, 2016, **Target Account 1** wrote, "great. [D]id it work?" Guccifer 2.0 wrote back, "[I] haven't tried yet." **Target Account 1** responded, "Oh. We arranged that server just for that purpose. Nothing bigger?" Guccifer 2.0 wrote back, "let's move step by step, u have released nothing of what [I] sent u yet." **Target Account 1** replied, "How about you transfer it all to us encrypted. [T]hen when you are happy, you give us the decrypt key. [T]his way we can move much faster. [A]lso it is protective for you if we already have everything because then there is no point in trying to shut you up." Guccifer 2.0 wrote back, "ok, i'll ponder it."

#### **D. Contacts Involving the Julian Assange, Roger Stone, and the Target Accounts**

38. Approximately eight days after the last communication between Guccifer 2.0 and WikiLeaks described above, on or about July 25, 2016, Stone sent an email to Jerome Corsi, an author and political commentator, with the subject line, "Get to Assange."<sup>3</sup> The body of the message read: "Get to Assange [a]t Ecuadorian Embassy in London and get the pending wikileaks emails...they deal with Foundation, allegedly."

39. On or about August 2, 2016, Corsi emailed 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

---

<sup>3</sup> 1. On August 7, 2017, Chief Judge Beryl A. Howell of the District of Columbia issued a search warrant for Roger Stone's Twitter account, @RogerJStoneJr. On September 11, 2017, Chief Judge Beryl A. Howell of the District of Columbia issued a search warrant for Stone's Hotmail address, [REDACTED]. The relevant results of those search warrants are summarized in the paragraphs which follow.



...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 user of **Target Account 2**), the founder of WikiLeaks, who resided in Ecuador’s London Embassy in 2016.

40. On or about August 16, 2016, Corsi emailed Stone a link to a piece Corsi had written about Stone titled, “Trump Adviser: Wikileaks Plotting Email Dump to Derail Hillary.”

41. As discussed above, on or about August 21, 2016, Roger Stone directed a publicly-available 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.”

42. On or about August 31, 2016, Corsi emailed Stone: “Did you get the PODESTA write-up.” STONE replied “Yes.”

43. On or about September 6, 2016, Corsi emailed: “Roger[,] Is NY Post going to use the Podesta [sic] stuff?”

44. On or about October 7, 2016, WikiLeaks began releasing emails hacked from John Podesta’s account.

45. WikiLeaks continued to release John Podesta’s hacked emails throughout October 10-21, 2016. On October 12, 2016, John Podesta 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 on or about that same date, 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."

46. On or about that same day, October 12, 2016, Corsi emailed Stone on both the 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 titled, "Podesta talking points," with the text "sent a second time just to be sure you go it." Stone emailed Corsi back, "Got them and used them."

47. On or about the next day, October 13, 2016, Stone sent a private direct message to **Target Account 1** stating, "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 reexamine the strategy of attacking me- cordially R." **Target Account 1** responded, "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."

48. On or about October 16, 2016, Roger Stone wrote to **Target Account 1**, "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."



49. On or about October 17, 2016, Corsi emailed Stone 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 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 if Trump speaks out to save him[.] Otherwise he's 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."

50. The presidential election was held on November 8, 2016.

51. On or about November 9, 2016, **Target Account 1** messaged Roger Stone, "Happy?" and then wrote, "We are now more free to communicate."

52. On or about March 27, 2017, **Target Account 1** wrote to Roger Stone, "FYI, while we continue to be unhappy about false \"back channel\" claims, today CNN deliberately broke our off the record comments."

53. 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."

54. On or about April 7, 2017, Roger Stone wrote to **Target Account 1**, "I am JA's only hope for a pardon the chances of which are actually (weirdly) enhanced by the bombing in Syria (which I opposed) . You have no idea how much your operation leaks. Discrediting me only hurts you. Why not consider saying nothing? PS- Why would anyone listen to that asshole Daniel Ellsberg." Based on my training, experience, and review of materials in this case, I believe that "JA" refers to Julian Assange, the user of **Target Account 2**.

55. On or about April 19, 2017, Assange, using **Target Account 2**, wrote to Stone, "Ace article in infowars. Appreciated. But note that U.S. intel is engages in slight of hand maoevers [sic]. Listen closely and you see they only claim that we received U.S. election leaks \"not directly\" or via a \"third party\" and do not know \"when\" etc. This line is Pompeo appears to be getting at with his \"abbeted\". This correspnds to the same as all media and they do not make any allegation that WL or I am a Russia asset."

56. On or about June 4, 2017, Roger Stone wrote back to **Target Account 2**, "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." **Target Account 2** 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."

57. On or about June 10, 2017, Roger Stone wrote to **Target Account 2**, "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.” **Target Account 2** wrote back, “Appreciated. Of course it is!”

**E. Target Account 1 Sends the “Guessed” Password to “[REDACTED]” to [REDACTED]**

58. During the events described above, **Target Account 1** also engaged in a separate private conversation regarding a “guessed” password to the non-public website “PutinTrump.org.” On or about September 20, 2016, at approximately 9:07PM, **Target Account 1** publicly tweeted, “‘Let’s bomb Iraq’ Progress for America PAC to launch ‘PutinTrump.org’ at 9:30am. Oops pw is [REDACTED] putintrump.org.”

59. On or about September 20, 2016, at approximately 11:59PM, **Target Account 1** sent a private message to a high level individual associated with the Campaign (the “high-level Campaign individual”).<sup>4</sup> The message stated: “A PAC run anti-Trump site [REDACTED] is about to launch. The PAC is a recycled pro-Iraq war PAC. We have guessed the password. It is [REDACTED]. See ‘About’ for who is behind it. Any comments?”

60. According to publicly available reporting, at approximately 9:31AM on or about September 21, 2016, the website “[REDACTED]” was launched. The website was run by individuals who stated they wanted to focus attention to what they described as the “dangerous and unprecedented ties” between Vladimir Putin and Donald J. Trump.

61. On or about September 21, 2016, at approximately 11:50AM (approximately two hours after PutinTrump.org went “live” according to publicly available press accounts), the high-

---

<sup>4</sup> These records were obtained via a search warrant signed by Chief Judge Beryl A. Howell of the District of Columbia on October 12, 2017.

level Campaign individual sent **Target Account 1** a private message: "Off the record I don't know who that is but I'll ask around. Thanks."

### **INFORMATION CONCERNING TWITTER**

62. Twitter owns and operates a free-access social-networking website of the same name that can be accessed at <http://www.twitter.com>. Twitter allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and location information. Twitter also permits users to create and read 140-character messages called "Tweets," and to restrict their "Tweets" to individuals whom they approve. These features are described in more detail below.

63. Upon creating a Twitter account, a Twitter user must create a unique Twitter username and an account password, and the user may also select a different name of 20 characters or fewer to identify his or her Twitter account. The Twitter user may also change this username, password, and name without having to open a new Twitter account.

64. Twitter asks users to provide basic identity and contact information, either during the registration process or thereafter. This information may include the user's full name, e-mail addresses, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers. For each user, Twitter may retain information about the date and time at which the user's profile was created, the date and time at which the account was created, and the Internet Protocol ("IP") address at the time of sign-up. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a given Twitter account.

65. A Twitter user can post a personal photograph or image (also known as an "avatar") to his or her profile, and can also change the profile background or theme for his or her



account page. In addition, Twitter users can post “bios” of 160 characters or fewer to their profile pages.

66. Twitter also keeps IP logs for each user. These logs contain information about the user’s logins to Twitter including, for each access, the IP address assigned to the user and the date stamp at the time the user accessed his or her profile.

67. As discussed above, Twitter users can use their Twitter accounts to post “Tweets” of 140 characters or fewer. Each Tweet includes a timestamp that displays when the Tweet was posted to Twitter. Twitter users can also “favorite,” “retweet,” or reply to the Tweets of other users. In addition, when a Tweet includes a Twitter username, often preceded by the @ sign, Twitter designates that Tweet a “mention” of the identified user. In the “Connect” tab for each account, Twitter provides the user with a list of other users who have “favorited” or “retweeted” the user’s own Tweets, as well as a list of all Tweets that include the user’s username (*i.e.*, a list of all “mentions” and “replies” for that username).

68. Twitter users can include photographs or images in their Tweets. Each Twitter account also is provided a user gallery that includes images that the user has shared on Twitter, including images uploaded by other services.

69. Twitter users can also opt to include location data in their Tweets, which will reveal the users’ locations at the time they post each Tweet. This “Tweet With Location” function is off by default, so Twitter users must opt in to the service. In addition, Twitter users may delete their past location data.

70. When Twitter users want to post a Tweet that includes a link to a website, they can use Twitter’s link service, which converts the longer website link into a shortened link that begins with <http://t.co>. This link service measures how many times a link has been clicked.

71. A Twitter user can “follow” other Twitter users, which means subscribing to those users’ Tweets and site updates. Each user profile page includes a list of the people who are following that user (*i.e.*, the user’s “followers” list) and a list of people whom that user follows (*i.e.*, the user’s “following” list). Twitter users can “unfollow” users whom they previously followed, and they can also adjust the privacy settings for their profile so that their Tweets are visible only to the people whom they approve, rather than to the public (which is the default setting). A Twitter user can also group other Twitter users into “lists” that display on the right side of the user’s home page on Twitter. Twitter also provides users with a list of “Who to Follow,” which includes a few recommendations of Twitter accounts that the user may find interesting, based on the types of accounts that the user is already following and who those people follow.

72. In addition to posting Tweets, a Twitter user can also send DMs to one of his or her followers. These messages are typically visible only to the sender and the recipient, and both the sender and the recipient have the power to delete the message from the inboxes of both users. As of January 2012, Twitter displayed only the last 100 DMs for a particular user, but older DMs are stored on Twitter’s database.

73. Twitter users can configure the settings for their Twitter accounts in numerous ways. For example, a Twitter user can configure his or her Twitter account to send updates to the user’s mobile phone, and the user can also set up a “sleep time” during which Twitter updates will not be sent to the user’s phone.

74. Twitter includes a search function that enables its users to search all public Tweets for keywords, usernames, or subject, among other things. A Twitter user may save up to 25 past searches.



75. Twitter users can connect their Twitter accounts to third-party websites and applications, which may grant these websites and applications access to the users' public Twitter profiles.

76. If a Twitter user does not want to interact with another user on Twitter, the first user can "block" the second user from following his or her account.

77. In some cases, Twitter users may communicate directly with Twitter about issues relating to their account, such as technical problems or complaints. Social-networking providers like Twitter typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Twitter may also suspend a particular user for breaching Twitter's terms of service, during which time the Twitter user will be prevented from using Twitter's services.

78. As explained herein, information stored in connection with a Twitter account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Twitter user's account information, IP log, stored electronic communications, and other data retained by Twitter, can indicate who has used or controlled the Twitter account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, communications, "tweets" (status updates) and "tweeted" photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Twitter account at a relevant time. Further, Twitter account activity can show how and when the account was accessed or

used. For example, as described herein, Twitter logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Twitter access, use, and events relating to the crime under investigation. Additionally, Twitter builds geo-location into some of its services. If enabled by the user, physical location is automatically added to “tweeted” communications. This geographic and timeline information may tend to either inculcate or exculpate the Twitter account owner. Last, Twitter account activity may provide relevant insight into the Twitter account owner’s state of mind as it relates to the offense under investigation. For example, information on the Twitter account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a criminal plan) or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

79. Therefore, the computers of Twitter are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Twitter, such as account access information, transaction information, and other account information.

**INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

80. 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 Twitter to disclose to the government copies of the records and other information (including the content of communications) associated with the accounts in Attachment A and



particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

**CONCLUSION**

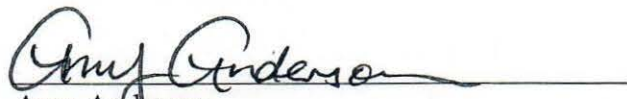
81. Based on the forgoing, I request that the Court issue the proposed search warrant.

82. 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.

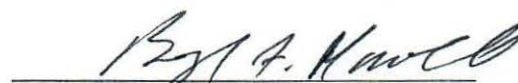
**REQUEST FOR SEALING**

83. 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 4<sup>th</sup> day of November, 2017.

  
The Honorable Beryl A. Howell  
Chief United States District Judge

**ATTACHMENT A**

**Property to Be Searched**

All information that is associated with the Twitter profile with usernames from the period from July 1, 2015 to the present:

@Wikileaks (twitter.com/wikileaks) (**Target Account 1**)

@JulianAssange (twitter.com/JulianAssange) (**Target Account 2**)

that is stored at premises owned, maintained, controlled, or operated by Twitter, a company headquartered in San Francisco, California.



**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Twitter**

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

- a. All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;
- b. All past and current usernames, account passwords, and names associated with the account;
- c. The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;
- d. All IP logs and other documents showing the IP address, date, and time of each login to the account;
- e. All data and information associated with the profile page, including photographs, "bios," and profile backgrounds and themes;
- f. All "Tweets" and Direct Messages sent, received, "favorited," or retweeted by the account, and all photographs or images included in those Tweets and Direct Messages;

- g. All information from the “Connect” tab for the account, including all lists of Twitter users who have favorited or retweeted Tweets posted by the account, as well as a list of all Tweets that include the username associated with the account (*i.e.*, “mentions” or “replies”);
- h. All photographs and images in the user gallery for the account;
- i. All location data associated with the account, including all information collected by the “Tweet With Location” service;
- j. All information about the account’s use of Twitter’s link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the account was clicked;
- k. All data and information that has been deleted by the user;
- l. A list of all of the people that the user follows on Twitter and all people who are following the user (*i.e.*, the user’s “following” list and “followers” list);
- m. A list of all users that the account has “unfollowed” or blocked;
- n. All “lists” created by the account;
- o. All information on the “Who to Follow” list for the account;
- p. All privacy and account settings;
- q. All records of Twitter searches performed by the account, including all past searches saved by the account;
- r. All information about connections between the account and third-party websites and applications;



- s. All records pertaining to communications between Twitter and any person regarding the user or the user's Twitter account, including contacts with support services, and all records of actions taken, including suspensions of the account.

## II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 1030 (fraud and related activities in connection with computers), 50 U.S.C. § 30121 (foreign contribution ban), 18 U.S.C. § 371 (conspiracy to commit an offense against the United States), and 18 U.S.C. § 2 (aiding and abetting) since March 1, 2016 including, for each user ID identified on Attachment A, information pertaining to the following matters:

- a. Any correspondence regarding hacked emails or other data from:
  - i. the Democratic National Committee (DNC)
  - ii. the email belonging to John Podesta (“the email hack”)
  - iii. any other individual related to the 2016 United States election.
- b. Any communications between the **Target Accounts** and individuals associated with the DNC email hack;
- c. Any communications indicating any advance knowledge or direction, planning, or control of the email hack;
- d. Any communications related to the website PutinTrump.Org.
- e. Evidence indicating how and when the Twitter account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Twitter account owner;
- f. Evidence indicating the Twitter account owner’s state of mind as it relates to the crime under investigation;



- g. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- h. The identity of the person(s) who communicated with the accounts about matters related to 18 U.S.C. § 1030, including records that help reveal their whereabouts.