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 THREE ACCOUNT STORED AT PREMISES CONTROLLED BY GOOGLE	Case: 1:18-sc-02524 Assigned To : Howell, Beryl A. Assign. Date : 7/27/2018 Description: Search & Seizure Warrant

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

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

See Attachment A

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

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before August 10, 2018 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

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

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Beryl A. Howell, Chief U.S. District Judge *(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: 7/27/2018 at 3:00 PM

/Beryl A. Howell/
Judge's signature

City and state: Washington, DC

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

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

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

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

Certification

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

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to be Searched

This warrant applies to search history information associated with the following accounts stored at premises owned, maintained, controlled, or operated by Google, LLC, in Mountain View, California:

ATTACHMENT B

Particular Things to be Seized

I. Files and Accounts to be produced by the Provider:

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

a. All search history information associated with each account.

II. Information to be Seized by Law Enforcement Personnel

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. § 2 (aiding and abetting), 18 U.S.C. § 3 (accessory after the fact), 18 U.S.C. § 4 (misprision of a felony), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1030 (unauthorized access of a protected computer); 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1349 (attempt and conspiracy to commit wire fraud), and 52 U.S.C. § 30121 (foreign contribution ban) for the period from June 2015 to the present, including:

a. 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, or communications regarding disinformation, denial, dissembling or other obfuscation about knowledge of, or access to hacked material;

b. All records, information, documents or tangible materials that relate in any way to communications or meetings involving Roger Stone, [redacted] Julian Assange, or any individual associated with the Trump Campaign;

e. Evidence indicating the account owner's state of mind as it relates to the crimes under investigation;

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

d. Information, documentation and records relating to who created, used, or communicated with the account or identifier concerning the messages identified above, including records about their identities and whereabouts;

e. Evidence of the times the account was used;

f. All evidence of wiping software, encryption or other methods to avoid detection by law enforcement;

g. Evidence of passwords and encryption keys, and other access information that may be necessary to access the account and other associated accounts;

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

I. Review Protocols

Review of the items described in Attachment A and Attachment B shall be conducted pursuant to established procedures designed to collect evidence in a manner consistent with professional responsibility requirements concerning the maintenance of attorney-client and other operative privileges. When appropriate, the procedures shall include use of a designated "filter team," separate and apart from the investigative team, in order to address potential privileges.

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Columbia

FILED
JUL 27 2018
Clerk, 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 THREE ACCOUNTS STORED AT PREMISES CONTROLLED BY GOOGLE

Case: 1:18-sc-02524
Assigned To : Howell, Beryl A.
Assign. Date : 7/27/2018
Description: Search & Seizure Warrant

APPLICATION FOR A SEARCH WARRANT

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

See Attachment A

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

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2, 3, 4, 371	Aiding & Abetting, Accessory after the Fact, Misprision of a Felony, Conspiracy
18 U.S.C. §§ 1030, 1343, 1349	Unauthorized Access of Protected Computer, Wire Fraud, Wire Fraud Conspiracy
52 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.

Applicant's signature

Reviewed by AUSA/SAUSA:
Kyle R. Freeny (ASC)

Andrew Mitchell, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 7/27/2018

Judge's signature

City and state: Washington, D.C.

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

FILED
JUL 27 2018
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 THREE ACCOUNTS STORED AT PREMISES CONTROLLED BY GOOGLE	Case: 1:18-sc-02524 Assigned To : Howell, Beryl A. Assign. Date : 7/27/2018 Description: Search & Seizure Warrant

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Andrew Mitchell, 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 search history information associated with the following Google accounts [redacted] ("**Target Accounts**"), stored at premises owned, maintained, controlled, or operated by Google, LLC ("Google"), 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.

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

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other FBI personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the **Target Accounts** contain information relevant to

violations of 18 U.S.C. § 2 (aiding and abetting); 18 U.S.C. § 3 (accessory after the fact); 18 U.S.C. § 4 (misprision of a felony); 18 U.S.C. § 371 (conspiracy); 18 U.S.C. § 1030 (unauthorized access of a protected computer); 18 U.S.C. § 1343 (wire fraud); 18 U.S.C. § 1349 (attempt and conspiracy to commit wire fraud); and 52 U.S.C. § 30121 (foreign contribution ban) (the "Subject Offenses").

JURISDICTION

5. 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 19.

SUMMARY

6. The Special Counsel's Office, with FBI's assistance, is investigating the Russian government's efforts to interfere in the 2016 presidential election, as well as any links and/or coordination between the Russian government and individuals associated with the campaign of President Donald Trump. This includes investigating Roger Stone (STONE) and others known and unknown, in connection with the hacking of email accounts associated with the Democratic National Committee (DNC), Democratic Congressional Campaign Committee (DCCC), and individuals involved in the presidential campaign of Hillary Clinton, as well as the subsequent dissemination of hacked materials via the persona Guccifer 2.0 and the organization WikiLeaks, among others.

7. On or about July 25, 2016, STONE emailed Jerome CORSI to "Get to Assange" at the Ecuadorian Embassy and "get pending WikiLeaks emails[.]" On or about July 31, 2016, STONE also instructed CORSI to have [redacted] contact Julian ASSANGE. On or about August 2, 2016, CORSI responded to STONE that the "word is friend in embassy [ASSANGE] plans 2 more dumps. One shortly after I'm back. 2nd in October. 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." After receipt of that message, on or about August 21, 2016, using @RogerJStoneJR, Stone tweeted: "Trust me, it will soon the [sic] Podesta's time in the barrel. #CrookedHillary."

8. Information disclosures subsequently occurred on or about the times CORSI predicted: On or about August 12, 2016, the day CORSI was scheduled to return to the United States ("shortly after I'm back"), Guccifer 2.0 released hacked information related to the DCCC. On or about October 7, 2016, the day the Washington Post published a breaking story about an Access Hollywood videotape of then-candidate Trump making disparaging remarks about women, WikiLeaks released emails hacked from the account of John Podesta.

9. Furthermore, on the day of the Access Hollywood video disclosure, there were phone calls between STONE and CORSI after the Washington Post contacted STONE prior to publication. At approximately 11:00AM, the Washington Post received a tip regarding the Access Hollywood video. Approximately one hour later, shortly before noon, STONE received a call from the Washington Post. Approximately ninety minutes later, before 2:00 PM, STONE called CORSI and they spoke. Approximately forty minutes later, CORSI called STONE and the two spoke again at length. At approximately 4:00PM, the Washington Post published its story

regarding the Access Hollywood tape. By approximately 4:30PM, WikiLeaks tweeted out its first release of emails hacked from John Podesta.

PROBABLE CAUSE

A. Background on Relevant Individuals

i. Roger STONE

11. Roger STONE is a self-employed political strategist/consultant and has been actively involved in U.S. politics for decades. STONE 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. As described further below, STONE also maintained contact with individuals employed by the

Campaign, including then-campaign chairman Paul MANAFORT and deputy chairman Rick GATES.

ii. Jerome CORSI

12. Jerome CORSI is a political commentator who, according to publicly available information, currently serves as the "Washington Bureau Chief for Inforwars.com." According to publicly-available sources, from 2014 until January 2017, CORSI was a "senior staff reporter" for the website "World Net Daily" a/k/a "WND.com." CORSI has also written a number of books regarding Democratic presidential candidates. As described further below, CORSI was in contact with STONE during the summer and fall of 2016 regarding forthcoming disclosures of hacked information by WikiLeaks, and appears to have obtained information regarding upcoming disclosures which he relayed to STONE.

[redacted]

B. Russian Government-Backed Hacking Activity During the 2016 Presidential Election

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

> The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of emails from US persons and institutions, including from US political organizations. The recent disclosures of alleged hacked emails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts. These thefts and disclosures are intended to interfere with the US election process. Such activity is not new to Moscow—the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there. We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities.

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

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

16. In its assessment, the USIC also described, at a high level, some of the techniques that the Russian government employed during its interference. The USIC summarized the efforts as a "Russian messaging strategy that blends covert intelligence operations—such as cyber

activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or 'trolls.'"

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

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

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

20. The Special Counsel's Office has determined that individuals associated with the GRU continued to engage in hacking activity related to the 2016 presidential election through at least November 1, 2016.

21. For example, in or around September 2016, these individuals successfully gained access to DNC computers housed on a third-party cloud-computing service. In or around late September, these individuals stole data from these cloud-based computers by creating backups of the DNC's cloud-based systems using the cloud provider's own technology. The individuals used three new accounts with the same cloud computing service to move the "snapshots" to

those accounts.

22. On or about September 4, 2016, individuals associated with the GRU stole the emails from a former White House advisor who was then advising the Clinton Campaign. These emails were later post on DCLeaks.

23. On or about November 1, 2016, individuals associated with the GRU spearphished over 100 accounts used by organizations and personnel involved in administering elections in numerous Florida counties.

24. On July 13, 2018, a grand jury in the District of Columbia returned an indictment against twelve Russia military officers for criminal offenses related to efforts to influence the 2016 presidential election, including conspiracy to commit authorized access to protected computers. (Case No. 1:18-cr-00125).

C. Roger Stone's Public Interactions with Guccifer 2.0 and WikiLeaks

25. On June 14, 2016, Crowdstrike, the forensic firm that sought to remediate an unauthorized intrusion into the computer systems of the DNC, publicly attributed the hack to Russian government actors and the media reported on the announcement. On June 15, 2016, the persona Guccifer 2.0 appeared and publicly claimed responsibility for the DNC hack. It stated on its WordPress blog that, with respect to the documents stolen from the DNC, "[t]he main part of the papers, thousands of files and mails, I gave to Wikileaks. They will publish them soon." In that post, Guccifer 2.0 also began releasing hacked DNC documents.

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

27. On August 5, 2016, STONE published an article on Breitbart.com entitled, "Dear Hillary: DNC Hack Solved, So Now Stop Blaming Russia." The article stated: "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." The article contained embedded publicly available Tweets from Guccifer 2.0 in the article and stated: "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." The article 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."

28. 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 any 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.

29. 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 DCCC.

30. 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.

31. 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."

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

33. On August 21, 2016, using @RogerJStoneJR, STONE tweeted 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."

34. 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 Hillary on a weekly basis fairly soon. And that of course will answer the question as to what exactly what was erased on that email server."

35. On Saturday, October 1, 2016, using @RogerJStoneJr, STONE tweeted, "Wednesday @ HillaryClinton is done. #WikiLeaks."

36. On Sunday, October 2, 2016, MSNBC Morning Joe producer Jesse Rodriquez tweeted regarding an announcement 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 October 5, 2016, STONE used @RogerJStoneJr to tweet: "Payload coming. #Lockthemup."

37. On Friday, October 7, 2016, at approximately 4:03 PM, 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.

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

39. WikiLeaks continued to release John Podesta's hacked emails through Election Day, November 8, 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 NBC News, 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."

40. 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."

D. STONE's Private Twitter Direct Messages with WikiLeaks and ASSANGE

41. On October 13, 2016, while WikiLeaks was in the midst of releasing the hacked Podesta emails, the Twitter account @RogerJStoneJr sent a private direct message to the Twitter account @wikileaks.[1] The latter 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."

42. 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."

43. On or about October 15, 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."

44. On or about November 9, 2016, one day after the presidential election, @wikileaks sent a direct message to @RogerJStoneJr containing a single word: "Happy?"

---

[1] On August 7, 2017, Chief Judge Beryl A. Howell issued a search warrant for the Twitter account @RogerJStoneJr.

@wikileaks immediately followed up with another message less than a minute later: "We are now more free to communicate."

45. In addition, @RogerJStoneJr also exchanged direct messages with 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."

46. 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."

E. CORSI's Communications with STONE, [redacted] and Others Regarding Forthcoming Leaks

47. On September 11, 2017, Chief Judge Beryl A. Howell of the District of Columbia issued a search warrant for STONE's [redacted] address [redacted]. On October 17, 2017, Chief Judge Beryl A. Howell issued a search warrant for one of STONE's [redacted]

addresses, [redacted] On or about December 19, 2017, Chief Judge Beryl A. Howell issued a search warrant for [redacted] email account. On or about March 14, 2018, Chief Judge Beryl A. Howell issued a search warrant for STONE's iCloud account. Information recovered pursuant to those search warrants indicated the following:

48. On or about May 15, 2016, [redacted] emailed CORSI: "Here is my flight schedule. Need to get something confirmed now . . . ." CORSI responded, "I copied Roger Stone so he knows your availability to meet Manafort and DT this coming week." CORSI appears to have forwarded the message to STONE at [redacted] who replied to CORSI that, "May meet Manafort -guarantee nothing."

49. On or about May 18, 2016, CORSI emailed STONE at [redacted] with the title, "Roger -- why don't you look this over before I send it [redacted] I believe that [redacted] CORSI wrote, [redacted] and I did manage to see Mr. Trump for a few minutes today as we were waiting in Trump Tower to say hello to Mike Cohen. Mr. Trump recognized us immediately and was very cordial. He would look for this memo from you this afternoon."

50. On July 25, 2016, STONE, using [redacted] sent an email to CORSI with the subject line, "Get to Assange." The body of the message read: "Get to Assange [a]t Ecuadorian Embassy in London and get the pending WikiLeaks emails…they deal with Foundation, allegedly."

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

52. On or about August 2, 2016 (approximately 19 days before STONE publicly tweeted about "Podesta's time in the barrel"), CORSI emailed STONE at [redacted] "Word is friend in embassy plans 2 more dumps. One shortly after I'm back. 2nd in Oct. Impact planned to be very damaging. Signs are Fox will have me on mid-Aug. more post Ailes shakeup underway. Expect Shine to surface victor, for now. Post-DNC bump for HRC an artifact of rigged polling. Won't last. I expect presidential campaign to get serious starting Sept. Still in pre-season games. Time to let more than Podesta to be exposed as in bed w enemy if they are not ready to drop HRC. That appears to be the game hackers are now about. Would not hurt to start suggesting HRC old, memory bad, has stroke -- neither he nor she well. I expect that much of next dump focus, setting stage for Foundation debacle." Investigators believe that CORSI's reference to a "friend in embassy [who] plans 2 more dumps" refers to Julian ASSANGE, the founder of WikiLeaks, who resided in Ecuador's London Embassy in 2016.

53. On or about August 5, 2016, [redacted] an associate of STONE's, emailed STONE at [redacted] The email contained a link to a poll indicating that Clinton led Trump by 15 points. STONE responded "enjoy it while u can[.] I dined with my new pal Julian Assange last night." [redacted] subsequently stated to investigators that, around the same time, STONE told him he had gone to London to meet ASSANGE. [redacted] also stated that in 2018, [redacted] told STONE he would be interviewed by the FBI and would have to divulge the conversation about meeting ASSANGE. STONE told [redacted] he was joking and had not actually met ASSANGE.

54. On or about August 15, 2016, CORSI emailed STONE at [redacted] "Give me a call today if you can. Despite MSM drumroll that HRC is

already elected, it's not over yet. More to come than anyone realizes. Won't really get started until after Labor Day. I'm in NYC this week. Jerry."

55. On or about August 31, 2016, CORSI emailed STONE at [redacted] "Did you get the PODESTA writeup." STONE replied "yes."

56. On or about August 31, 2016, CORSI messaged STONE, "Podesta paid $180k to invest in Uranium One – was hired by Rosatom in Giustra scandal. Podesta now under FBI investigation – tied to Ukraine Yanukovych – Panama papers reveals Podesta hired by S[b]erbank, Russia's largest financial institution – Podesta $$$ ties to Russia undermine Clinton false narrative attempting to tie Trump to Putin."

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

58. On or about September 24, 2016, [redacted] emailed CORSI, "I will have much more on Turkey. Need a back channel highly sensitive stuff." CORSI responded, "We have secure back channel through Roger. I saw him again in NYC last Friday and spoke to him about it again today." [redacted] wrote back, "Awaiting secret file. Explosive... Hope you are well. Can't wait for the debate. Channeling Reagan, I hope!" CORSI responded, "Keep me posted about file[.]" In a subsequent meeting with investigators, [redacted] indicated this conversation concerned possible derogatory information he was trying to obtain from Turkey.

59. On or about October 3, 2016, an associate of STONE emailed STONE at [redacted] and asked: "Assange – what's he got? Hope it's good." STONE wrote back, "It is. I'd tell Bannon but he doesn't call me back. My book on the TRUMP campaign will be out in Jan. Many scores will be settled." The associate forwarded the email to Steve BANNON and wrote: "You should call Roger. See below. You didn't get from me." BANNON

wrote back, "I've got important stuff to worry about." The associate responded, "Well clearly he knows what Assange has. I'd say that's important."

60. On or about October 4, 2016, ASSANGE gave a press conference at the Ecuadorian Embassy. There had been speculation in the press leading up to that event that ASSANGE would release information damaging to then-candidate Clinton, but WikiLeaks did not make any new releases. Instead, ASSANGE promised more documents, including information "affecting three powerful organizations in three different states, as well as, of course, information previously referred to about the U.S. election process." ASSANGE also stated that WikiLeaks would publish documents on various subjects every week for the next ten weeks, and vowed that the U.S. election-related documents would all come out before Election Day.

61. On or about October 4, 2016, CORSI messaged STONE at his iCloud account: "Assange made a fool of himself. Has nothing or he would have released it. Total BS hype."

62. That same day, BANNON emailed STONE at [redacted] "What was that this morning???" STONE replied, "Fear. Serious security concern. He thinks they are going to kill him and the London police are standing done [sic]." BANNON wrote back, "He didn't cut deal w/ clintons???" Stone replied, "Don't think so BUT his lawyer [redacted] is a big democrat."

63. When BANNON spoke with investigators during a voluntary proffer on February 14, 2018, he initially denied knowing whether the October 4, 2016 email to STONE was about WikiLeaks. Upon further questioning, BANNON acknowledged that he was asking STONE about WikiLeaks, because he had heard that STONE had a channel to ASSANGE, and BANNON had been hoping for releases of damaging information that morning.

F. STONE and CORSI Communications on October 7, 2016, when the Podesta Emails Are Released.

64. According to a publicly available news article,[2] at approximately 11AM on Friday, October 7, 2016, Washington Post reporter David Fahrenthold received a phone call from a source regarding a previously unaired video of candidate Trump. According to the same article, "Fahrenthold didn't hesitate. Within a few moments of watching an outtake of footage from a 2005 segment on 'Access Hollywood,' the Washington Post reporter was on the phone, calling Trump's campaign, 'Access Hollywood,' and NBC for reaction."

65. According to phone records [redacted] at approximately 11:27 AM, CORSI placed a call to STONE, which STONE did not answer.

66. At approximately 11:53AM, STONE received a phone call from the Washington Post. The call lasted approximately twenty minutes.

67. At approximately 1:42PM, STONE called CORSI and the two spoke for approximately seventeen minutes.

68. At approximately 2:18PM, CORSI called STONE and the two spoke for approximately twenty minutes.

69. At approximately 4:00PM, the Washington Post published a story regarding the Access Hollywood tape.

70. At approximately 4:30PM, WikiLeaks tweeted out its first release of emails hacked from John Podesta that focused primarily on materials related to the Clinton Foundation.

---

[2] https://www.washingtonpost.com/lifestyle/style/the-caller-had-a-lewd-tape-of-donald-trump-then-the-race-was-on/2016/10/07/31d74714-8ce5-11e6-875e-2c1bfe943b66_story.html

On or about August 2, 2016, when CORSI emailed STONE on [redacted] he wrote, "I expect that much of next dump focus, setting stage for Foundation debacle."

71. At approximately 6:27PM, [redacted] sent STONE an email titled, "WikiLeaks – The Podesta Emails," with a link to the newly-released Podesta emails. Approximately ten minutes later, STONE, using [redacted] forwarded [redacted] message to CORSI without comment. STONE does not appear to have forwarded the email to any other individual.

G. STONE Requests to CORSI for "SOMETHING" to Post About Podesta After STONE Is Accused of Advance Knowledge of the Leak

72. On or about October 8, 2016, STONE messaged CORSI, "Lunch postponed – have to go see T." CORSI responded to STONE, "Ok. I understand." Approximately twenty minutes later, CORSI texted, "Clintons know they will lose a week of Paula Jones media with T attacking Foundation, using Wikileaks Goldman Sachs speech comments, attacking bad job numbers."

73. On or about Wednesday, October 12, 2016, at approximately 8:17AM, STONE, using [redacted], emailed Corsi asking him to "send me your best podesta links." STONE emailed CORSI at approximately 8:44AM EDT, "need your BEST podesta pieces." CORSI wrote back at approximately 8:54AM EDT, "Ok. Monday. The remaining stuff on Podesta is complicated. Two articles in length. I can give you in raw form the stuff I got in Russian translated but to write it up so it's easy to understand will take weekend. Your choice?"

74. On or about that same day, October 12, 2016, Podesta accused STONE of having advance knowledge of the publication of his emails. At approximately 3:25PM EDT, CORSI emailed STONE at both [redacted], 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."

75. 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 got it." STONE emailed CORSI back via the Hotmail Account, "Got them and used them."

76. On or about Thursday, October 13, 2016, CORSI emailed STONE at [redacted] "PODESTA -- Joule & ties to RUSSIA MONEY LAUNDERING to CLINTON FOUNDATION." STONE responded, "Nice but I was hoping for a piece I could post under my by-line since I am the one under attack by Podesta and now Mook." CORSI wrote back to STONE, "I'll give you one more — NOBODY YET HAS THIS[:] It looks to me like [redacted] skimmed maybe billions off Skolkovo — Skolkovo kept their money with Metcombank[.] The Russians launched a criminal investigation[.] [web link] Once [redacted] had the channel open from Metcombank to Deutsche Bank America to Ban[k] of America's Clinton Fund account, there's no telling how much money he laundered, or where it ended up. Nothing in Clinton Foundation audited financials or IRS Form 990s about $$$ received via Russia & Metcombank[.] I'm working on that angle now." STONE replied, "Ok Give me SOMETHING to post on Podesta since I have now promised it to a dozen MSM reporters[.]"

77. On or about Thursday, October 13, 2016 at approximately 6:30PM EDT, CORSI sent STONE an email at [redacted] with the subject, "ROGER STONE article RUSSIAN MAFIA STYLE MONEY-LAUNDERING, the CLINTON FOUNDATION, and JOHN PODESTA." The text stated: "Roger[,] You are free to publish this under your own

name." That same day, STONE posted a blog post with the title, "Russian Mafia money laundering, the Clinton Foundation and John Podesta." In that post, STONE wrote, "although I have had some back-channel communications with Wikileaks I had no advance notice about the hacking of Mr. Podesta nor I have I ever received documents or data from Wikileaks." The post then asked, "Just how much money did [redacted] a controversial Russian billionaire investor with ties to the Vladimir Putin and the Russian government, launder through Metcombank, a Russian regional bank owned 99.978 percent by [redacted] with the money transferred via Deutsche Bank and Trust Company Americas in New York City, with the money ending up in a private bank account in the Bank of America that is operated by the Clinton Foundation?"

78. On or about October 14, 2016, CORSI sent a message to STONE at his iCloud account, "I'm in NYC. Thinking about writing piece attacking Leer and other women. It's basically a rewrite of what's out there. Going through new Wikileaks drop on Podesta."

79. On or about October 17, 2016, CORSI messaged STONE at his iCloud account, "On Assange, can you call me now – before 2pm[.]" STONE responded, "Missed u – just landed JFK – on Infowars now." CORSI wrote back, "Call afterwards. Have some important intel to share."

80. On or about October 17, 2016, CORSI emailed STONE at [redacted] 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'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."

81. On or about October 18, 2016, CORSI messaged STONE at his iCloud account, "Pls call. Important."

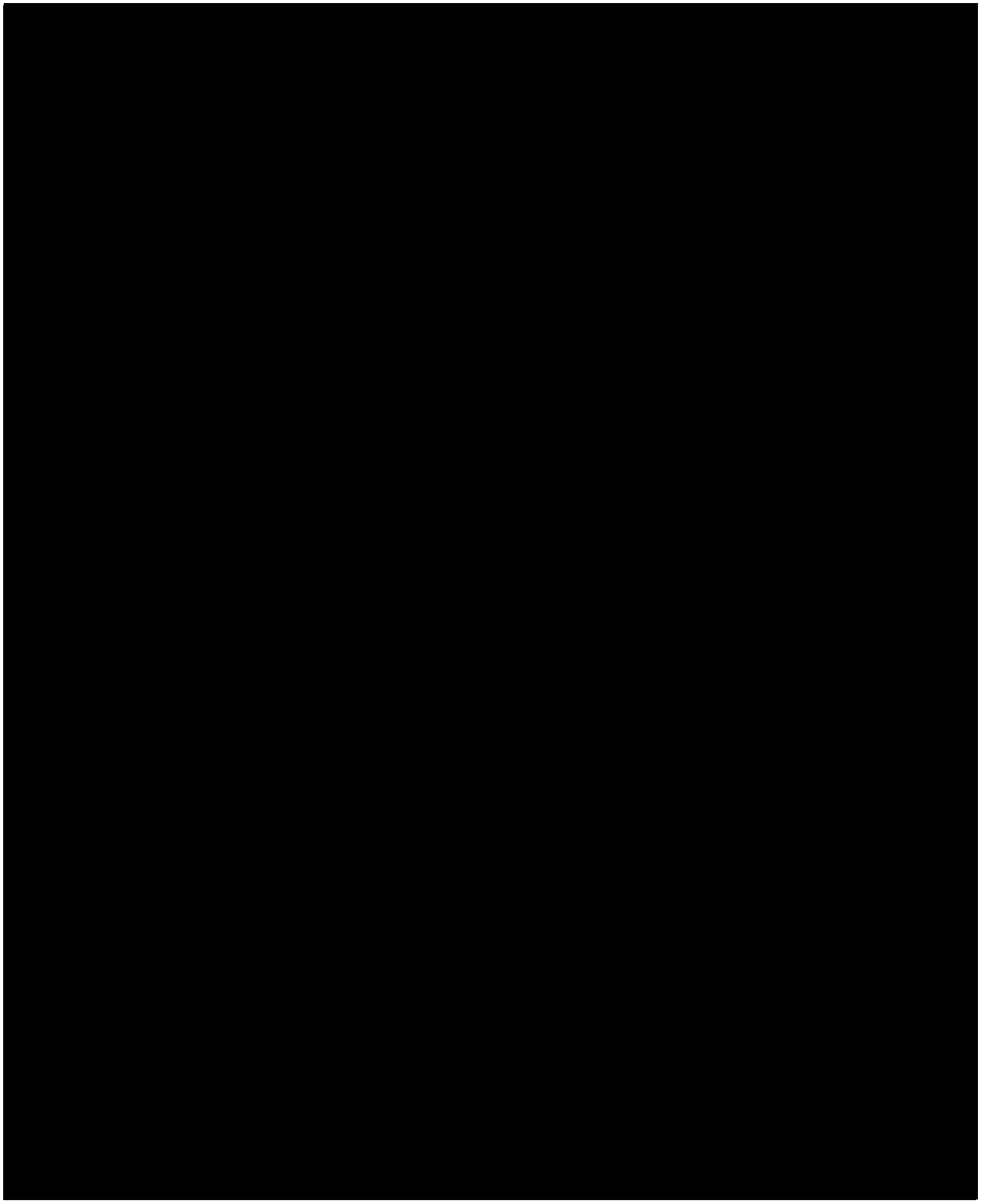
82. On or about October 19, 2016, STONE published an article on Breitbart.com in which he claimed he had, "no advance notice of Wikileaks' hacking of Podesta's e-mails." STONE stated that, "I predicted that Podesta's business dealings would be exposed. I didn't hear it from Wikileaks, although Julian Assange and I share a common friend. I reported the story on my website." STONE linked to the story he had asked CORSI to write for him on October 13, 2016 discussed above.

83. On or about November 8, 2016, the United States presidential election took place.

84. On or about November 9, 2016, CORSI messaged STONE at his iCloud account, "Congratulations, Roger. He could not have done it without you."

85. On or about November 10, 2016, CORSI messaged STONE at his iCloud account, "Are you available to talk on phone?" Several minutes later, CORSI messaged, "I'm in London. Have some interesting news for you."

[redacted]



I. Evidence of Google Searches Relating to the Conduct Under Investigation

92. The search history associated with the account [redacted], which was obtained pursuant to search warrant, shows that STONE searched for terms that appear to be related to the DNC hack and the stolen emails, including his nexus thereto, while logged into the [redacted] For example, on or about October 13, 2016, STONE searched for the words "Roger Stone john Podesta." The search history for [redacted] appears to have been deleted between January 18, 2016, and July 23, 2016.

93. During the course of its investigation, the FBI has also identified a series of searches that appear to relate to the personas Guccifer 2.0 and DCLeaks, which predate the public unveiling of those two personas. In particular, between May 17, 2016, and June 15, 2016

(prior to the publication of the Guccifer 2.0 WordPress blog), records from Google show that searches were conducted for the terms "dcleaks," "guccifer," and "guccifer june," from IP addresses within one of two ranges: 172.56.26.0/24, 107.77.216.0/24.[3] These IP ranges are assigned to T-Mobile USA, Inc., and AT&T Mobility LLC, respectively, and, according to Google, the searches were all conducted from Florida. On or about June 13, 2018, this Court issued a search warrant for information associated with these searches and, in particular, for the full search histories associated with the CookieIDs that conducted the search.[4] As set forth in the affidavit submitted in support of that search warrant, IP logs obtained from Twitter showed that STONE used multiple IP addresses within the ranges 172.56.26.0/24 and 107.77.216.0/24 to log into his Twitter account @RogerJStoneJr. A Facebook account controlled by STONE also used an IP address within the range 172.56.26.0/24 on or about June 13, 2016, to purchase a Facebook advertisement.

J. The Target Accounts

94. Subscriber records show that, in addition to [redacted] STONE maintains at least two additional Google accounts registered in his name:

a. [redacted] ("**Target Account 1**") was created on July 28, 2016, and uses the recovery email address [redacted]. According to subscriber records, **Target Account 1** was last accessed on July 5, 2017. Search warrant returns for [redacted] show that on or about August 3, 2016, STONE sent an email from

[3] Google does not retain full IP addresses for searches conducted more than one year ago. The truncated IP addresses designated here as 107.77.216.0/24 and 17.56.26.0/24 each encompass a range of up to 256 IP addresses.

[4] Google assigns unique CookieIDs to searches conducted while a user is not logged into a Google account. All searches conducted from the same device and browser during a 24-hour window are associated with the same CookieID.

[redacted] to **Target Account 1**, with no subject, attaching what appears to be an advertisement for his book tour, entitled, "Clinton's War on Women."

b. [redacted] ("**Target Account 2**") was created on or about October 26, 2016, and uses **Target Account 1** as the recovery email. **Target Account 2** was last accessed on or about August 8, 2017.

95. The search of STONE's Hotmail account indicates that STONE uses the address [redacted] ("**Target Account 3**"). For example, on or about June 27, 2016, Stone received an email in his [redacted] account from the "Gmail Team" with the subject, "Your Gmail address, [redacted], has been created." Subscriber records show that **Target Account 3** was created on June 27, 2016, and is registered in the name of "Swash Buckler." On or about April 16, 2018, this Court issued an order pursuant to 18 U.S.C. § 2703(d) for non-content information associated with **Target Account 3**. Based on a review of the header information obtained from Google pursuant to that Order, it appears that STONE frequently used **Target Account 3** to communicate with others via the classified advertisement website Craigslist.org ("Craigslist").

96. This warrant application seeks only search history for the **Target Accounts**; it does not seek the content of email communications to and from the **Target Accounts**.[5] Google maintains records of the Google searches that a user conducts while signed into a particular Google email account (provided the user has not disabled the retention of this information). In my training and experience, I know that users are often not aware of whether or not they are

[5] The government is also contemporaneously seeking an order pursuant to 18 U.S.C. § 2703(d) for non-content information associated with **Target Accounts 1 and 2**, including header information.

experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

99. As explained herein, information stored in connection with an email 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, the information stored in connection with a Google account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, an account's search history may indicate who used or controlled the account at a relevant time. Further, information maintained by the email Providers can show how and when the account was accessed or used. Additionally, information stored in an account's search history may indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Lastly, stored electronic data, including search history information, may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, searches relating to the crime), or consciousness of guilt (*e.g.*, deleting search history in an effort to conceal information from law enforcement).

FILTER REVIEW PROCEDURES

100. Review of the items described in Attachment A and Attachment B will be conducted pursuant to established procedures designed to collect evidence in a manner consistent with professional responsibility requirements concerning the maintenance of attorney-client and

other operative privileges. The procedures include use, if necessary, of a designated "filter team," separate and apart from the investigative team, in order to address potential privileges. The government, however, does not at this time anticipate that any of the items described in Attachment A will contain materials requiring review by a designated filter team.

CONCLUSION

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

102. 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

103. 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,

Andrew Mitchell
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on this 27th day of July, 2018.

The Honorable Beryl A. Howell
Chief United States District Judge

ATTACHMENT A

Property to be Searched

This warrant applies to search history information associated with the following accounts stored at premises owned, maintained, controlled, or operated by Google, LLC, in Mountain View, California:

ATTACHMENT B

Particular Things to be Seized

I. Files and Accounts to be produced by the Provider:

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

a. All search history information associated with each account.

II. Information to be Seized by Law Enforcement Personnel

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. § 2 (aiding and abetting), 18 U.S.C. § 3 (accessory after the fact), 18 U.S.C. § 4 (misprision of a felony), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1030 (unauthorized access of a protected computer); 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1349 (attempt and conspiracy to commit wire fraud), and 52 U.S.C. § 30121 (foreign contribution ban) for the period from June 2015 to the present, including:

a. 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, or communications regarding disinformation, denial, dissembling or other obfuscation about knowledge of, or access to hacked material;

b. All records, information, documents or tangible materials that relate in any way to communications or meetings involving Roger Stone, [redacted], Julian Assange, or any individual associated with the Trump Campaign;

e. Evidence indicating the account owner's state of mind as it relates to the crimes under investigation;

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

d. Information, documentation and records relating to who created, used, or communicated with the account or identifier concerning the messages identified above, including records about their identities and whereabouts;

e. Evidence of the times the account was used;

f. All evidence of wiping software, encryption or other methods to avoid detection by law enforcement;

g. Evidence of passwords and encryption keys, and other access information that may be necessary to access the account and other associated accounts;

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

I. Review Protocols

Review of the items described in Attachment A and Attachment B shall be conducted pursuant to established procedures designed to collect evidence in a manner consistent with professional responsibility requirements concerning the maintenance of attorney-client and other operative privileges. When appropriate, the procedures shall include use of a designated "filter team," separate and apart from the investigative team, in order to address potential privileges.