

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 THE EMAIL
ACCOUNT [REDACTED]

) Case: 1:17-mj-00661
) Assigned To : Howell, Beryl A.
) Assian. Date : 9/11/2017
) 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 September 25, 2017 *(not to exceed 14 days)*
 in the daytime 6:00 a.m. to 10:00 p.m. at any time in the day or night because good cause has been established.

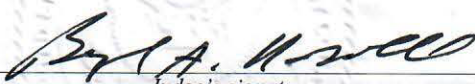
Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

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

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

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

Date and time issued: September 11, 2017 @ 11:30 AM


Judge's signature

City and state: Washington, DC

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

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

Return

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

Inventory made in the presence of :

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

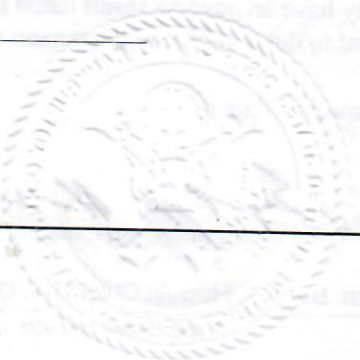
Certification

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

Date: _____

Executing officer's signature

Printed name and title



FILED

SEP 11 2017

UNITED STATES DISTRICT COURT

for the District of Columbia

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

In the Matter of the Search of (Briefly describe the property to be searched or identify the person by name and address) INFORMATION ASSOCIATED WITH THE EMAIL ACCOUNT [REDACTED]

Case: 1:17-mj-00661 Assigned To : Howell, Beryl A. Assian. Date : 9/11/2017 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

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):

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

The search is related to a violation of:

Table with 2 columns: Code Section, Offense Description. Rows include 18 U.S.C. § 1030 (Fraud and related activities in connection with computers) and 18 U.S.C. § 371 (Conspiracy to commit an offense against the United States).

The application is based on these facts:

See attached Affidavit.

- [x] 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)

[Signature of Amy Anderson] Applicant's signature

Amy Anderson, Special Agent, FBI Printed name and title

Sworn to before me and signed in my presence.

Date: 09/11/2017 @ 11:30 AM

[Signature of Beryl A. Howell] Judge's signature

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

City and state: Washington, D.C.

FILED

SEP 11 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
EMAIL ACCOUNT

[REDACTED]

Case No.

Filed Under Seal

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

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

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the Email Account [REDACTED] (hereafter the “**Target Account**”), that is stored at premises owned, maintained, controlled, or operated by Microsoft Corp., d/b/a Hotmail, an email provider headquartered at One Microsoft Way, Redmond, WA 98052 (hereinafter “Microsoft”). The information to be disclosed by Microsoft and searched by the Government is described in the following paragraphs and in Attachments A and B. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A).

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

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

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the **Target Account** contains communications relevant to violations of 18 U.S.C. § 1030 (fraud and related activities in connection with computers) and 18 U.S.C. § 371 (conspiracy to commit an offense against the United States). As set forth below, Roger Stone used Twitter's private direct messaging function to message Wikileaks, Julian Assange, and Guccifer 2.0, a Twitter account used by Russian intelligence to disseminate hacked information. Stone also repeatedly used Twitter's private direct messaging function to instruct individuals to email him on the **Target Account** to continue conversations begun on Twitter's private direct messaging system. These conversations included discussion of information related to the Campaign and potential derogatory information concerning a presidential candidate in the Republican primary. 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.

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 in paragraphs 6, 20, and 28.

PROBABLE CAUSE

A. The 2016 Email Hack and Russia’s Use of “Guccifer 2.0” and Wikileaks to Disseminate Hacked Information.

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

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

B. Roger Stone’s Publicly Disclosed Interactions with Guccifer 2.0 and Wikileaks.

8. Roger Stone is a self-employed political strategist/consultant and has been actively involved in U.S. politics since 1975. Stone worked on the presidential campaign of Donald J. Trump (the “Campaign”) until he was fired in August 2015. Although Stone had no

official relationship with the Campaign thereafter, Stone maintained his support for Trump and continued to make media appearances in support of Trump's presidential campaign.

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

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

11. On July 22, 2016, Wikileaks published approximately 20,000 emails stolen from the DNC.

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

13. On August 8, 2016, Stone addressed the Southwest Broward Republican Organization. During his speech, he was asked about a statement by Wikileaks founder Julian Assange to Russia Today (RT) several days earlier about an upcoming "October Surprise" aimed at the Hillary Clinton presidential campaign. Specifically, Stone was asked: "With regard to the

October surprise, what would be your forecast on that given what Julian Assange has intimated he's going to do?" Stone responded: "Well, it could be a number of things. I actually have communicated with Assange. I believe the next tranche of his documents pertain to the Clinton Foundation but there's no telling what the October surprise may be." A few days later, Stone clarified that while he was not personally in touch with Assange, he had a close friend who served as an intermediary.

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

15. 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.

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

17. On August 15, 2016, Guccifer 2.0 replied to Stone on Target Account 1, stating: "wow. thank u for writing back, and thank u for an article about me!!! did you find anything interesting in the docs I posted."

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

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

19. 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.”

20. On August 18, 2016, Paul Manafort, Stone’s longtime friend and associate, resigned as Chairman of the Campaign. Contemporary press reports at the time indicated that Manafort had been involved in using Washington D.C.-based lobbying firms to influence U.S. policy toward the Ukraine, including the lobbying group of Anthony Podesta (the brother of John Podesta), the Podesta Group. At the same time, press reports indicated that investigators were examining Manafort for potential violations of the Foreign Agent Registration Act (FARA), and that investigators were also examining the Podesta Group.

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

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

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

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

25. 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.

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

27. Wikileaks continued to release John Podesta’s hacked emails throughout October 10-21, 2016. On October 12, 2016, John Podesta – referring back to Stone’s August 21, 2016 C-SPAN and Twitter references – argued publicly that “[it is] a reasonable assumption to - or at least a reasonable conclusion - that [Stone] had advanced warning [of the release of his emails] and the Trump campaign had advanced warning about what Assange was going to do. I think there’s at least a reasonable belief that [Assange] may have passed this information on to

[Stone].” Commenting to the Miami Herald, Stone responded: “I have never met or spoken with Assange, we have a mutual friend who’s traveled to London several times, and everything I know is through that channel of communications. I’m not implying I have any influence with him or that I have advanced knowledge of the specifics of what he is going to do. I do believe he has all of the e-mails that Huma Abedin and Cheryl Mills, the Clinton aides, thought were deleted. I hear that through my emissary.”

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

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

C. Roger Stone’s Private Twitter Direct Messages with Wikileaks and Julian Assange.

30. On August 7, 2017, Chief Judge Beryl A. Howell issued a search warrant for the Twitter account @RogerJStoneJr. While the full review of that returned information is ongoing, the initial review indicates that, contrary to Stone’s representation to CNN that he “never communicated with WikiLeaks,” Stone in fact communicated via private direct messaging with

Wikileaks during the Campaign. Stone also used the @RogerJStoneJr Twitter account's private direct messaging system to communicate directly with Julian Assange since at least June 2017.

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

32. 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."

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

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

35. In addition, @RogerJStoneJr has also recently exchanged direct messages with Julian Assange, the founder of Wikileaks. For example, on June 4, 2017, @RogerJStoneJr directly messaged @JulianAssange, an address associated with Julian Assange in numerous public reports, stating: "Still nonsense. As a journalist it doesn't matter where you get

information only that it is accurate and authentic. The New York Times printed the Pentagon Papers which were indisputably stolen from the government and the courts ruled it was legal to do so and refused to issue an order restraining the paper from publishing additional articles. If the US government moves on you I will bring down the entire house of cards. With the trumped-up sexual assault charges dropped I don't know of any crime you need to be pardoned for - best regards. R.” That same day, @JulianAssange responded: “Between CIA and DoJ they're doing quite a lot. On the DoJ side that's coming most strongly from those obsessed with taking down Trump trying to squeeze us into a deal.”

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

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

37. Using the direct messaging function associated with the account @RogerJStoneJr, Stone sent direct messages to individuals instructing them to email the **Target Account** to continue conversations began via Twitter direct message. For example, on August 8, 2015, an individual sent @RogerJStoneJr a direct message asking if he had “a few minutes this afternoon to talk about all of today’s drama with Trump.” Stone responded the next day: “Sorry I missed this – my email [**Target Account**].”

38. On August 8, 2015, an individual sent a direct message to @RogerJStoneJr reading: “Just got some stuff from the campaign you may want to respond to.” That same day, @RogerJStoneJr responded: “Such as -? My email is [**Target Account**].”

39. On August 9, 2015, an individual sent @RogerJStoneJr a direct message asking to arrange an interview. @RogerJStoneJr replied, "Okay – what do you need from me." The individual replied, "Your email address. Twitter too public." Stone replied with the **Target Account**.

40. On September 7, 2015, an individual sent a private direct message to @RogerJStoneJr containing a "White Paper," regarding the "Most likely questions to be asked of Mr. Trump on Foreign Policy." @RogerJStoneJr replied: "Send to me at [**Target Account**]."

41. On February 17, 2016, an individual sent a direct message to Stone reading: "Mr. Stone I have a delightful story about one foul tempered governor currently pretending to be Ned Flanders up on the stage. Interested?" @RogerJStoneJr responded on Friday, February 19, 2016: "Sure---tell me what u know—[**Target Account**]."

42. On March 21, 2016, an individual sent a private direct message to @RogerJStoneJr reading: "Im trying to get a list of upcoming Trump events so I can Fly out and Film these Anti-Trump protesters. To show the American people that these are the people that are actually creating the Chaos. No one is showing whats really going on outside at these events honestly and quite frankly its pissing me off." The next day, @RogerJStoneJr responded: "Email me at [**Target Account**]."

43. On April 30, 2016, an individual sent a private direct message to @RogerJStoneJr stating: "Give me a shout if you need a story moved. My followers are RTing fiends! lol." @RogerJStoneJr responded: "Great- please e-mail me again at [**Target Account**]."

44. On September 13, 2016, an individual send a private direct message to @RogerJStoneJr asking for a "contact info so I can stay in touch in a more appropriate way than Twitter DM." @RogerJStoneJr replied, "email me at [**Target Account**]."

BACKGROUND CONCERNING HOTMAIL

45. In my training and experience, I have learned that Microsoft provides a variety of on-line services, including electronic mail (“email”) access, to the public. Microsoft allows subscribers to obtain email accounts at the domain name Hotmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Hotmail. During the registration process, Hotmail asks subscribers to provide basic personal information. Therefore, the computers of Microsoft are likely to contain stored electronic communications (including retrieved and unretrieved email for Hotmail subscribers and information concerning subscribers and their use of Hotmail services, such as account access information, email transaction information, and account application information. In my training and 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.

46. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and 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. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

47. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This

information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

48. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and 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.

49. This application seeks a warrant to search all responsive records and information under the control of Microsoft, a provider subject to the jurisdiction of this court, regardless of where Microsoft has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Microsoft's possession, custody, or

control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

50. 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 an email 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, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further 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). Last, stored electronic data 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.*,

communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

51. 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 Hotmail to disclose to the government copies of the records and other information (including the content of communications) associated with the account in Attachment A and particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B. The items identified in Attachments A and B will also be screened by reviewers not on the prosecution team to identify and filter out privileged material.

CONCLUSION

52. Roger Stone used the @RogerJStoneJr to communicate directly with Wikileaks during the campaign, even though he publicly claimed to have “never” communicated with Wikileaks. He also sent private messages to Julian Assange and Guccifer 2.0, the entity which claimed responsibility for the DNC hack. Using @RogerJStoneJr, Stone has repeatedly instructed individuals to continue conversations, including particularly sensitive issues related to the Campaign, on the **Target Account**. There is therefore probable cause to believe that evidence of the DNC hack and the hacking of other emails associated with the 2016 election will be found on the **Target Account**.

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

54. 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

55. 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 11th day of September, 2017.



The Honorable Beryl A. Howell
Chief United States District Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the [REDACTED] Account [REDACTED] (the “**Target Account**”) that is stored at premises owned, maintained, controlled, or operated by Microsoft Corp., d/b/a Hotmail, a company headquartered at One Microsoft Way, Redmond, WA 98052.

ATTACHMENT B

I. Information to be disclosed by Microsoft, Corp.

To the extent that the information described in Attachment A is within the possession, custody, or control of the Microsoft, Corp. (hereinafter “the Provider”), regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A2:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, all other user names associated with the account, all account names associated with the subscriber, methods of connecting;

- f. All search history or web history;
- g. All records indicating the services available to subscribers of the account;
- h. All usernames associated with or sharing a login IP address or browser cookie with the account;
- i. All cookies, including third-party cookies, associated with the user;
- j. All records that are associated with the machine cookies associated with the user;
and
- k. All telephone or instrument numbers associated with the Account (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), International Mobile Subscriber Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”).

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, contraband, fruits, and/or instrumentalities of violations of 18 U.S.C. § 1030 (fraud and related activities in connection with computers) and 18 U.S.C. §371 (conspiracy to commit and offense against the United States) involving Roger Stone or others associated with him and occurring after January 1, 2015, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Communications, records, documents and other files that reveal efforts by Roger Stone to communicate with any individuals associated with carrying out the hacks of the DNC or individual email addresses associated with the Clinton Campaign.
- (b) Records of any funds or benefits received by or offered to Roger Stone or an individuals or entities associated with him by, or on behalf of, any individuals associated with the hacks of the DNC or individual email addresses associated with the Clinton Campaign.

- (c) Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account owner;
- (d) Evidence indicating the account owner's state of mind as it relates to the crimes under investigation;
- (e) The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).
- (f) The identity of any person(s)—including records that help reveal the person(s)' whereabouts—who communicated with the account about any matters relating to activities conducted by Roger Stone on behalf of, for the benefit of, any individual associated with hacks of the DNC or individual email addresses associated with the Clinton Campaign.