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 ACCOUNTS STORED AT PREMISES CONTROLLED BY MICROSOFT	Case: 1:18-sc-02920 Assigned To : Howell, Beryl A. Assign. Date : 9/27/2018 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 Western District of Washington *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

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

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before October 11, 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: 9/27/2018 at 4:05 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

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 information associated with the following Microsoft accounts, stored at premises owned, maintained, controlled, or operated by Microsoft Corporation ("Microsoft"), a company headquartered in Redmond, Washington:

[redacted]

This warrant also applies to information associated with the following Skype usernames and/or email addresses, stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, an electronic communication and/or remote computing service provider with headquarters in Redmond, Washington:

[redacted]

ATTACHMENT B

I. Information to be disclosed by Microsoft

To the extent that the information described in Attachment A is within the possession, custody, or control of the Microsoft Corporation (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 have been deleted but are 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 A:

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. The contents of all Skype communications sent to or from the account, including videos, instant messages, group messages, and attachments, as well as the complete conversation history for the account;

c. 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);

d. The types of service utilized;

e. All Windows Live and OneDrive data and content;

f. All Microsoft Developer information and content and any other information and content relating to software development and testing;

g. 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;

h. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;

i. All Lync content;

j. All subscriber "change history" associated with the account;

k. All search history and web history associated with the account (including Bing history);

l. All location and maps information associated with the account;

m. All device information associated with the account, including all instrument or telephone numbers (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")); and

n. For any accounts linked to the accounts listed in Attachment A, including accounts linked by cookie, SMS number, or recovery email address, and for accounts for

which the accounts described in Attachment A are the recovery email address, provide 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).

II. Information to be Seized by the Government

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. § 1001 (false statements), 18 U.S.C. § 1030 (unauthorized access of a protected computer); 18 U.S.C. §§ 1505 and 1512 (obstruction of justice), 18 U.S.C. § 1513 (witness tampering), 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 contributions ban) for the period from March 1, 2016 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 Jerome Corsi, [redacted] Julian Assange, [redacted] Randy Credico, any individual associated with the Trump Campaign, any witness in the investigation;

c. Communications, records, documents, and other files related to any expenditure, independent expenditure, or disbursement for an electioneering communication;

d. Records of any funds or benefits disbursed by or offered on behalf of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

e. 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;

f. Communications, records, documents, and other files that reveal efforts by any person to conduct activities on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

g. 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;

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

i. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s);

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

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

l. The identity of any non-U.S. person(s)—including records that help reveal the whereabouts of the person(s)—who made any expenditure, independent expenditure, or disbursement for an electioneering communication; and

m. The identity of any person(s)—including records that help reveal the whereabouts of the person(s)—who communicated with the account about any matters relating to activities conducted by on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals.

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

o. All existing printouts from original storage which concern the categories identified in subsection II.a.

III. 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.

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 MICROSOFT CORPORATION

Case: 1:18-sc-02920
Assigned To : Howell, Beryl A.
Assign. Date : 9/27/2018
Description: Search & Seizure Warrant

ORDER

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

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

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

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

THE HONORABLE BERYL A. HOWELL
CHIEF UNITED STATES DISTRICT JUDGE

9/27/2018
Date

UNITED STATES DISTRICT COURT

for the
District of Columbia

FILED
SEP 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 MICROSOFT

Case: 1:18-sc-02920
Assigned To : Howell, Beryl A.
Assign. Date : 9/27/2018
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 Western District of Washington, 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*
52 U.S.C. § 30121	Foreign Contribution Ban
18 U.S.C. §§ 1001, 1030, 371	False Statements, Unauthorized Access of Protected Computer, Conspiracy

See Affidavit for add'l

The application is based on these facts:
See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

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

Applicant's signature

Patrick J. Myers, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 9/27/2018

Judge's signature

City and state: Washington, D.C.

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

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 MICROSOFT

Case: 1:18-sc-02920
Assigned To : Howell, Beryl A.
Assign. Date : 9/27/2018
Description: Search & Seizure Warrant

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Patrick J. Myers, 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 Microsoft email account [redacted] ("**Target Accounts 1**") and the Skype accounts registered to [redacted] ("**Target Account 2**") and to [redacted] ("**Target Account 3**"), stored at premises owned, maintained, controlled or operated by Microsoft Corporation ("Microsoft"), a company headquartered in Redmond, Washington. [redacted]

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

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") assigned to FBI Pittsburgh working directly with the Special Counsel's Office. I have been a Special Agent with the FBI since 2017. I was previously employed as a network and software engineer for approximately fifteen years, including for the FBI. As a Special Agent, I have conducted national security investigations relating to foreign intelligence and cybersecurity.

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** contains evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 371 (conspiracy), 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. § 1001 (false statements), 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), 18 U.S.C. §§ 1505 and 1512 (obstruction of justice), 18 U.S.C. § 1513 (witness tampering), and 52 U.S.C. § 30121(a)(1)(C) (foreign expenditure ban). There also is probable cause to search the information described in Attachment A for evidence, contraband, fruits, and/or instrumentalities of the Subject Offenses, further 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.

PROBABLE CAUSE

A. Background on Relevant Individuals

i. *Roger STONE*

6. 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 the 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*

7. Jerome CORSI is a political commentator who, according to publicly available information, served 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

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

> [] 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.

10. 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.'"

11. 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."

12. 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."

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

14. 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.

15. 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.

16. 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.

17. 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.

18. 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. *See United States* v. *Viktor Borisovich Netyksho, et al.* (Case No. 1:18-cr-00125).

C. STONE's Public Interactions with Guccifer 2.0 and WikiLeaks

19. 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.

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

21. 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."

22. 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.

23. 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.

24. 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.

25. 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."

26. 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.

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

28. 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."

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

30. 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."

31. 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.

32. 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.

33. WikiLeaks continued to release John Podesta's hacked emails through Election Day, November 8, 2016. On October 12, 2016, 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 indicated that he had never met or spoken with Assange, saying that "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."

34. 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

35. 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."

36. 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."

37. 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."

38. On or about 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."

39. In addition, @RogerJStoneJr also exchanged direct messages with ASSANGE,

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

the founder of WikiLeaks. For example, on June 4, 2017, @RogerJStoneJr directly messaged @JulianAssange, an address associated with 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."

40. On Saturday, June 10, 2017, @RogerJStoneJr sent a direct message to @JulianAssange, 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

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

42. 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."

43. 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."

44. 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."

45. 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."

46. 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." The email continued, "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 ASSANGE, who resided in Ecuador's London Embassy in 2016.

47. 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.[2]

48. Through a search of STONE's iCloud account, the FBI has uncovered evidence suggesting that STONE was in Los Angeles for one or more meetings at the time that he claimed, in his email to [redacted] to have "dined" with ASSANGE. For example, an associate of

[redacted]

STONE sent a text to STONE at approximately 3:38PM on August 2, asking "How did ur meeting go in LA?" STONE responded. "It's this afternoon[.]" The following day, the associate asked, "Any report from ur meeting?" On or about August 4, 2016, STONE texted the associate, "Will call later – heading for airport now[.]" Additionally, investigators have identified a photograph in STONE's iCloud that appears to have been taken on August 3, 2016 and had geo-location information indicating that it was taken in Los Angeles.

49. 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."

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

51. 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."

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

53. 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.

54. On or about October 3, 2016, an associate of STONE emailed STONE at [redacted] 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, who was CEO of the Campaign at the time, 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."

55. 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.

56. 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."

57. 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."

58. When BANNON spoke with investigators during a voluntary interview 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.

59. According to a publicly available news article,[3] 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."

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

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

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

---

[3] 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

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

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

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

66. At approximately 6:27PM, [redacted] an author who has written about the Clinton Foundation, and who, according to emails and phone records, regularly communicates with STONE, 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 Asks CORSI for "SOMETHING" to Post About Podesta After STONE Is Accused of Advance Knowledge of the Leak

67. 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."

68. 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?"

69. 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]ith the 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."

70. 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."

71. 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[.]"

72. 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?"

73. 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."

74. 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."

75. 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." Based on review of the original email that CORSI forwarded, the "trusted source" was a self-identified retired librarian who gathers information from public chat rooms.

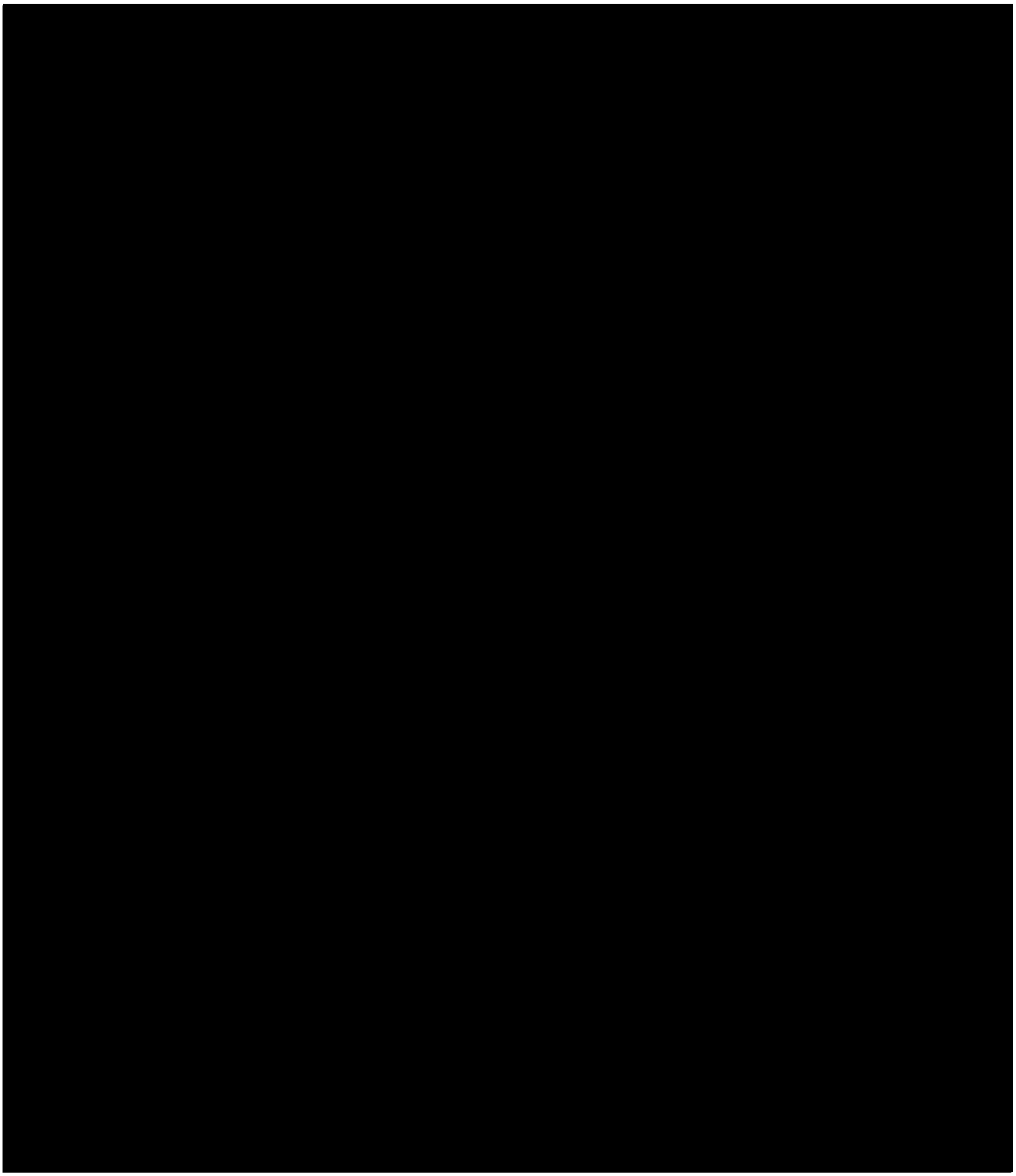
76. On or about October 18, 2016, CORSI messaged STONE at his iCloud account, "Pls call. Important."

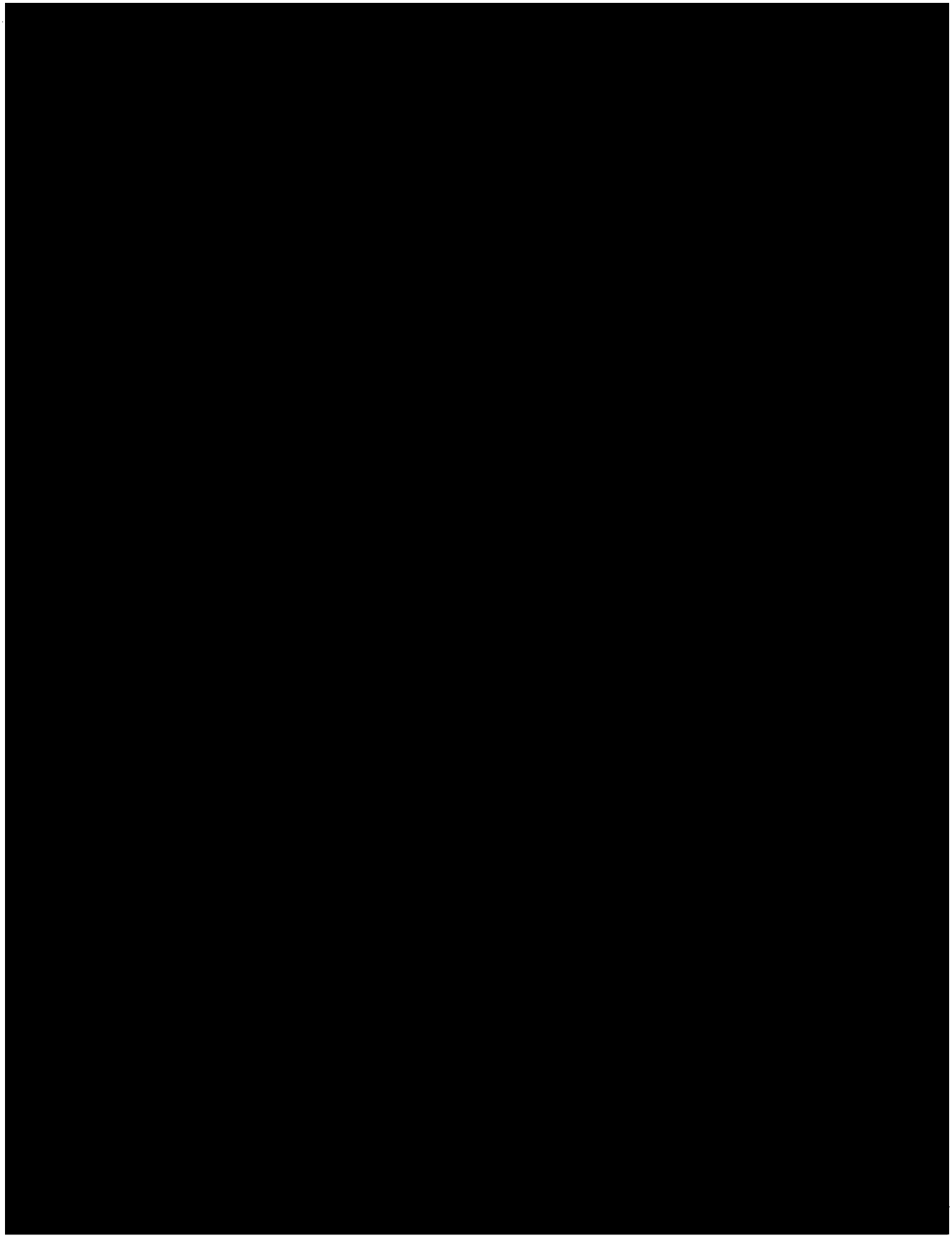
77. On or about October 19, 2016, STONE published an article on Breitbart.com in which he claimed he had, "no advance notice of Wikileaks' hacking of Podesta's e-mails." STONE stated that, "I predicted that Podesta's business dealings would be exposed. I didn't hear it from Wikileaks, although Julian 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.

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

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

80. 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. STONE's Congressional Testimony and Public Statements About His Relationship with Wikileaks

88. On September 26, 2017, STONE testified before the House Permanent Select Committee on Intelligence (HPSCI). Although the hearing was closed, STONE released to the public what he said were his opening remarks to the committee. In them, STONE stated:

> Members of this Committee have made three basic assertions against me which must be rebutted here today. The charge that I knew in advance about, and predicted, the hacking of Clinton campaign chairman John Podesta's email, that I had advanced knowledge of the source or actual content of the WikiLeaks disclosures regarding Hillary Clinton or that, my now public exchange with a persona that our intelligence agencies claim, but cannot prove, is a Russian asset, is anything but innocuous and are entirely false. Again, such assertions are conjecture, supposition, projection, and allegations but none of them are facts. . . .
>
> My Tweet of August 21, 2016, in which I said, "Trust me, it will soon be the Podesta's time in the barrel. #CrookedHillary" must be examined in context. I posted this at a time that my boyhood friend and colleague, Paul Manafort, had just resigned from the Trump campaign over allegations regarding his business activities in Ukraine. I thought it manifestly unfair that John Podesta not be held to the same standard. Note, that my Tweet of August 21, 2016, makes no mention, whatsoever, of Mr. Podesta's email, but does accurately predict that the Podesta brothers' business activities in Russia with the oligarchs around Putin, their uranium deal, their bank deal, and their Gazprom deal, would come under public scrutiny. . . .
>
> [L]et me address the charge that I had advance knowledge of the timing, content and source of the WikiLeaks disclosures from the DNC. On June 12, 2016, WikiLeaks' publisher Julian Assange[] announced that he was in possession of Clinton DNC emails. I learned this by reading it on Twitter. I asked a journalist who I knew had interviewed Assange to independently confirm this report, and he subsequently did. This journalist assured me that WikiLeaks would release this information in October and continued to assure me of this throughout the balance of August and all of September. This information proved to be correct. I have referred publicly to this journalist as an, "intermediary", "go-between" and "mutual friend." All of these monikers are equally true.

89. In a document dated March 26, 2018 titled "Minority Views," Democratic members of HPSCI published excerpts from Stone's September 2017 testimony before HPSCI. Those excerpts include the following:

> Q: Have any of your employees, associates, or individuals acting on your behest or encouragement been in any type of contact with Julian Assange?
> MR. STONE: No.
> ...
> Q: So throughout the many months in which you represented you were either in communication with Assange or communication through an intermediary with Assange, you were only referring to a single fact that you had confirmed with the intermediary –
> MR. STONE: That –
> Q: -- was the length and the breadth of what you were referring to?
> MR. STONE: That is correct, even though it was repeated to me on numerous separate occasions.

90. In the month that followed his testimony before HPSCI, on or about October 24, 2017, STONE published an article on his website, stonecoldtruth.com, titled "Is it the Podesta's Time in the Barrel Yet?" In that article, STONE stated: "[I]t was this inevitable scrutiny of the Podestas' underhanded business dealings that my 'time in the barrel' referred to and not, as some have quite falsely claimed, to the hacking and publication almost two months later of John Podesta's emails. . . . [M]y tweet referred to Podesta's business dealings with Russia, and the expectation that it would become a news story."

J. STONE's Messaging to Randy CREDICO about STONE's "Back channel"

91. On or about November 19, 2017, Randy CREDICO (who, as described further below, STONE publicly identified as his "intermediary" to ASSANGE), messaged STONE, "My lawyer wants to see me today." STONE responded, "'Stonewall it. Plead the fifth. Anything to save the plan'.....Richard Nixon[.]" CREDICO responded, "Ha ha."

92. On or about November 21, 2017, CREDICO messaged STONE, "I was told that the house committee lawyer told my lawyer that I will be getting a subpoena[.]" STONE wrote

back, "That was the point at which your lawyers should have told them you would assert your 5th Amendment rights if compelled to appear." They continued to message, and CREDICO wrote, "My lawyer wants me to cut a deal." STONE wrote back, "To do what ? Nothing happening in DC the day before Thanksgiving – why are u busting my chops?"

93. On or about November 24, 2017, STONE, texted CREDICO, "Assange is a journalist and a damn good one- meeting with him is perfectly legal and all you ever told me was he had the goods [o]n Hillary and would publish them – which he himself said in public b4 u told me . It's a fucking witchunt [sic]." CREDICO replied, "I told you to watch his tweets. That's what I was basing it on. I told you to watch his Tweets in October not before that I knew nothing about the DNC stuff[.] I just followed his tweets[.]" STONE responded, "U never said anything about the DNC but it was August." CREDICO wrote back, "It was not August because I didn't interview him or meet him until August 26th[.] That was my first communication with his secretary in London, August 26th." STONE wrote back, "Not the way I remember it – oh well I guess Schiff will try to get one of us indicted for perjury[.]"

94. STONE and CREDICO continued to exchange messages and on November 24, 2017, CREDICO wrote to STONE, "Forensic evidence proves that there is no back Channel. So now you can relax."

95. On or about November 28, 2017, CREDICO tweeted a copy of a subpoena he received from HPSCI that was dated November 27, 2017. Toll records show that on November 27 and 28, 2017, CREDICO and STONE communicated via text message more than a dozen times.

96. On November 29, 2017, STONE publicly stated that CREDICO was his "intermediary." In a public Facebook post, STONE further stated that "Credico merely []

confirmed for Mr. Stone the accuracy of Julian Assange's interview of June 12, 2016 with the British ITV network, where Assange said he had 'e-mails related to Hillary Clinton which are pending publication,' . . . Credico never said he knew or had any information as to source or content of the material."

97. On or about December 1, 2017, CREDICO messaged STONE, "I don't know why you had to lie and say you had a back Channel now I had to give all of my forensic evidence to the FBI today what a headache[.][4] You could have just told him the truth that you didn't have a back Channel they now know that I was not in London until September of this year[.] You had no back-channel and you could have just told the truth . . . You want me to cover you for perjury now[.]" STONE responded, "What the fuck is your problem? Neither of us has done anything wrong or illegal. You got the best press of your life and you can get away with asserting for 5th Amendment rights if u don't want talk about AND if you turned over anything to the FBI you're a fool." CREDICO responded, "You open yourself up to six counts of perjury[.] But I'm sure that wasn't sworn testimony so you're probably clear[.] Council for the committee knows you never had a back Channel and if you had just told the truth wouldn't have put me in this bad spot . . . you should go back . . . and amend your testimony and tell them the truth." CREDICO repeated: "you need to amend your testimony before I testify on the 15th." STONE replied, "If you testify you're a fool. Because of tromp [sic] I could never get away with a certain [sic] my Fifth Amendment rights but you can. I guarantee you you [sic] are the one who gets indicted for perjury if you're stupid enough to testify[.]"

[4] Contrary to his statement, CREDICO had not at that time provided any forensic evidence to the FBI.

98. STONE and CREDICO continued to message each other on or about December 1, 2017. In response to STONE's message about being "stupid enough to testify," CREDICO told STONE: "Whatever you want to say I have solid forensic evidence." STONE responded: "Get yourself a real lawyer instead of some liberal wimp who doesn't know how to tell his guys to fuck off good night." CREDICO then wrote: "Just tell them the truth and swallow your ego you never had a back Channel particularly on June 12th[.]" STONE responded: "You got nothing."

99. On or about December 13, 2017, according to public reporting, CREDICO indicated that he would not testify before HPSCI and would invoke his Fifth Amendment rights.

100. STONE and CREDICO continued to exchange text messages, and on or about January 6, 2018, CREDICO indicated to STONE that he was having dinner with a reporter. STONE responded, "Hope u don't fuck Up my efforts to get Assange a pardon[.]" CREDICO messaged STONE, "I have the email from his chief of staff August 25th 2016 responding to an email I sent to WikiLeaks website email address asking you would do my show[.] That was my initial contact."

101. On or about January 8, 2018, CREDICO messaged STONE, stating: "Embassy logs . . . + 17 other pieces of information prove that I did not have any conversations with Assange until September of last year."

102. CREDICO and STONE continued to message each other, and on or about January 25, 2018, CREDICO wrote to STONE: "You lied to the house Intel committee . . . But you'll get off because you're friends with Trump so don't worry. I have all the forensic evidence[.] I was not a ba[ck] Channel and I have all those emails from September of 2016 to prove it[.]"

103. On or about April 13, 2018, news reports stated that CREDICO had shown reporters copies of email messages he had received from STONE in the prior few days that

stated, "You are a rat. You are a stoolie. You backstab your friends — run your mouth my lawyers are dying Rip you to shreds." Another message stated, "I'm going to take that dog away from you," referring to CREDICO's therapy dog. CREDICO stated that it was "certainly scary . . . When you start bringing up my dog, you're crossing the line[.]"[5]

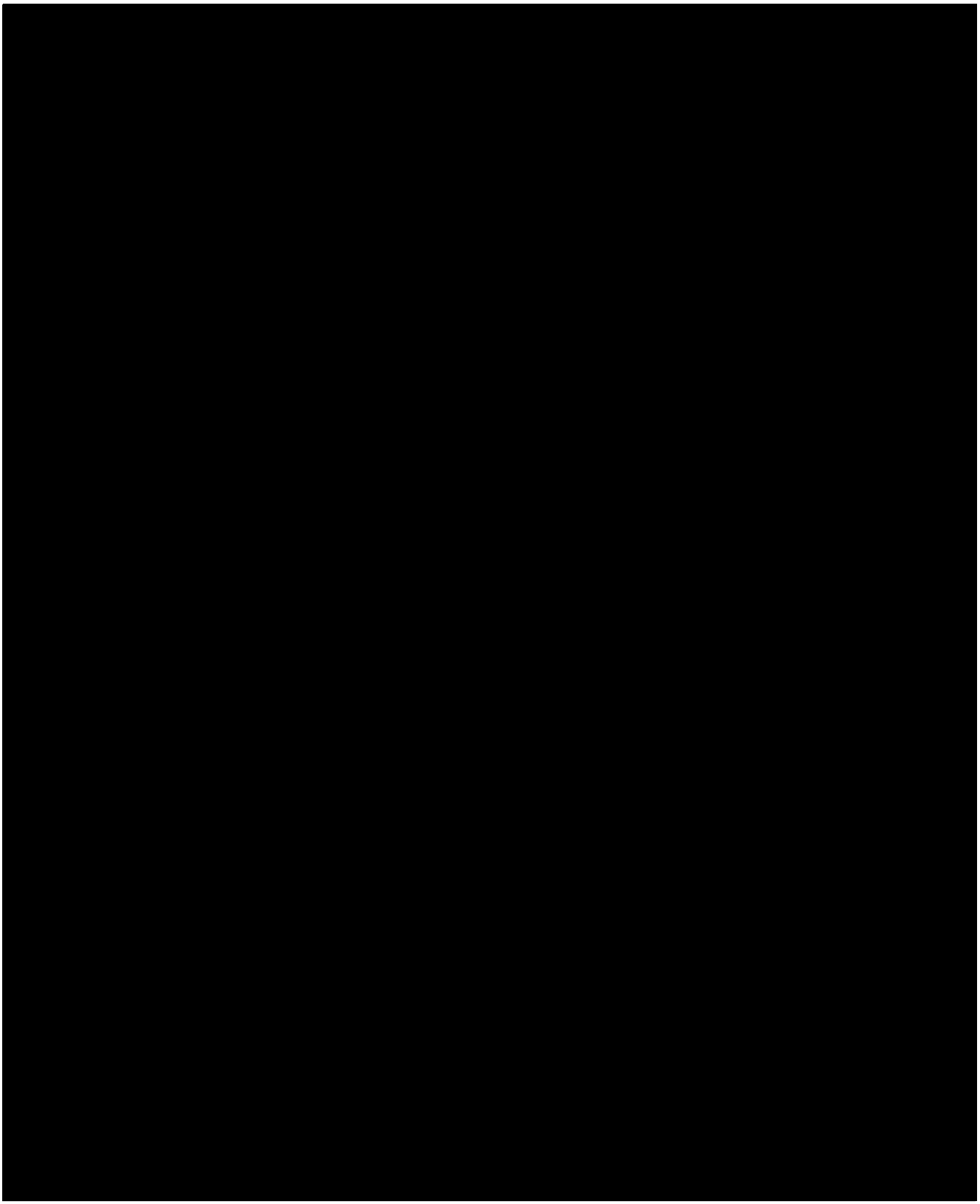
104. On or about May 25, 2018, CREDICO provided additional messages he stated were from STONE to another news agency.[6] In these messages, STONE, on April 9, 2018, stated: "I am so ready. Let's get it on. Prepare to die[.]" In the article, CREDICO stated that he considered this email from STONE a threat. STONE stated in the article that CREDICO "told me he had terminal prostate cancer . . . It was sent in response to that. We talked about it too. He was depressed about it. Or was he lying." The article noted that CREDICO stated he did not have prostate cancer and did not have any such discussion with STONE.

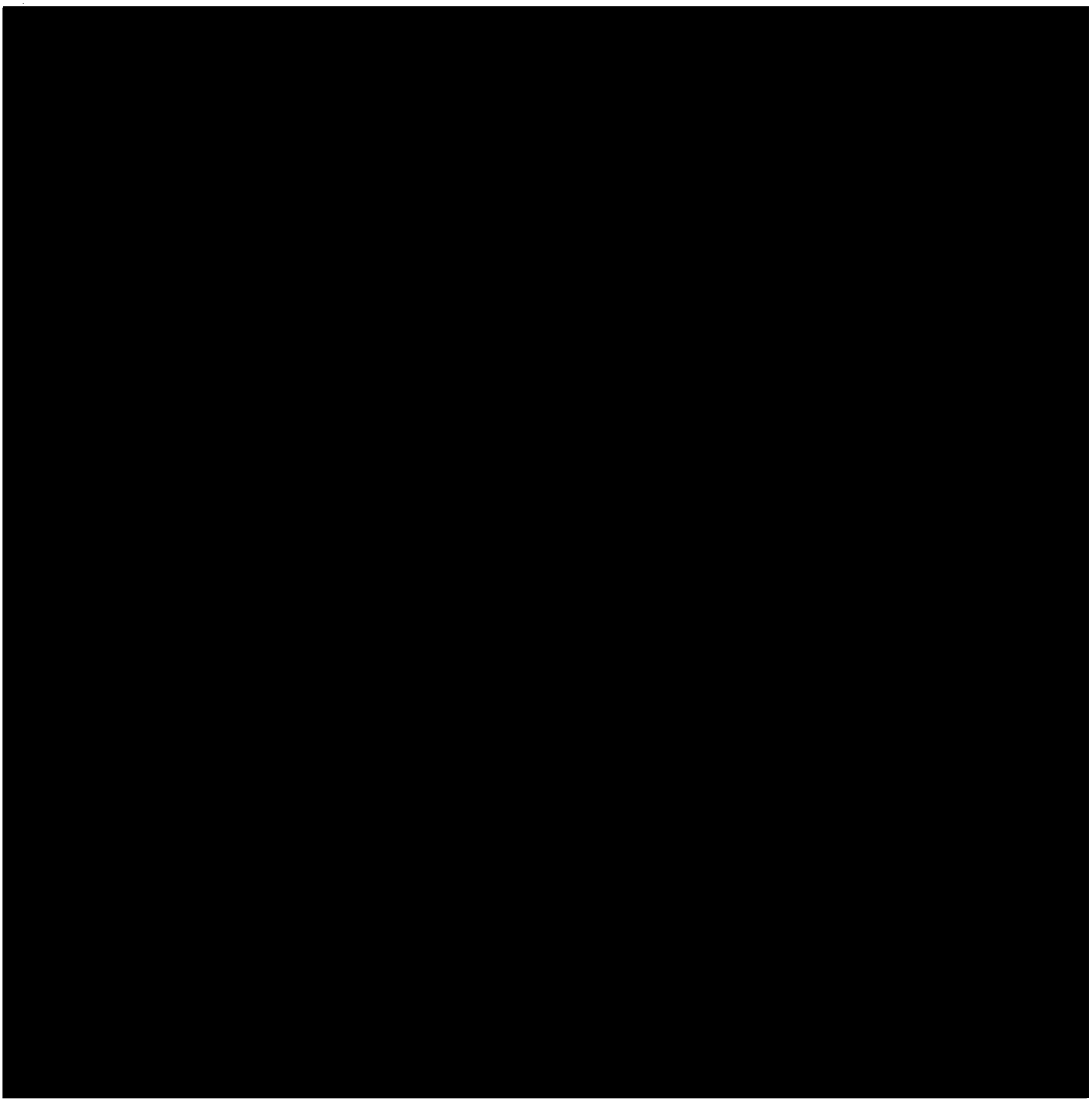
K. The Target Accounts

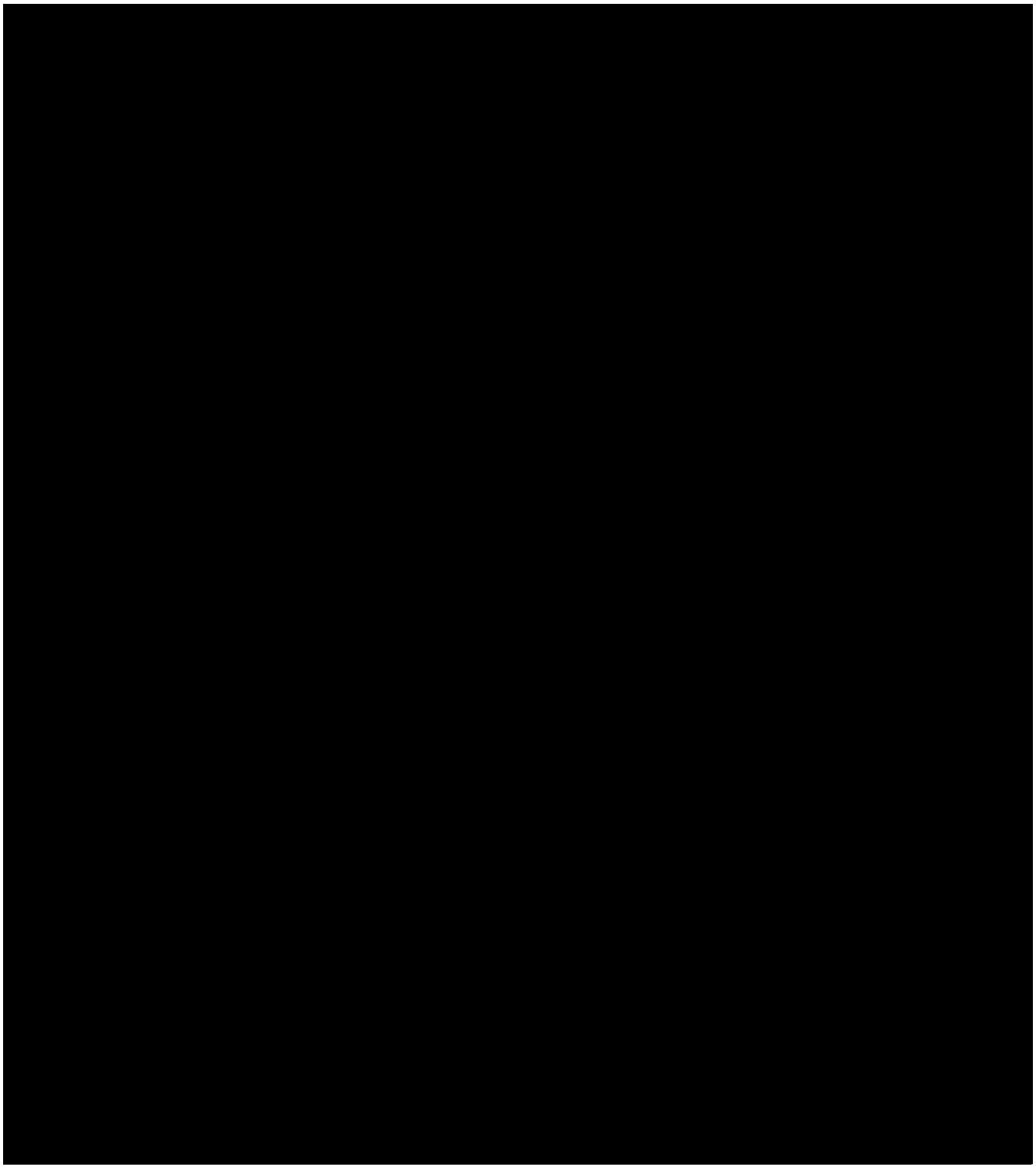
[redacted]

[5] https://www.yahoo.com/news/comedian-randy-credico-says-trump-adviser-roger-stone-threatened-dog-135911370.html

[6] https://www.motherjones.com/politics/2018/05/roger-stone-to-associate-prepare-to-die/







BACKGROUND CONCERNING MICROSOFT

115. In my training and experience, I have learned that Microsoft provides a variety of online services, including electronic mail ("email") access, voice communications services such

as Skype, Windows Live services, cloud storage services such as OneDrive, and software development kit accounts, to the public. Subscribers obtain any of these types of accounts by registering with Microsoft. During the registration process, Microsoft 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 email subscribers and information concerning subscribers and their use of email 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.

116. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for a services 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.

117. 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.

118. In my training and experience, in some cases, account users will communicate directly with a service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. 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.

119. 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. It is my understanding that Microsoft has access to email accounts with the top level domain .au, which is associated with Australia.

120. 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 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 inculpate 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).

FILTER REVIEW PROCEDURES

121. 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.

CONCLUSION

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

123. 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

124. 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,

Patrick J. Myers
Special Agent
Federal Bureau of Investigation

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

The Honorable Beryl A. Howell
Chief United States District Judge

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with the following Microsoft accounts, stored at premises owned, maintained, controlled, or operated by Microsoft Corporation ("Microsoft"), a company headquartered in Redmond, Washington:

[redacted]

This warrant also applies to information associated with the following Skype usernames and/or email addresses, stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, an electronic communication and/or remote computing service provider with headquarters in Redmond, Washington:

[redacted]

ATTACHMENT B

I. Information to be disclosed by Microsoft

To the extent that the information described in Attachment A is within the possession, custody, or control of the Microsoft Corporation (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 have been deleted but are 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 A:

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. The contents of all Skype communications sent to or from the account, including videos, instant messages, group messages, and attachments, as well as the complete conversation history for the account;

c. 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);

d. The types of service utilized;

which the accounts described in Attachment A are the recovery email address, provide 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).

II. Information to be Seized by the Government

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. § 1001 (false statements), 18 U.S.C. § 1030 (unauthorized access of a protected computer); 18 U.S.C. §§ 1505 and 1512 (obstruction of justice), 18 U.S.C. § 1513 (witness tampering), 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 contributions ban) for the period from March 1, 2016 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 Jerome Corsi, [redacted] Julian Assange, [redacted] Randy Credico, any individual associated with the Trump Campaign, any witness in the investigation;

c. Communications, records, documents, and other files related to any expenditure, independent expenditure, or disbursement for an electioneering communication;

d. Records of any funds or benefits disbursed by or offered on behalf of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

e. 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;

f. Communications, records, documents, and other files that reveal efforts by any person to conduct activities on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals;

g. 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;

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

i. The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s);

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

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

l. The identity of any non-U.S. person(s)—including records that help reveal the whereabouts of the person(s)—who made any expenditure, independent expenditure, or disbursement for an electioneering communication; and

m. The identity of any person(s)—including records that help reveal the whereabouts of the person(s)—who communicated with the account about any matters relating to activities conducted by on behalf of, for the benefit of, or at the direction of any foreign government, foreign officials, foreign entities, foreign persons, or foreign principals.

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

o. All existing printouts from original storage which concern the categories identified in subsection II.a.

III. 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.

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 MICROSOFT CORPORATION	Case: 1:18-sc-02920 Assigned To : Howell, Beryl A. Assign. Date : 9/27/2018 Description: Search & Seizure Warrant

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

The United States of America, moving by and through its undersigned counsel, respectfully moves the Court for an Order placing the above-captioned warrant and the application and affidavit in support thereof (collectively herein the "Warrant") under seal, and precluding the provider from notifying any person of the Warrant pursuant to 18 U.S.C. § 2705(b). In regard to the non-disclosure, the proposed Order would direct Microsoft Corporation ("Microsoft"), an electronic communication and/or remote computing services provider headquartered in Redmond, Washington, not to notify any other person (except attorneys for Microsoft for the purpose of receiving legal advice) of the existence or content of the Warrant for a period of one year or until further order of the Court.

JURISDICTION AND LEGAL BACKGROUND

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

2. In addition, this Court has jurisdiction to issue the requested order because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. Specifically, the Court is a "district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Acts or omissions in furtherance of the offense under investigation occurred within Washington, D.C. *See* 18 U.S.C. § 3237.

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

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

> (b) Preclusion of notice to subject of governmental access. — A governmental entity acting under section 2703 . . . may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court

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

> deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—
>
> (1) endangering the life or physical safety of an individual;
> (2) flight from prosecution;
> (3) destruction of or tampering with evidence;
> (4) intimidation of potential witnesses; or
> (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

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

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

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

5. Accordingly, this motion to seal sets forth facts showing reasonable grounds to command Microsoft not to notify any other person (except attorneys for Microsoft for the purpose of receiving legal advice) of the existence of the Subpoena for a period of one year or until further order of the Court.

FACTS SUPPORTING SEALING AND NON-DISCLOSURE

6. The Federal Bureau of Investigation ("FBI") is investigating 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. § 951 (acting as an unregistered foreign agent), 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 22 U.S.C. § 611 *et seq.*

(Foreign Agents Registration Act), and 52 U.S.C. § 30121 (foreign contribution ban) (the "Subject Offenses"), in connection with efforts to compromise the networks of the Democratic National Convention ("DNC"), the Democratic Congressional Campaign Committee ("DCCC"), and the email accounts of U.S. persons involved in the 2016 presidential election, followed by the public release of stolen materials through various outlets.

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

8. Given the complex and sensitive nature of the criminal activity under investigation, and also given that the criminal scheme may be ongoing, the Government anticipates that this confidential investigation will continue for the next year or longer. However, should circumstances change such that court-ordered nondisclosure under Section 2705(b) becomes no longer needed, the Government will notify the Court and seek appropriate relief.

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

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

WHEREFORE, for all the foregoing reasons, the government respectfully requests that the above-captioned warrant, the application and affidavit in support thereof, and all attachments thereto and other related materials be placed under seal, and furthermore, that the Court command Microsoft not to notify any other person of the existence or contents of the above-captioned warrant (except attorneys for Microsoft for the purpose of receiving legal advice) for a period of one year or until further order of the Court.

Respectfully submitted,

ROBERT S. MUELLER, III
Special Counsel

Dated: 9/27/18

By: _____

Kyle R. Freeny
The Special Counsel's Office
(202) 616-3812