

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, GOOGLE, AND APPLE

Case: 1:18-sc-02581
Assigned To : Howell, Beryl A.
Assign. Date : 8/3/2018
Description: Search & Seizure Warrant

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

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

See Attachment E

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 F

YOU ARE COMMANDED to execute this warrant on or before August 15, 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: 8/3/2018 at 2:58 PM
Judge's signature

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

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

Return

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

Inventory made in the presence of :

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

Certification

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

Date: _____

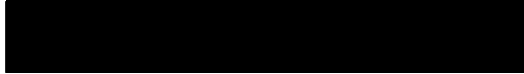
Executing officer's signature

Printed name and title

ATTACHMENT E

Property to be Searched

This warrant applies to information associated with the following Apple DSID:



created or maintained between March 14, 2018 and the present, that is stored at premises owned, maintained, controlled, or operated by Apple, Inc., located at One Apple Park Way, Cupertino, California 95014.

ATTACHMENT F

Particular Things to be Seized

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

To the extent that the information described in Attachment E is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment E:

- a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);
- b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);
- c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;
- d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

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

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be Seized by Law Enforcement Personnel

Any and all records that relate in any way to the accounts described in Attachment A which consists of evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 2 (aiding and abetting), 18 U.S.C. § 3 (accessory after the fact), 18 U.S.C. § 4 (misprision of a felony), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 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 contribution ban), from June 1, 2015 to 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, or any individual associated with the Trump Campaign;
- c. All images, messages, communications, calendar entries, search terms, "address book" entries and contacts, including any and all preparatory steps taken in furtherance of the above-listed offenses;
- d. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier concerning the messages identified above, including records about their identities and whereabouts;
- e. Evidence of the times the account was used;
- f. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
- g. Passwords and encryption keys, and other access information that may be necessary to access the account and other associated accounts;
- h. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;
- i. All existing printouts from original storage which concern the categories identified in subsection II.a

UNITED STATES DISTRICT COURT

for the District of Columbia

FILED

AUG - 3 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, GOOGLE, AND APPLE

Case: 1:18-sc-02581 Assigned To : Howell, Beryl A. Assign. Date : 8/3/2018 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 E

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

See Attachment F

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. §§ 1505, 1512, 1513 (Obstruction of justice, Witness tampering) and 18 U.S.C. §§ 1001, 1030, 371 (False Statements, Unauthorized Access of Protected Computer, Conspiracy).

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)

Handwritten signature of Andrew Mitchell

Applicant's signature

Andrew Mitchell, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date:

8/3/2018

Handwritten signature of Beryl A. Howell

Judge's signature

City and state: Washington, D.C.

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

Printed name and title

FILED

AUG - 3 2018

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

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
THREE ACCOUNTS STORED AT
PREMISES CONTROLLED BY
MICROSOFT, GOOGLE, AND APPLE

Case: 1:18-sc-02581
Assigned To : Howell, Beryl A.
Assign. Date : 8/3/2018
Description: Search & Seizure Warrant

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

I, Andrew Mitchell, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the following:

a. The email account [REDACTED] (hereafter "**Target Account 1**"), that is stored at premises owned, maintained, controlled, or operated by Microsoft, Inc., a business with offices located at One Microsoft Way, Redmond, Washington, 98052. The information to be disclosed by Microsoft and searched by the government is described in the following paragraphs and in Attachments A and B.

b. The email account [REDACTED] (hereafter "**Target Account 2**"), that is stored at premises owned, maintained, controlled, or operated by Google, Inc., a business with offices located at 1600 Amphitheatre Parkway, Mountain View, California, 94043. The information to be disclosed by Google and searched by the government is described in the following paragraphs and in Attachments C and D.

c. The iCloud account [REDACTED] associated with the Apple email account [REDACTED] (hereafter "**Target Account 3**"), that is stored at premises owned,

maintained, controlled, or operated by Apple, Inc., a business with offices located at 1 Infinite Loop, Cupertino, California 95014. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachment E and F.

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

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other 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 Accounts** contain communications relevant to 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 contribution ban) (the "Subject Offenses").

5. On September 11, 2017, Chief Judge Beryl A. Howell of the District of Columbia issued a search warrant for Roger STONE's Hotmail address, [REDACTED] (**Target Account 1**). On October 17, 2017, Chief Judge Howell issued a search warrant for STONE's Gmail address, [REDACTED] (**Target Account 2**). On or about March 14, 2018, Chief Judge Howell issued a search warrant for STONE's iCloud account (**Target Account 3**). This

warrant seeks to search those accounts from the date each respective warrant was issued to the present.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. *Id.* §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States (including a magistrate judge of such a court) . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). The offense conduct included activities in Washington, D.C., as detailed below, including in paragraphs 14, 19, and 61.

SUMMARY

7. This application seeks authority to search, from the date of search warrants previously issued by the Court to the present, three accounts believed to be used by Roger STONE: **Target Account 1**, which is STONE’s [REDACTED] account; **Target Account 2**, which is STONE’s [REDACTED] account; and **Target Account 3**, which is STONE’s iCloud account. As set forth herein, there is probable cause to believe that each of the Subject Accounts contains evidence of the Subject Offenses, including ongoing efforts to obstruct justice, tamper with witnesses, and make false statements.

8. For example, as set forth in more detail below, in recent months STONE has reached out to communicate with multiple witnesses he knew or had reason to believe were scheduled to testify before Congress about interactions with STONE during the 2016 presidential campaign or were scheduled to meet with the Special Counsel’s Office [REDACTED]
[REDACTED]. After STONE learned that one witness, Randy CREDICO, was prepared to contradict STONE’s congressional testimony, STONE repeatedly

urged CREDICO to assert the Fifth Amendment and decline to answer questions, and did so through multiple text messages. In June 2018, STONE instructed his private investigator to provide him with a full background investigation on another witness, [REDACTED] who had done information technology work for STONE during the campaign [REDACTED]

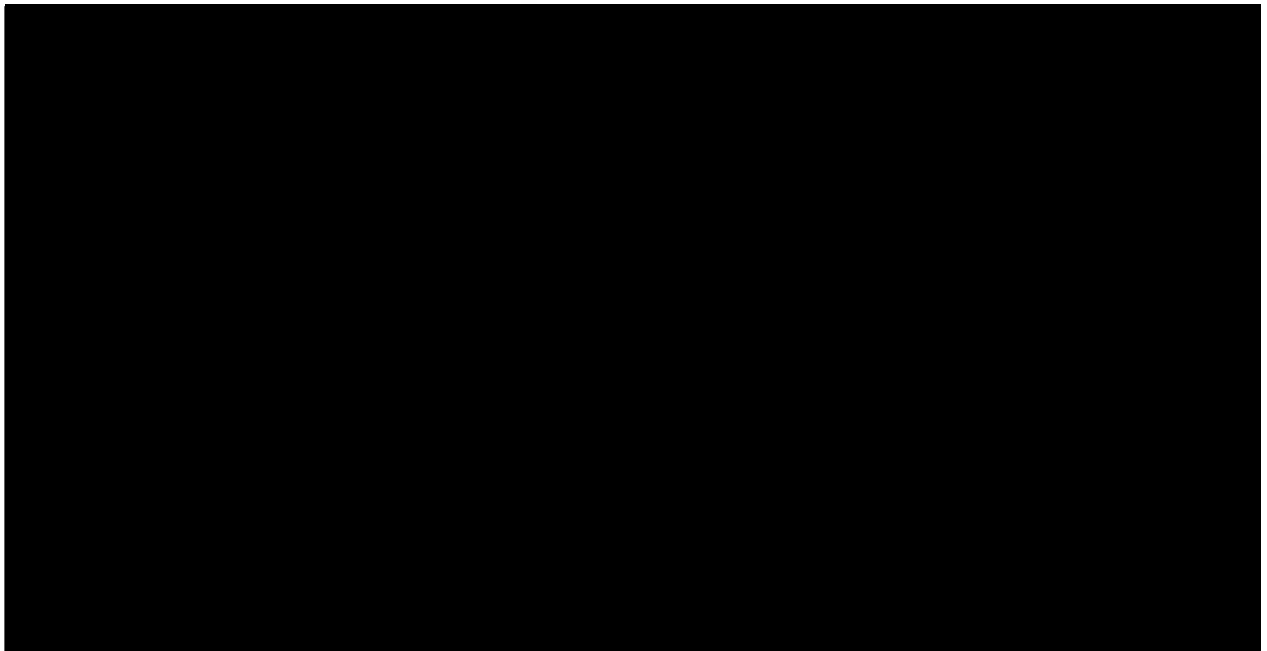
9. In September 2017, STONE released a statement he said he provided to Congress in which he denied having advance knowledge of “the source or actual content of the Wikileaks disclosures regarding Hillary Clinton.” He also stated publicly that when he tweeted during the campaign, on August 21, 2016, “it will soon be the Podesta’s time in the barrel,” he was not referring to the hacking or publication of John Podesta’s emails, but rather to “Podesta’s business dealings with Russia.” Evidence obtained in the investigation, however, shows the following:

a. On or about July 25, 2016, Roger STONE emailed Jerome CORSI to “Get to Assange” at the Ecuadorian Embassy and “get pending WikiLeaks emails[.]” Julian ASSANGE is the founder of WikiLeaks. On or about July 31, 2016, STONE also instructed CORSI to have [REDACTED] contact ASSANGE. On or about August 2, 2016, CORSI responded to STONE that the “[w]ord is friend in embassy plans 2 more dumps. One shortly after I’m back. 2nd in Oct. Impact planned to be very damaging... Time to let more than Podesta to be exposed as in bed w enemy if they are not ready to drop HRC.” After receipt of that message, on or about August 21, 2016, using @RogerJStoneJR, STONE tweeted: “Trust me, it will soon be the Podesta’s time in the barrel. #CrookedHillary.”

b. Information disclosures subsequently occurred on or about the times CORSI predicted: On or about August 12, 2016, the day CORSI was scheduled to return to the United States (“shortly after I’m back”), Guccifer 2.0 released hacked information related to the

Democratic Congressional Campaign Committee (DCCC). On or about October 7, 2016, the day the Washington Post published a breaking story about an Access Hollywood videotape of then-candidate Trump making disparaging remarks about women, WikiLeaks released emails hacked from the account of John Podesta.

c. Furthermore, on the day of the Access Hollywood video disclosure, there were phone calls between STONE and CORSI after the Washington Post contacted STONE prior to publication. At approximately 11:00AM, the Washington Post received a tip regarding the Access Hollywood video. Approximately one hour later, shortly before noon, STONE received a call from the Washington Post. Approximately ninety minutes later, before 2:00PM, STONE called CORSI and they spoke. Approximately forty minutes later, CORSI called STONE and the two spoke again at length. At approximately 4:00PM, the Washington Post published its story regarding the Access Hollywood tape. By approximately 4:30PM, WikiLeaks tweeted out its first release of emails hacked from John Podesta.



PROBABLE CAUSE.

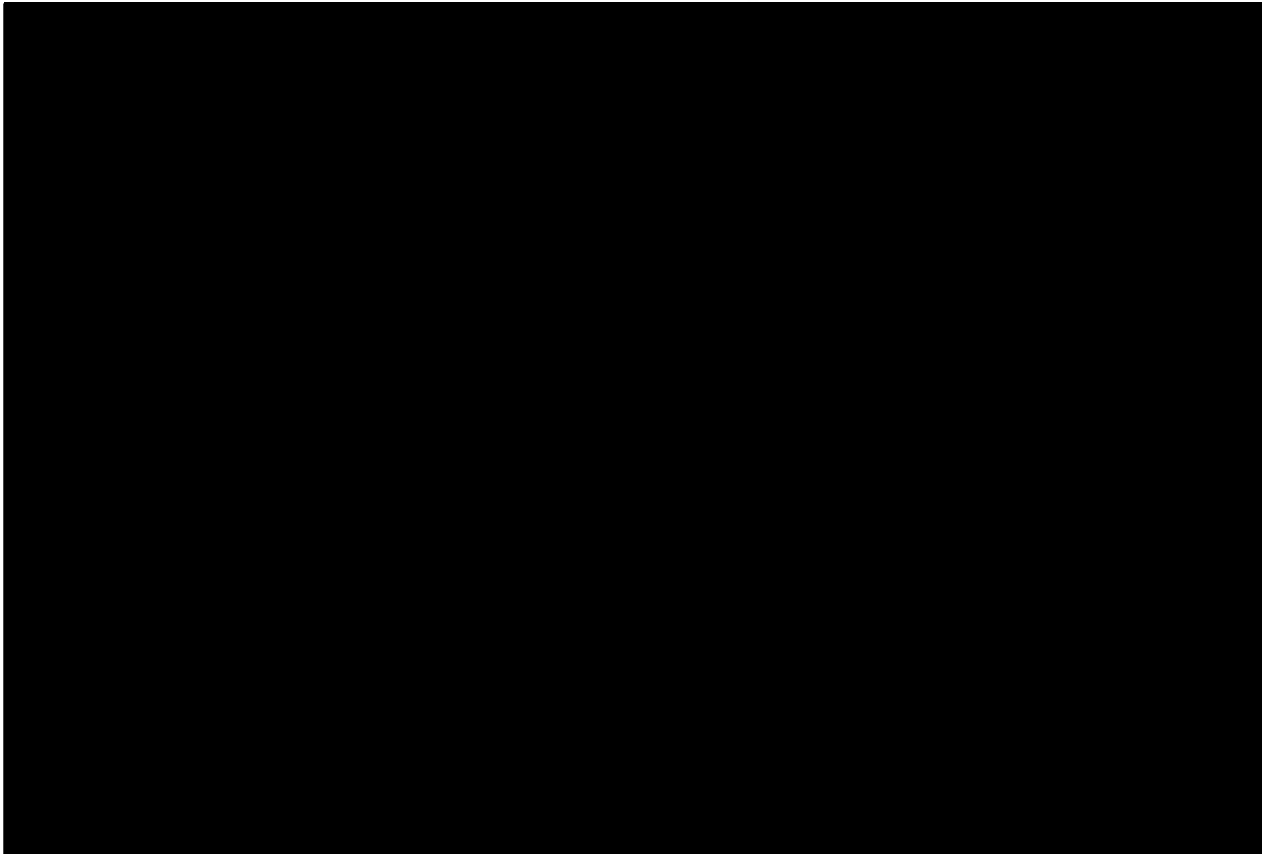
A. Background on Relevant Individuals

i. Roger STONE

10. 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

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



B. U.S. Intelligence Community Assessment of Russian Government-Backed Hacking Activity during the 2016 Presidential Election

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

a. The U.S. Intelligence Community (“USIC”) is confident that the Russian Government directed the recent compromises of emails from US persons and institutions, including from US political organizations. The recent disclosures of alleged hacked emails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts. These thefts and disclosures were

intended to interfere with the U.S. election process. Such activity is not new to Moscow—the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there. We believe, based on the scope and sensitivity of these efforts, that only Russia’s senior-most officials could have authorized these activities.

14. 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:

a. “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.”

b. 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.’”

c. 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.” The GRU is the foreign military intelligence agency of the Russian Ministry of Defense, and is Russia’s largest foreign intelligence agency.

d. 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.”

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

C. Additional Hacking Activity by Individuals Associated with the GRU

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

16. 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.

17. 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 posted on DCLeaks.

18. 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.

19. On or about July 13, 2018, a grand jury in this District indicted eleven GRU officers for knowingly and intentionally conspiring to hack into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election, steal documents from those computers, and stage releases of stolen documents in order to interfere with the election. The victims of the hacking and releases included the DNC, the Democratic Congressional Campaign Committee (“DCCC”), and the chairman of the Clinton campaign (John Podesta). *See United States v. Viktor Borisovich Netyksho, et al.* (1:18-cr-215) (D.D.C.).¹

D. Roger STONE’s Public Interactions with Guccifer 2.0 and WikiLeaks

20. 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. 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.

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

¹ A twelfth defendant was charged with conspiring to infiltrate computers of organizations responsible for administering elections, including state boards of election, secretaries of state, and companies that supply software and other technology used to administer elections.

22. 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."

23. On August 8, 2016, STONE addressed the Southwest Broward Republican Organization. During his speech, he was asked about a statement by 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.

24. 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.

25. 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.

26. 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.”

27. On August 18, 2016, Paul Manafort, STONE’s longtime friend and associate, resigned as Chairman of the Trump Campaign.

28. As noted above, 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 acquaintancē’ 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.”

29. 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.”

30. On Saturday, October 1, 2016, using @RogerJStoneJr, STONE tweeted, “Wednesday @ HillaryClinton is done. #WikiLeaks.”

31. On Sunday, October 2, 2016, MSNBC Morning Joe producer Jesse Rodriguez 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.”

32. 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.

33. 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.

34. 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.”

35. 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.”

E. STONE’s Private Twitter Direct Messages with WikiLeaks and ASSANGE

36. On August 7, 2017, Chief Judge Beryl A. Howell issued a search warrant for the Twitter account @RogerJStoneJr. Information recovered from the search of that account includes the following:

a. 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.”

b. 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.”

c. 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.”

d. 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."

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

f. 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."

F. STONE's Communications with STONE, [REDACTED] and Others Regarding Forthcoming Leaks

37. As indicated above, on September 11, 2017, Chief Judge Howell issued a search warrant for STONE's [REDACTED] address, [REDACTED] (**Target Account 1**); on October 17, 2017, Chief Judge Howell issued a search warrant for STONE's [REDACTED] address, [REDACTED] (**Target Account 2**); and on or about March 14, 2018, Chief Judge Howell issued a search warrant for STONE's iCloud account (**Target Account 3**). In addition, on or about December 19, 2017, Chief Judge Howell issued a search warrant for [REDACTED] email account. Information recovered pursuant to those search warrants includes the following:

a. 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 **Target Account 1**, who replied to CORSI that, "May meet Manafort -guarantee nothing."

b. On or about May 18, 2016, CORSI emailed STONE at **Target Account 1** 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."

c. On July 25, 2016, STONE, using **Target Account 1**, 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.”

d. On or about July 31, 2016, STONE, using **Target Account 1**, 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.”

e. As noted above, on or about August 2, 2016 (approximately 19 days before STONE publicly tweeted about “Podesta’s time in the barrel”), CORSI emailed STONE at **Target Account 1**: “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.

f. On or about August 5, 2016, [REDACTED], an associate of STONE’s, emailed Stone at **Target Account 1**. 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

g. On or about August 15, 2016, CORSI emailed STONE at **Target Account 1**: “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.”

h. On or about August 31, 2016, CORSI emailed STONE at **Target Account 1**: “Did you get the PODESTA writeup.” STONE replied “[y]es.”

i. On or about August 31, 2016, CORSI messaged STONE at **Target Account 3**, “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.”

j. On or about September 6, 2016, CORSI emailed STONE at **Target Account 1**: “Roger[,] Is NY Post going to use the Pedesta [sic] stuff?”

k. 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,

[REDACTED]

“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.

l. On or about October 3, 2016, an associate of STONE emailed STONE at **Target Account 2** and asked: “Assange – what’s he got? Hope it’s good.” STONE wrote back, “It is. I’d tell Bannon but he doesn’t call me back. My book on the TRUMP campaign will be out in Jan. Many scores will be settled.” The associate forwarded the email to Steve BANNON, 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.”

m. 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.

n. On or about October 4, 2016, CORSI messaged STONE at **Target Account 3**, “Assange made a fool of himself. Has nothing or he would have released it. Total BS hype.”

o. That same day, BANNON emailed STONE at **Target Account 2**, “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.”

p. 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.

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

38. 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.”

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

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

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

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

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

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

44. 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 on **Target Account 1**, "I expect that much of next dump focus, setting stage for Foundation debacle."

45. 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 **Target Account 2**, forwarded [REDACTED] message to CORSI without comment. STONE does not appear to have forwarded the email to any other individual.

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

46. On or about October 8, 2016, STONE, using **Target Account 3**, 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.”

47. On or about Wednesday, October 12, 2016, at approximately 8:17AM, STONE, using **Target Account 2**, emailed Corsi asking him to “send me your best podesta links.” STONE emailed CORSI at approximately 8:44AM, “need your BEST podesta pieces.” CORSI wrote back at approximately 8:54AM, “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?”

48. On or about that same day, October 12, 2016, Podesta accused STONE of having advance knowledge of the publication of his emails, as noted above. At approximately 3:25PM, CORSI emailed STONE at both **Target Account 1** and **2** with 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.”

49. 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 **Target Account 1**: “Got them and used them.”

50. On or about Thursday, October 13, 2016, CORSI emailed STONE at **Target Account 2**: “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

██████████ skimmed maybe billions off Skolkovo — Skolkovo kept their money with Metcombank[.] The Russians launched a criminal investigation[.] [web link] Once ██████████ 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[.]"

51. On or about Thursday, October 13, 2016, at approximately 6:30PM, CORSI sent STONE an email at **Target Account 2**, 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 ██████████, 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 ██████████, 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?"

52. On or about October 14, 2016, CORSI sent a message to STONE at **Target Account 3**, "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."

53. On or about October 17, 2016, CORSI messaged STONE at **Target Account 3**, “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.”

54. On or about October 17, 2016, CORSI emailed STONE at **Target Accounts 1 and 2** 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.”

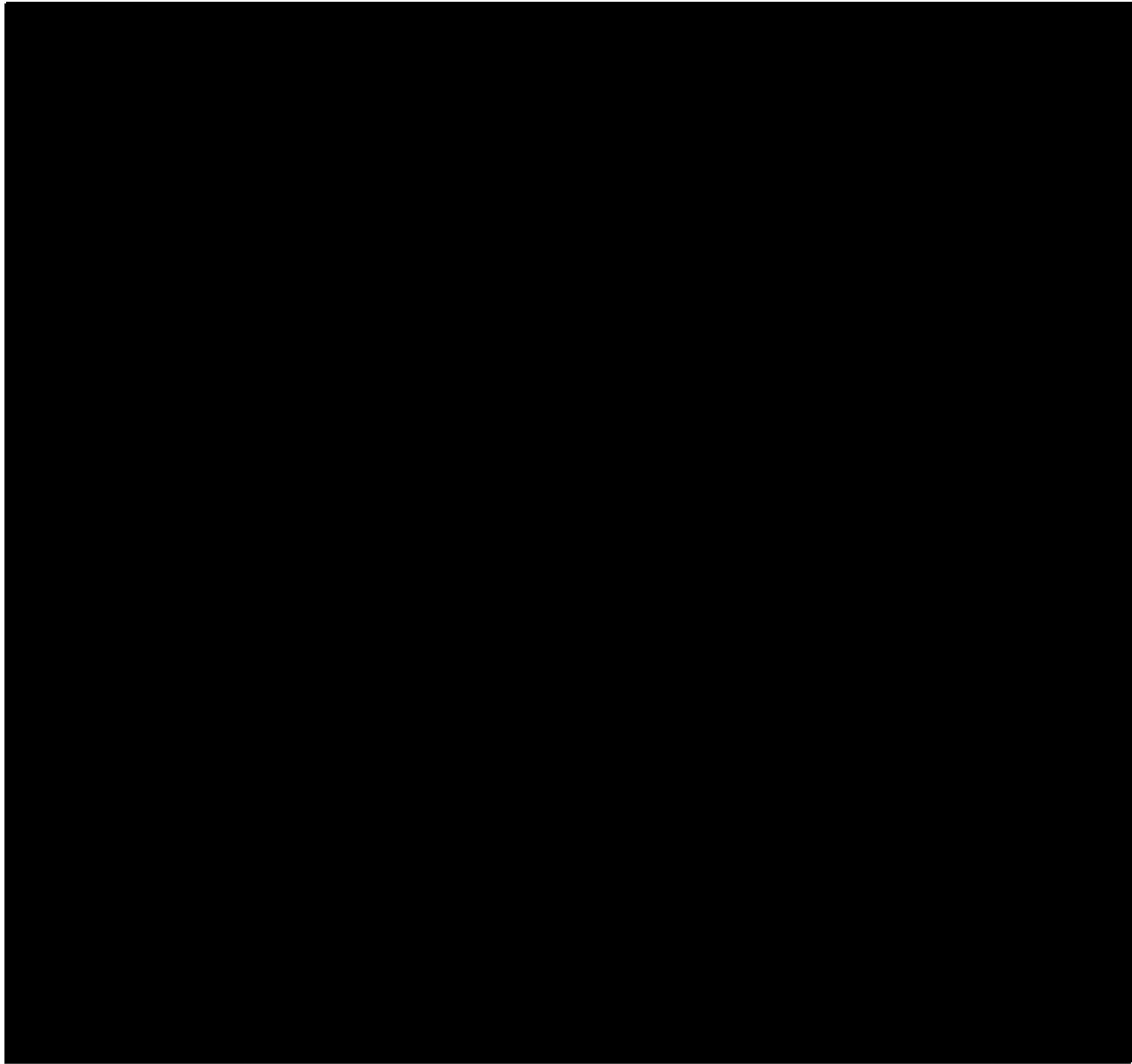
55. On or about October 18, 2016, CORSI messaged STONE at **Target Account 3**, “Pls call. Important.”

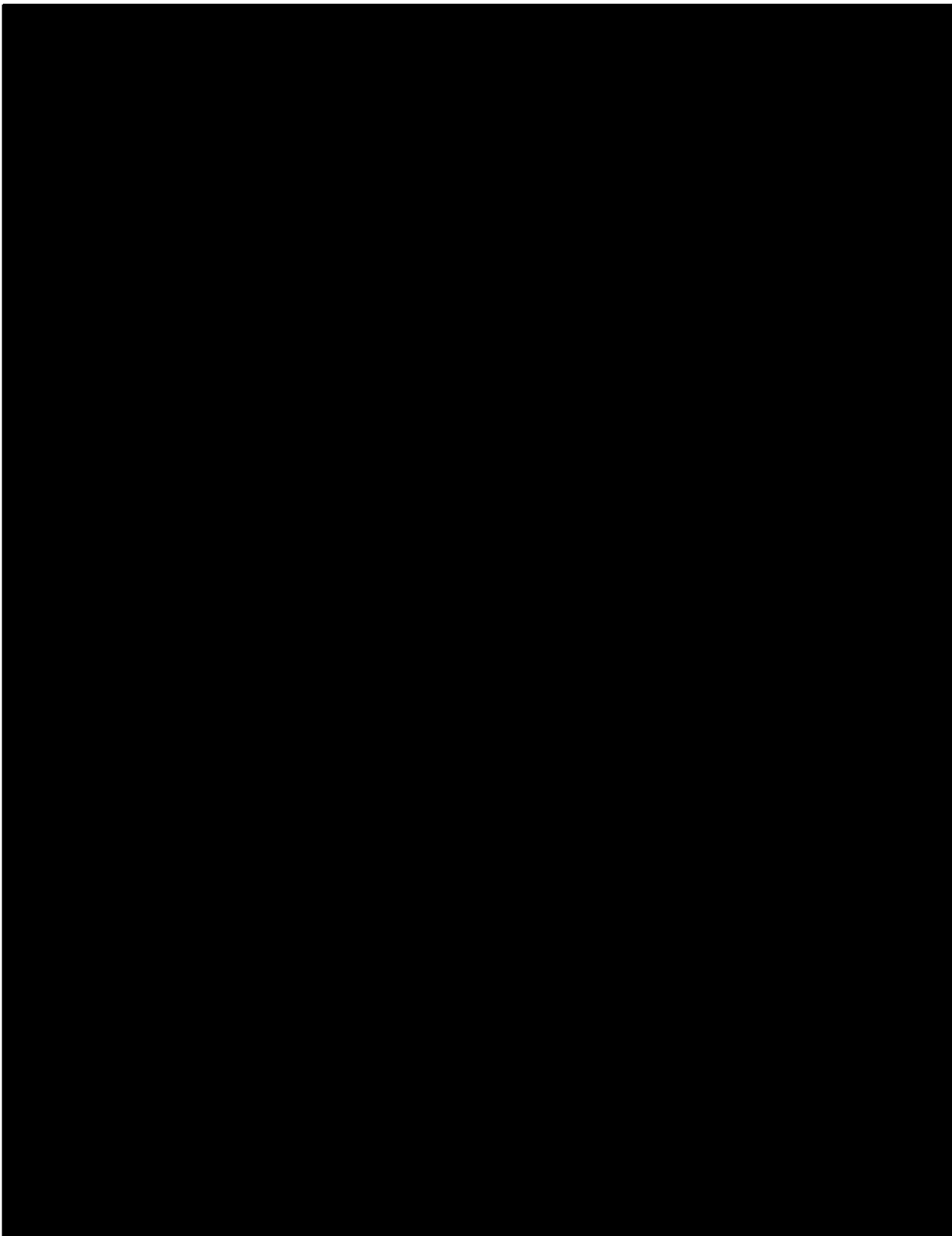
56. On or about October 19, 2016, STONE published an article on Breitbart.com in which he claimed he had “no advance notice of Wikileaks’ hacking of Podesta’s e-mails.” STONE stated, “I predicted that Podesta’s business dealings would be exposed. I didn’t hear it from Wikileaks, although Julian Assange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

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

58. On or about November 9, 2016, CORSI messaged STONE at **Target Account 3**, “Congratulations, Roger. He could not have done it without you.”

59. On or about November 10, 2016, CORSI messaged STONE at **Target Account 3**, “Are you available to talk on phone?” Several minutes later, CORSI messaged, “I’m in London. Have some interesting news for you.”





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

61. 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.

62. 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.

63. 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.”

K. STONE’s Use of Target Account 3 to Message Randy CREDICO about STONE’s “Back channel”

64. On November 19, 2017, Randy CREDICO (who, as described further below, STONE publicly identified as his “intermediary” to ASSANGE), messaged STONE on **Target Account 3**, “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.”

65. On or about November 21, 2017, CREDICO messaged STONE on **Target Account 3**, “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?”

66. On or about November 24, 2017, STONE, using **Target Account 3**, 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 witchhunt [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[.]”

67. STONE and CREDICO continued to exchange messages via **Target Account 3**, and on November 24, 2017, CREDICO wrote to STONE, “Forensic evidence proves that there is no back Channel. So now you can relax.”

68. 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.

69. 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.”

70. On or about December 1, 2017, CREDICO messaged STONE on **Target Account 3**, stating, “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

⁴ Contrary to his statement, CREDICO has not provided any forensic evidence to the FBI.

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[.]"

71. 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."

72. 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.

73. STONE and CREDICO continued to exchange messages via **Target Account 3**, 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."

74. On or about January 8, 2018, CREDICO messaged STONE on **Target Account 3** stating: “Embassy logs . . . + 17 other pieces of information prove that I did not have any conversations with Assange until September of last year.”

75. CREDICO and STONE continued to message each other, and on or about January 25, 2018, CREDICO wrote to STONE on **Target Account 3**: “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[.]”

76. 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

77. 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.

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/>

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.

L. STONE’s Use of the Target Accounts to Communicate with Individuals Related to the Investigation

78. On May 17, 2018, Chief Judge Howell issued an order for the use of pen-trap devices on **Target Account 1** and **Target Account 2**. The information obtained from that order, along with information obtained from toll records, revealed that STONE has continued to use **Target Account 1** and **Target Account 2**, and that he has used them to communicate with individuals related to the investigation.

79. For example, STONE and [REDACTED] communicated twice on May 28 and May 29, 2018 using **Target Account 1**. [REDACTED], a former associate of STONE’s, was interviewed by the Special Counsel’s Office on or about May 2, 2018. Toll records show that [REDACTED] and STONE communicated multiple times on May 5, 2018, and STONE communicated with [REDACTED] using **Target Account 1** on June 1, 2018 and June 6, 2018. [REDACTED], a private investigator who had previously worked with STONE and who was hired by STONE to research individuals associated with this case (as described further below), communicated with STONE on **Target Account 1** at least four times between May 27, 2018 and July 12, 2018.

80. STONE has also used **Target Account 2** to communicate with individuals associated with this investigation.

a. For example, between May 23, 2018 and the present, STONE and CORSI exchanged at least five messages using **Target Account 2**. In the same time period, STONE exchanged at least 75 emails with CREDICO using **Target Account 2**.

b. Also in this same time period, STONE emailed [REDACTED] at least ten times using **Target Account 2**. [REDACTED] is a former employee of STONE. On May 9, 2018, FBI agents approached [REDACTED] and [REDACTED]. That day, and again on May 10, 2018, [REDACTED] communicated by phone with STONE. Overall, between May 23, 2018 and the present, STONE exchanged over 100 emails with [REDACTED], using **Target Account 2**. In addition, between on or about June 14, 2018 and June 17, 2018, [REDACTED] and STONE exchanged five emails using **Target Account 2**.

[REDACTED]

81. STONE has also used a phone number associated with **Target Account 3** to communicate with [REDACTED] a private investigator hired by STONE. [REDACTED] was interviewed by investigators on June 7, 2018, and subsequently informed investigators that in June 2018, STONE instructed him to conduct a full background investigation on [REDACTED] [REDACTED] who had been employed by STONE during the Campaign as an information technology specialist. [REDACTED] [REDACTED] also told investigators that in June 2018, STONE instructed him to find an address for CREDICO that could be used to serve CREDICO with legal process. [REDACTED] told investigators that his primary form of communication with STONE is by text message on **Target Account 3**.

BACKGROUND CONCERNING EMAIL

82. In my training and experience, I have learned the Providers provide a variety of on-line services, including electronic mail ("email") to the public. The Providers allow

subscribers to obtain email accounts at the domain names identified in the email address contained in Attachment A and C. Subscribers obtain an account by registering with the Providers. During the registration process, the Providers ask subscribers to provide basic personal information. Therefore, the computers of the Providers are likely to contain stored electronic communications (including retrieved and unretrieved email) for their subscribers and information concerning subscribers and their use of 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.

83. 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.

84. 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 Providers' 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.

85. In my training and experience, in some cases, email account users will communicate directly with an email service Providers 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 Providers' support services, as well as records of any actions taken by the Providers 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.

86. 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 Providers 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).

87. In my training and experience, information such as search history can help to show the state of mind of an individual at the time the search was made, as well as the individuals potential advance knowledge of events, as they search to see if the anticipated event has occurred.

INFORMATION REGARDING APPLE ID AND iCloud⁷

⁷ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; "Create and start using an Apple ID," available at <https://support.apple.com/en-us/HT203993>; "iCloud," available at <http://www.apple.com/icloud/>; "What does iCloud back up?," available at <https://support.apple.com/kb/PH12519>; "iOS Security," available at

88. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

89. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user

https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

90. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

91. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

92. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in 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 and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

93. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

94. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

95. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

96. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish 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.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

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

CONCLUSION

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

99. 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

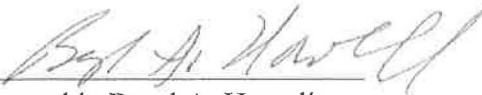
100. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation, the full nature and extent of which is not known to all of the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

Respectfully submitted,



Andrew Mitchell
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on this 31st day of August, 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 email address:



created or maintained between September 11, 2017 and present, 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

Particular Things to be Seized

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

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

- a. The contents of all e-mails, attachments and chat messages stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination e-mails sent addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All existing printouts from original storage of all of the electronic mail described above in Section I.A. above;
- c. All internet search data including all queries and location data;
- d. All transactional information of all activity of the account described above in Section I.A, including log files, dates, times, methods of connecting, ports, dial ups, and/or locations;
- e. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- f. Records or other information regarding the identification of the account described above in Section I.A, to include application, full name, physical address, telephone numbers and other identifiers, records of session times and durations, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, all screen names associated with subscribers and/or accounts, all account names associated with the subscriber,
- g. All records indicating the services available to subscribers of the electronic mail address described above in Section I.A.;

II. Information to be Seized by Law Enforcement Personnel

Any and all records that relate in any way to the accounts described in Attachment A which consists of evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 2 (aiding and abetting), 18 U.S.C. § 3 (accessory after the fact), 18 U.S.C. § 4 (misprision of a felony), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 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 contribution ban) from June 1, 2015 to 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, or any individual associated with the Trump Campaign;
- c. All images, messages, communications, calendar entries, search terms, "address book" entries and contacts, including any and all preparatory steps taken in furtherance of the above-listed offenses;
- d. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier concerning the messages identified above, including records about their identities and whereabouts;
- e. Evidence of the times the account was used;
- f. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
- g. Passwords and encryption keys, and other access information that may be necessary to access the account and other associated accounts;
- h. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;

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

ATTACHMENT C

Property to be Searched

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



created or maintained between October 17, 2017 and the present, that is stored at premises owned, maintained, controlled, or operated by Google, Inc., a business with offices located at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT D

Particular Things to be Seized

I. Files and Accounts to be produced by Google, Inc.

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

- a. The contents of all e-mails, attachments and chat messages stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination e-mails sent addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All existing printouts from original storage of all of the electronic mail described above in Section I.A. above;
- c. All internet search data including all queries and location data;
- d. All transactional information of all activity of the account described above in Section I.A, including log files, dates, times, methods of connecting, ports, dial ups, and/or locations;
- e. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- f. All records or other information regarding the identification of the account described above in Section I.A, to include application, full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, all screen names associated with subscribers and/or accounts, all account names associated with the subscriber, methods of connecting, log files, means and source of payment (including any credit or bank account number), and detailed billing records;
- g. All records indicating the services available to subscribers of the electronic mail address described above in Section I.A.;
- h. Google+ subscriber information, circle information, including name of circle and members, contents of posts, comments, and photos, to include date and timestamp;

- i. Google Drive files created, accessed or owned by the account;
- j. YouTube subscriber information, private videos and files, private messages, and comments;
- k. Google+ Photos contents to include all images, videos and other files, and associated upload/download date and timestamp;
- l. Google Talk and Google Hangouts conversation logs associated with the account.

II. Information to be Seized by Law Enforcement Personnel

Any and all records that relate in any way to the accounts described in Attachment C 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 contribution ban), from June 1, 2015 to 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, or any individual associated with the Trump Campaign;
- c. All images, messages, communications, calendar entries, search terms, "address book" entries and contacts, including any and all preparatory steps taken in furtherance of the above-listed offenses;
- d. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier concerning the messages identified above, including records about their identities and whereabouts;
- e. Evidence of the times the account was used;
- f. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
- g. Passwords and encryption keys, and other access information that may be necessary to access the account and other associated accounts;
- h. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;
- i. All existing printouts from original storage which concern the categories identified in subsection II.a

ATTACHMENT E

Property to be Searched

This warrant applies to information associated with the following Apple DSID:



created or maintained between March 14, 2018 and the present, that is stored at premises owned, maintained, controlled, or operated by Apple, Inc., located at One Apple Park Way, Cupertino, California 95014.

ATTACHMENT F

Particular Things to be Seized

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

To the extent that the information described in Attachment E is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment E:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

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

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be Seized by Law Enforcement Personnel

Any and all records that relate in any way to the accounts described in Attachment A which consists of evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 2 (aiding and abetting), 18 U.S.C. § 3 (accessory after the fact), 18 U.S.C. § 4 (misprision of a felony), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 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 contribution ban), from June 1, 2015 to 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, or any individual associated with the Trump Campaign;
- c. All images, messages, communications, calendar entries, search terms, "address book" entries and contacts, including any and all preparatory steps taken in furtherance of the above-listed offenses;
- d. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier concerning the messages identified above, including records about their identities and whereabouts;
- e. Evidence of the times the account was used;
- f. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
- g. Passwords and encryption keys, and other access information that may be necessary to access the account and other associated accounts;
- h. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;
- i. All existing printouts from original storage which concern the categories identified in subsection II.a

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, GOOGLE, AND APPLE

Case: 1:18-sc-02582
Assigned To : Howell, Beryl A.
Assign. Date : 8/3/2018
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 August 15, 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: 8/3/2018 at 3:00 PM Beryl A. Howell
Judge's signature

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

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

Return

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

Inventory made in the presence of :

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

Certification

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

Date: _____

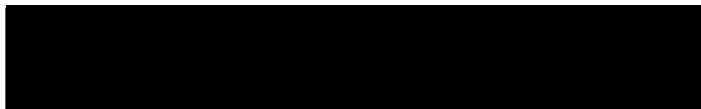
_____ *Executing officer's signature*

_____ *Printed name and title*

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with the email address:



created or maintained between September 11, 2017 and present, 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

Particular Things to be Seized

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

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

- a. The contents of all e-mails, attachments and chat messages stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination e-mails sent addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All existing printouts from original storage of all of the electronic mail described above in Section I.A. above;
- c. All internet search data including all queries and location data;
- d. All transactional information of all activity of the account described above in Section I.A, including log files, dates, times, methods of connecting, ports, dial ups, and/or locations;
- e. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- f. Records or other information regarding the identification of the account described above in Section I.A, to include application, full name, physical address, telephone numbers and other identifiers, records of session times and durations, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, all screen names associated with subscribers and/or accounts, all account names associated with the subscriber,
- g. All records indicating the services available to subscribers of the electronic mail address described above in Section I.A.;

II. Information to be Seized by Law Enforcement Personnel

Any and all records that relate in any way to the accounts described in Attachment A which consists of evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 2 (aiding and abetting), 18 U.S.C. § 3 (accessory after the fact), 18 U.S.C. § 4 (misprision of a felony), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 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 contribution ban) from June 1, 2015 to 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, or any individual associated with the Trump Campaign;
- c. All images, messages, communications, calendar entries, search terms, "address book" entries and contacts, including any and all preparatory steps taken in furtherance of the above-listed offenses;
- d. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier concerning the messages identified above, including records about their identities and whereabouts;
- e. Evidence of the times the account was used;
- f. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
- g. Passwords and encryption keys, and other access information that may be necessary to access the account and other associated accounts;
- h. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;

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

UNITED STATES DISTRICT COURT

for the District of Columbia

FILED

AUG - 3 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, GOOGLE, AND APPLE

Case: 1:18-sc-02582 Assigned To : Howell, Beryl A. Assign. Date : 8/3/2018 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):

- [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. §§ 1505, 1512, 1513 (Obstruction of justice, Witness tampering) and 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.

- [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)

Applicant's signature

Andrew Mitchell, Special Agent, FBI Printed name and title

Sworn to before me and signed in my presence.

Date: 8/3/2018

Judge's signature

City and state: Washington, D.C.

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

FILED

AUG - 3 2018

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

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
THREE ACCOUNTS STORED AT
PREMISES CONTROLLED BY
MICROSOFT, GOOGLE, AND APPLE

Case: 1:18-sc-02582
Assigned To : Howell, Beryl A.
Assign. Date : 8/3/2018
Description: Search & Seizure Warrant

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

I, Andrew Mitchell, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the following:

a. The email account [REDACTED] (hereafter "**Target Account 1**"), that is stored at premises owned, maintained, controlled, or operated by Microsoft, Inc., a business with offices located at One Microsoft Way, Redmond, Washington, 98052. The information to be disclosed by Microsoft and searched by the government is described in the following paragraphs and in Attachments A and B.

b. The email account [REDACTED] (hereafter "**Target Account 2**"), that is stored at premises owned, maintained, controlled, or operated by Google, Inc., a business with offices located at 1600 Amphitheatre Parkway, Mountain View, California, 94043. The information to be disclosed by Google and searched by the government is described in the following paragraphs and in Attachments C and D.

c. The iCloud account [REDACTED] associated with the Apple email account [REDACTED] (hereafter "**Target Account 3**"), that is stored at premises owned,

maintained, controlled, or operated by Apple, Inc., a business with offices located at 1 Infinite Loop, Cupertino, California 95014. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachment E and F.

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

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other 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 Accounts** contain communications relevant to 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 contribution ban) (the “Subject Offenses”).

5. On September 11, 2017, Chief Judge Beryl A. Howell of the District of Columbia issued a search warrant for Roger STONE’s [REDACTED] address, [REDACTED] (**Target Account 1**). On October 17, 2017, Chief Judge Howell issued a search warrant for STONE’s [REDACTED] address, [REDACTED] (**Target Account 2**). On or about March 14, 2018, Chief Judge Howell issued a search warrant for STONE’s iCloud account (**Target Account 3**). This

warrant seeks to search those accounts from the date each respective warrant was issued to the present.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. *Id.* §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States (including a magistrate judge of such a court) . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). The offense conduct included activities in Washington, D.C., as detailed below, including in paragraphs 14, 19, and 61.

SUMMARY

7. This application seeks authority to search, from the date of search warrants previously issued by the Court to the present, three accounts believed to be used by Roger STONE: **Target Account 1**, which is STONE’s [REDACTED] account; **Target Account 2**, which is STONE’s [REDACTED] account; and **Target Account 3**, which is STONE’s iCloud account. As set forth herein, there is probable cause to believe that each of the Subject Accounts contains evidence of the Subject Offenses, including ongoing efforts to obstruct justice, tamper with witnesses, and make false statements.

8. For example, as set forth in more detail below, in recent months STONE has reached out to communicate with multiple witnesses he knew or had reason to believe were scheduled to testify before Congress about interactions with STONE during the 2016 presidential campaign or were scheduled to meet with the Special Counsel’s Office and/or appear before the Grand Jury investigating such interactions. After STONE learned that one witness, Randy CREDICO, was prepared to contradict STONE’s congressional testimony, STONE repeatedly

urged CREDICO to assert the Fifth Amendment and decline to answer questions, and did so through multiple text messages. In June 2018, STONE instructed his private investigator to provide him with a full background investigation on another witness, [REDACTED] who had done information technology work for STONE during the campaign [REDACTED]

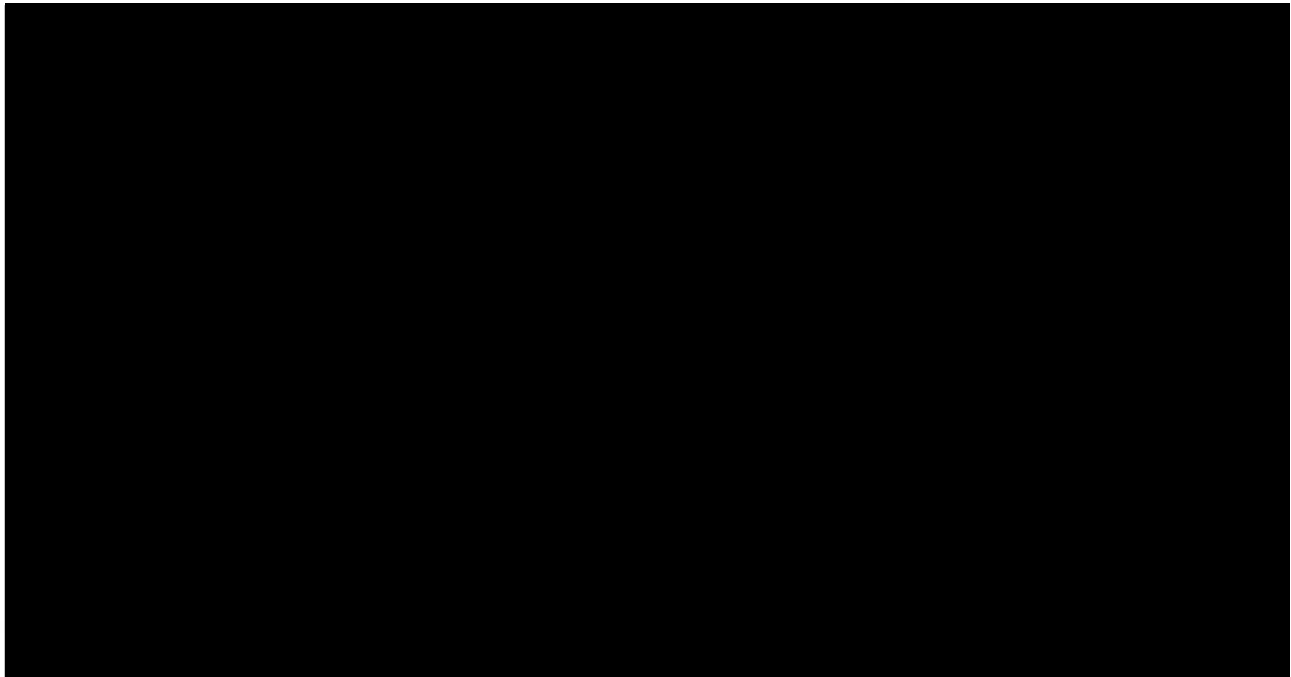
9. In September 2017, STONE released a statement he said he provided to Congress in which he denied having advance knowledge of “the source or actual content of the Wikileaks disclosures regarding Hillary Clinton.” He also stated publicly that when he tweeted during the campaign, on August 21, 2016, “it will soon the Podesta’s time in the barrel,” he was not referring to the hacking or publication of John Podesta’s emails, but rather to “Podesta’s business dealings with Russia.” Evidence obtained in the investigation, however, shows the following:

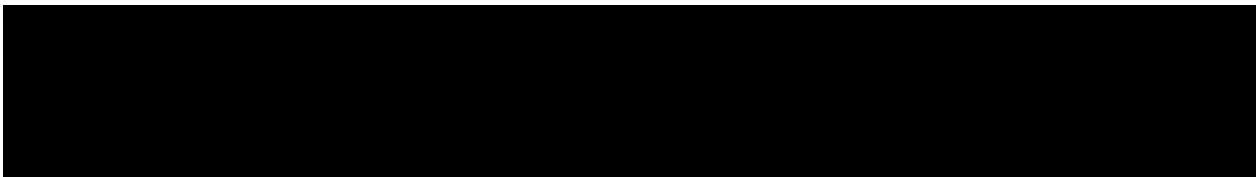
a. On or about July 25, 2016, Roger STONE emailed Jerome CORSI to “Get to Assange” at the Ecuadorian Embassy and “get pending WikiLeaks emails[.]” Julian ASSANGE is the founder of WikiLeaks. On or about July 31, 2016, STONE also instructed CORSI to have [REDACTED] contact ASSANGE. On or about August 2, 2016, CORSI responded to STONE that the “[w]ord is friend in embassy plans 2 more dumps. One shortly after I’m back. 2nd in Oct. Impact planned to be very damaging.... Time to let more than Podesta to be exposed as in bed w enemy if they are not ready to drop HRC.” After receipt of that message, on or about August 21, 2016, using @RogerJStoneJR, STONE tweeted: “Trust me, it will soon the Podesta’s time in the barrel. #CrookedHillary.”

b. Information disclosures subsequently occurred on or about the times CORSI predicted: On or about August 12, 2016, the day CORSI was scheduled to return to the United States (“shortly after I’m back”), Guccifer 2.0 released hacked information related to the

Democratic Congressional Campaign Committee (DCCC). On or about October 7, 2016, the day the Washington Post published a breaking story about an Access Hollywood videotape of then-candidate Trump making disparaging remarks about women, WikiLeaks released emails hacked from the account of John Podesta.

c. Furthermore, on the day of the Access Hollywood video disclosure, there were phone calls between STONE and CORSI after the Washington Post contacted STONE prior to publication. At approximately 11:00AM, the Washington Post received a tip regarding the Access Hollywood video. Approximately one hour later, shortly before noon, STONE received a call from the Washington Post. Approximately ninety minutes later, before 2:00PM, STONE called CORSI and they spoke. Approximately forty minutes later, CORSI called STONE and the two spoke again at length. At approximately 4:00PM, the Washington Post published its story regarding the Access Hollywood tape. By approximately 4:30PM, WikiLeaks tweeted out its first release of emails hacked from John Podesta.





PROBABLE CAUSE.

A. Background on Relevant Individuals

i. Roger STONE

10. 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

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





B. U.S. Intelligence Community Assessment of Russian Government-Backed Hacking Activity during the 2016 Presidential Election

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

a. The U.S. Intelligence Community (“USIC”) is confident that the Russian Government directed the recent compromises of emails from US persons and institutions, including from US political organizations. The recent disclosures of alleged hacked emails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts. These thefts and disclosures were

intended to interfere with the U.S. election process. Such activity is not new to Moscow—the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there. We believe, based on the scope and sensitivity of these efforts, that only Russia’s senior-most officials could have authorized these activities.

14. On January 6, 2017, theUSIC 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, theUSIC assessed the following:

a. “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.”

b. TheUSIC also described, at a high level, some of the techniques that the Russian government employed during its interference. TheUSIC 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.’”

c. With respect to “cyber activity,” theUSIC 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.” TheUSIC 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.” The GRU is the foreign military intelligence agency of the Russian Ministry of Defense, and is Russia’s largest foreign intelligence agency.

d. 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.”

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

C. Additional Hacking Activity by Individuals Associated with the GRU

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

16. 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.

17. 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 posted on DCLeaks.

18. 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.

19. On or about July 13, 2018, a grand jury in this District indicted eleven GRU officers for knowingly and intentionally conspiring to hack into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election, steal documents from those computers, and stage releases of stolen documents in order to interfere with the election. The victims of the hacking and releases included the DNC, the Democratic Congressional Campaign Committee (“DCCC”), and the chairman of the Clinton campaign (John Podesta). *See United States v. Viktor Borisovich Netyksho, et al.* (1:18-cr-215) (D.D.C.).¹

D. Roger STONE’s Public Interactions with Guccifer 2.0 and WikiLeaks

20. 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. 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.

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

¹ A twelfth defendant was charged with conspiring to infiltrate computers of organizations responsible for administering elections, including state boards of election, secretaries of state, and companies that supply software and other technology used to administer elections.

22. 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.”

23. On August 8, 2016, STONE addressed the Southwest Broward Republican Organization. During his speech, he was asked about a statement by 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.

24. 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.

25. 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.

26. 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.”

27. On August 18, 2016, Paul Manafort, STONE’s longtime friend and associate, resigned as Chairman of the Trump Campaign.

28. As noted above, 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.”

29. 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.”

30. On Saturday, October 1, 2016, using @RogerJStoneJr, STONE tweeted, “Wednesday @HillaryClinton is done. #WikiLeaks.”

31. On Sunday, October 2, 2016, MSNBC Morning Joe producer Jesse Rodriguez 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.”

32. 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.

33. 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.

34. 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.”

35. 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.”

E. STONE’s Private Twitter Direct Messages with WikiLeaks and ASSANGE

36. On August 7, 2017, Chief Judge Beryl A. Howell issued a search warrant for the Twitter account @RogerJStoneJr. Information recovered from the search of that account includes the following:

a. 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.”

b. 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.”

c. 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.”

d. 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."

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

f. 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."

F. STONE's Communications with STONE, [REDACTED] and Others Regarding Forthcoming Leaks

37. As indicated above, on September 11, 2017, Chief Judge Howell issued a search warrant for STONE's [REDACTED] address, [REDACTED] (**Target Account 1**); on October 17, 2017, Chief Judge Howell issued a search warrant for STONE's [REDACTED] address, [REDACTED] (**Target Account 2**); and on or about March 14, 2018, Chief Judge Howell issued a search warrant for STONE's iCloud account (**Target Account 3**). In addition, on or about December 19, 2017, Chief Judge Howell issued a search warrant for MALLOCH's email account. Information recovered pursuant to those search warrants includes the following:

a. 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 **Target Account 1**, who replied to CORSI that, "May meet Manafort -guarantee nothing."

b. On or about May 18, 2016, CORSI emailed STONE at **Target Account 1** 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."

c. On July 25, 2016, STONE, using **Target Account 1**, 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.”

d. On or about July 31, 2016, STONE, using **Target Account 1**, 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.”

e. As noted above, on or about August 2, 2016 (approximately 19 days before STONE publicly tweeted about “Podesta’s time in the barrel”), CORSI emailed STONE at **Target Account 1**: “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.

f. On or about August 5, 2016, [REDACTED] an associate of STONE’s, emailed Stone at **Target Account 1**. 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

g. On or about August 15, 2016, CORSI emailed STONE at **Target Account 1**: “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.”

h. On or about August 31, 2016, CORSI emailed STONE at **Target Account 1**: “Did you get the PODESTA writeup.” STONE replied “[y]es.”

i. On or about August 31, 2016, CORSI messaged STONE at **Target Account 3**, “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.”

j. On or about September 6, 2016, CORSI emailed STONE at **Target Account 1**: “Roger[,] Is NY Post going to use the Pedesta [sic] stuff?”

k. 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,

[REDACTED]

“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.

l. On or about October 3, 2016, an associate of STONE emailed STONE at **Target Account 2** and asked: “Assange – what’s he got? Hope it’s good.” STONE wrote back, “It is. I’d tell Bannon but he doesn’t call me back. My book on the TRUMP campaign will be out in Jan. Many scores will be settled.” The associate forwarded the email to Steve BANNON, 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.”

m. 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.

n. On or about October 4, 2016, CORSI messaged STONE at **Target Account 3**, “Assange made a fool of himself. Has nothing or he would have released it. Total BS hype.”

o. That same day, BANNON emailed STONE at **Target Account 2**, “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.”

p. 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.

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

38. 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.”

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

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

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

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

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

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

44. 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 on **Target Account 1**, "I expect that much of next dump focus, setting stage for Foundation debacle."

45. 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 **Target Account 2**, forwarded [REDACTED] message to CORSI without comment. STONE does not appear to have forwarded the email to any other individual.

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

46. On or about October 8, 2016, STONE, using **Target Account 3**, 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.”

47. On or about Wednesday, October 12, 2016, at approximately 8:17AM, STONE, using **Target Account 2**, emailed Corsi asking him to “send me your best podesta links.” STONE emailed CORSI at approximately 8:44AM, “need your BEST podesta pieces.” CORSI wrote back at approximately 8:54AM, “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?”

48. On or about that same day, October 12, 2016, Podesta accused STONE of having advance knowledge of the publication of his emails, as noted above. At approximately 3:25PM, CORSI emailed STONE at both **Target Account 1** and **2** with 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.”

49. 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 **Target Account 1**: “Got them and used them.”

50. On or about Thursday, October 13, 2016, CORSI emailed STONE at **Target Account 2**: “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

██████████ skimmed maybe billions off Skolkovo — Skolkovo kept their money with Metcombank[.] The Russians launched a criminal investigation[.] [web link] Once ██████████ 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[.]"

51. On or about Thursday, October 13, 2016, at approximately 6:30PM, CORSI sent STONE an email at **Target Account 2**, 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 ██████████ 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 ██████████ 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?"

52. On or about October 14, 2016, CORSI sent a message to STONE at **Target Account 3**, "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."

53. On or about October 17, 2016, CORSI messaged STONE at **Target Account 3**, “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.”

54. On or about October 17, 2016, CORSI emailed STONE at **Target Accounts 1 and 2** 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.”

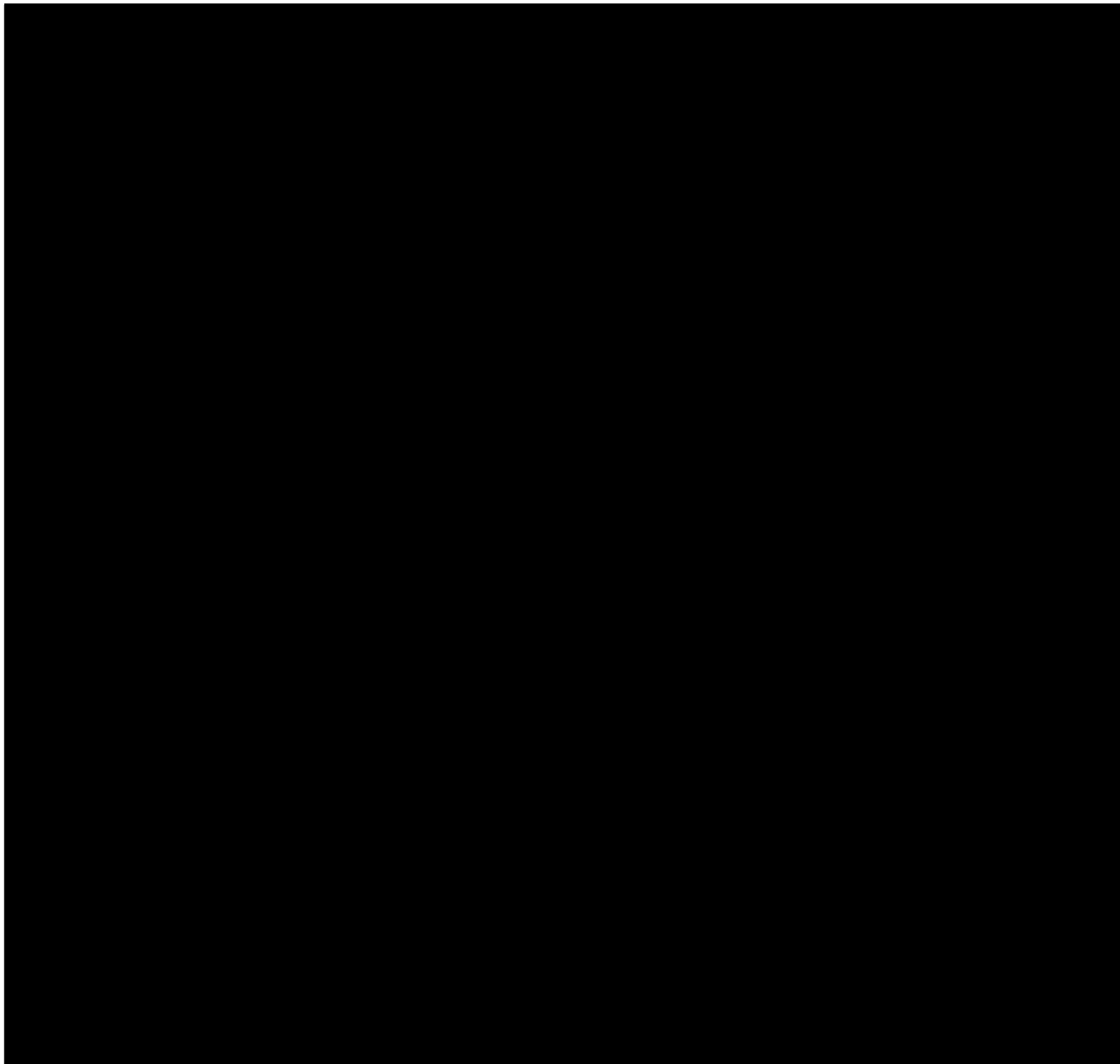
55. On or about October 18, 2016, CORSI messaged STONE at **Target Account 3**, “Pls call. Important.”

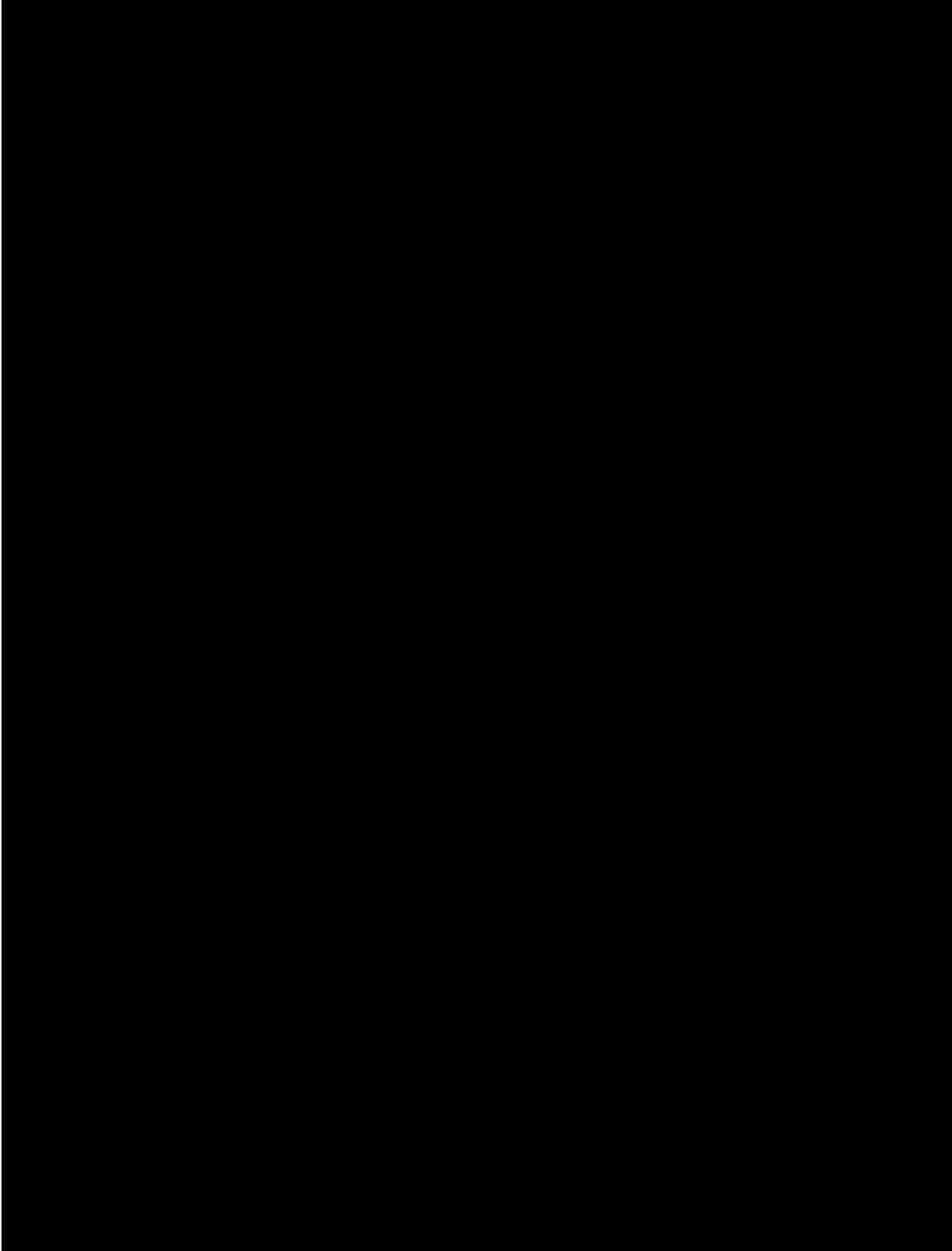
56. On or about October 19, 2016, STONE published an article on Breitbart.com in which he claimed he had “no advance notice of Wikileaks’ hacking of Podesta’s e-mails.” STONE stated, “I predicted that Podesta’s business dealings would be exposed. I didn’t hear it from Wikileaks, although Julian Assange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

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

58. On or about November 9, 2016, CORSI messaged STONE at **Target Account 3**, “Congratulations, Roger. He could not have done it without you.”

59. On or about November 10, 2016, CORSI messaged STONE at **Target Account 3**, “Are you available to talk on phone?” Several minutes later, CORSI messaged, “I’m in London. Have some interesting news for you.”





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

61. 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.

62. 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.

63. 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.”

K. STONE’s Use of Target Account 3 to Message Randy CREDICO about STONE’s “Back channel”

64. On November 19, 2017, Randy CREDICO (who, as described further below, STONE publicly identified as his “intermediary” to ASSANGE), messaged STONE on **Target Account 3**, “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.”

65. On or about November 21, 2017, CREDICO messaged STONE on **Target Account 3**, “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?”

66. On or about November 24, 2017, STONE, using **Target Account 3**, 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 witchhunt [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[.]”

67. STONE and CREDICO continued to exchange messages via **Target Account 3**, and on November 24, 2017, CREDICO wrote to STONE, “Forensic evidence proves that there is no back Channel. So now you can relax.”

68. 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.

69. 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.”

70. On or about December 1, 2017, CREDICO messaged STONE on **Target Account 3**, stating, “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

⁴ Contrary to his statement, CREDICO has not provided any forensic evidence to the FBI.

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 trump [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[.]"

71. 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."

72. 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.

73. STONE and CREDICO continued to exchange messages via **Target Account 3**, 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."

74. On or about January 8, 2018, CREDICO messaged STONE on **Target Account 3** stating: “Embassy logs . . . + 17 other pieces of information prove that I did not have any conversations with Assange until September of last year.”

75. CREDICO and STONE continued to message each other, and on or about January 25, 2018, CREDICO wrote to STONE on **Target Account 3**: “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[.]”

76. 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

77. 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.

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/>

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.

L. STONE’s Use of the Target Accounts to Communicate with Individuals Related to the Investigation

78. On May 17, 2018, Chief Judge Howell issued an order for the use of pen-trap devices on **Target Account 1** and **Target Account 2**. The information obtained from that order, along with information obtained from toll records, revealed that STONE has continued to use **Target Account 1** and **Target Account 2**, and that he has used them to communicate with individuals related to the investigation.

79. For example, STONE and [REDACTED] communicated twice on May 28 and May 29, 2018 using **Target Account 1**. [REDACTED], a former associate of STONE’s, was interviewed by the Special Counsel’s Office on or about May 2, 2018. Toll records show that [REDACTED] and STONE communicated multiple times on May 5, 2018, and STONE communicated with [REDACTED] using **Target Account 1** on June 1, 2018 and June 6, 2018. [REDACTED] a private investigator who had previously worked with STONE and who was hired by STONE to research individuals associated with this case (as described further below), communicated with STONE on **Target Account 1** at least four times between May 27, 2018 and July 12, 2018.

80. STONE has also used **Target Account 2** to communicate with individuals associated with this investigation.

a. For example, between May 23, 2018 and the present, STONE and CORSI exchanged at least five messages using **Target Account 2**. In the same time period, STONE exchanged at least 75 emails with CREDICO using **Target Account 2**.

b. Also in this same time period, STONE emailed [REDACTED] at least ten times using **Target Account 2**. [REDACTED] is a former employee of STONE. On May 9, 2018, FBI agents approached [REDACTED] and [REDACTED]. That day, and again on May 10, 2018, [REDACTED] communicated by phone with STONE. Overall, between May 23, 2018 and the present, STONE exchanged over 100 emails with [REDACTED] using **Target Account 2**. In addition, between on or about June 14, 2018 and June 17, 2018, [REDACTED] and STONE exchanged five emails using **Target Account 2**. [REDACTED]

81. STONE has also used a phone number associated with **Target Account 3** to communicate with [REDACTED] a private investigator hired by STONE. [REDACTED] was interviewed by investigators on June 7, 2018, and subsequently informed investigators that in June 2018, STONE instructed him to conduct a full background investigation on [REDACTED] who had been employed by STONE during the Campaign as an information technology specialist. [REDACTED] also told investigators that in June 2018, STONE instructed him to find an address for CREDICO that could be used to serve CREDICO with legal process. [REDACTED] told investigators that his primary form of communication with STONE is by text message on **Target Account 3**.

BACKGROUND CONCERNING EMAIL

82. In my training and experience, I have learned the Providers provide a variety of on-line services, including electronic mail (“email”) to the public. The Providers allow

subscribers to obtain email accounts at the domain names identified in the email address contained in Attachment A and C. Subscribers obtain an account by registering with the Providers. During the registration process, the Providers ask subscribers to provide basic personal information. Therefore, the computers of the Providers are likely to contain stored electronic communications (including retrieved and unretrieved email) for their subscribers and information concerning subscribers and their use of 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.

83. 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.

84. 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 Providers' 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.

85. In my training and experience, in some cases, email account users will communicate directly with an email service Providers 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 Providers' support services, as well as records of any actions taken by the Providers 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.

86. 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 Providers 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).

87. In my training and experience, information such as search history can help to show the state of mind of an individual at the time the search was made, as well as the individuals potential advance knowledge of events, as they search to see if the anticipated event has occurred.

INFORMATION REGARDING APPLE ID AND iCloud⁷

⁷ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; "Create and start using an Apple ID," available at <https://support.apple.com/en-us/HT203993>; "iCloud," available at <http://www.apple.com/icloud/>; "What does iCloud back up?," available at <https://support.apple.com/kb/PH12519>; "iOS Security," available at

88. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

89. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user

https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

90. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

91. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

92. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in 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 and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

93. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

94. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

95. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

96. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish 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.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

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

CONCLUSION

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

99. 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

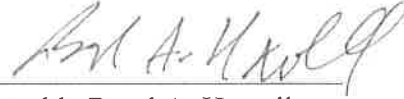
100. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation, the full nature and extent of which is not known to all of the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

Respectfully submitted,



Andrew Mitchell
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on this 3rd day of August, 2018.

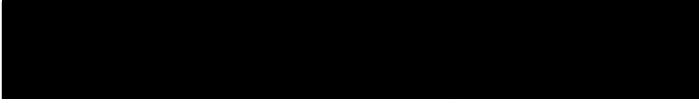


The Honorable Beryl A. Howell
Chief United States District Judge

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with the email address:



created or maintained between September 11, 2017 and present, 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

Particular Things to be Seized

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

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

- a. The contents of all e-mails, attachments and chat messages stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination e-mails sent addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All existing printouts from original storage of all of the electronic mail described above in Section I.A. above;
- c. All internet search data including all queries and location data;
- d. All transactional information of all activity of the account described above in Section I.A, including log files, dates, times, methods of connecting, ports, dial ups, and/or locations;
- e. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- f. Records or other information regarding the identification of the account described above in Section I.A, to include application, full name, physical address, telephone numbers and other identifiers, records of session times and durations, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, all screen names associated with subscribers and/or accounts, all account names associated with the subscriber,
- g. All records indicating the services available to subscribers of the electronic mail address described above in Section I.A.;

II. Information to be Seized by Law Enforcement Personnel

Any and all records that relate in any way to the accounts described in Attachment A which consists of evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 2 (aiding and abetting), 18 U.S.C. § 3 (accessory after the fact), 18 U.S.C. § 4 (misprision of a felony), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 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 contribution ban) from June 1, 2015 to present, including:

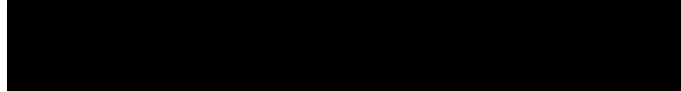
- a. All records, information, documents or tangible materials that relate in any way to communications regarding hacking, release of hacked material, communications with persons or entities associated with WikiLeaks, including but not limited to Julian Assange, or communications regarding disinformation, 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, or any individual associated with the Trump Campaign;
- c. All images, messages, communications, calendar entries, search terms, "address book" entries and contacts, including any and all preparatory steps taken in furtherance of the above-listed offenses;
- d. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier concerning the messages identified above, including records about their identities and whereabouts;
- e. Evidence of the times the account was used;
- f. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
- g. Passwords and encryption keys, and other access information that may be necessary to access the account and other associated accounts;
- h. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;

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

ATTACHMENT C

Property to be Searched

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



created or maintained between October 17, 2017 and the present, that is stored at premises owned, maintained, controlled, or operated by Google, Inc., a business with offices located at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT D

Particular Things to be Seized

I. Files and Accounts to be produced by Google, Inc.

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

- a. The contents of all e-mails, attachments and chat messages stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination e-mails sent addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All existing printouts from original storage of all of the electronic mail described above in Section I.A. above;
- c. All internet search data including all queries and location data;
- d. All transactional information of all activity of the account described above in Section I.A, including log files, dates, times, methods of connecting, ports, dial ups, and/or locations;
- e. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- f. All records or other information regarding the identification of the account described above in Section I.A, to include application, full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, all screen names associated with subscribers and/or accounts, all account names associated with the subscriber, methods of connecting, log files, means and source of payment (including any credit or bank account number), and detailed billing records;
- g. All records indicating the services available to subscribers of the electronic mail address described above in Section I.A.;
- h. Google+ subscriber information, circle information, including name of circle and members, contents of posts, comments, and photos, to include date and timestamp;

- i. Google Drive files created, accessed or owned by the account;
- j. YouTube subscriber information, private videos and files, private messages, and comments;
- k. Google+ Photos contents to include all images, videos and other files, and associated upload/download date and timestamp;
- l. Google Talk and Google Hangouts conversation logs associated with the account.

II. Information to be Seized by Law Enforcement Personnel

Any and all records that relate in any way to the accounts described in Attachment C 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 contribution ban), from June 1, 2015 to 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, or any individual associated with the Trump Campaign;
- c. All images, messages, communications, calendar entries, search terms, "address book" entries and contacts, including any and all preparatory steps taken in furtherance of the above-listed offenses;
- d. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier concerning the messages identified above, including records about their identities and whereabouts;
- e. Evidence of the times the account was used;
- f. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
- g. Passwords and encryption keys, and other access information that may be necessary to access the account and other associated accounts;
- h. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;
- i. All existing printouts from original storage which concern the categories identified in subsection II.a

ATTACHMENT E

Property to be Searched

This warrant applies to information associated with the following Apple DSID:



created or maintained between March 14, 2018 and the present, that is stored at premises owned, maintained, controlled, or operated by Apple, Inc., located at One Apple Park Way, Cupertino, California 95014.

ATTACHMENT F

Particular Things to be Seized

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

To the extent that the information described in Attachment E is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment E:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

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

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be Seized by Law Enforcement Personnel

Any and all records that relate in any way to the accounts described in Attachment A which consists of evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 2 (aiding and abetting), 18 U.S.C. § 3 (accessory after the fact), 18 U.S.C. § 4 (misprision of a felony), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 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 contribution ban), from June 1, 2015 to 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, or any individual associated with the Trump Campaign;
- c. All images, messages, communications, calendar entries, search terms, "address book" entries and contacts, including any and all preparatory steps taken in furtherance of the above-listed offenses;
- d. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier concerning the messages identified above, including records about their identities and whereabouts;
- e. Evidence of the times the account was used;
- f. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
- g. Passwords and encryption keys, and other access information that may be necessary to access the account and other associated accounts;
- h. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;
- i. All existing printouts from original storage which concern the categories identified in subsection II.a

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, GOOGLE, AND APPLE

Case: 1:18-sc-02583
Assigned To : Howell, Beryl A.
Assign. Date : 8/3/2018
Description: Search & Seizure Warrant

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

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

See Attachment C

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 D

YOU ARE COMMANDED to execute this warrant on or before August 15, 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: 8/3/2018 at 3:00 PM Beryl A. Howell
Judge's signature

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

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

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

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

Certification

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

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT C

Property to be Searched

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



created or maintained between October 17, 2017 and the present, that is stored at premises owned, maintained, controlled, or operated by Google, Inc., a business with offices located at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT D

Particular Things to be Seized

I. Files and Accounts to be produced by Google, Inc.

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

- a. The contents of all e-mails, attachments and chat messages stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination e-mails sent addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All existing printouts from original storage of all of the electronic mail described above in Section I.A. above;
- c. All internet search data including all queries and location data;
- d. All transactional information of all activity of the account described above in Section I.A, including log files, dates, times, methods of connecting, ports, dial ups, and/or locations;
- e. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- f. All records or other information regarding the identification of the account described above in Section I.A, to include application, full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, all screen names associated with subscribers and/or accounts, all account names associated with the subscriber, methods of connecting, log files, means and source of payment (including any credit or bank account number), and detailed billing records;
- g. All records indicating the services available to subscribers of the electronic mail address described above in Section I.A.;
- h. Google+ subscriber information, circle information, including name of circle and members, contents of posts, comments, and photos, to include date and timestamp;

- i. Google Drive files created, accessed or owned by the account;
- j. YouTube subscriber information, private videos and files, private messages, and comments;
- k. Google+ Photos contents to include all images, videos and other files, and associated upload/download date and timestamp;
- l. Google Talk and Google Hangouts conversation logs associated with the account.

II. Information to be Seized by Law Enforcement Personnel

Any and all records that relate in any way to the accounts described in Attachment C 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 contribution ban), from June 1, 2015 to 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, or any individual associated with the Trump Campaign;
- c. All images, messages, communications, calendar entries, search terms, "address book" entries and contacts, including any and all preparatory steps taken in furtherance of the above-listed offenses;
- d. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier concerning the messages identified above, including records about their identities and whereabouts;
- e. Evidence of the times the account was used;
- f. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
- g. Passwords and encryption keys, and other access information that may be necessary to access the account and other associated accounts;
- h. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;
- i. All existing printouts from original storage which concern the categories identified in subsection II.a

UNITED STATES DISTRICT COURT

for the
District of Columbia

FILED

AUG - 3 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, GOOGLE, AND APPLE

Case: 1:18-sc-02583
Assigned To : Howell, Beryl A.
Assign. Date : 8/3/2018
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 C

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

See Attachment D

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. §§ 1505, 1512, 1513 (Obstruction of justice, Witness tampering) and 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.

- [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)

Handwritten signature of Andrew Mitchell

Applicant's signature

Andrew Mitchell, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 8/3/2018

Handwritten signature of Beryl A. Howell

Judge's signature

City and state: Washington, D.C.

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

Printed name and title

FILED

AUG - 3 2018

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

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
THREE ACCOUNTS STORED AT
PREMISES CONTROLLED BY
MICROSOFT, GOOGLE, AND APPLE

Case: 1:18-sc-02583
Assigned To : Howell, Beryl A.
Assign. Date : 8/3/2018
Description: Search & Seizure Warrant

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

I, Andrew Mitchell, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the following:

a. The email account [REDACTED] (hereafter "**Target Account 1**"), that is stored at premises owned, maintained, controlled, or operated by Microsoft, Inc., a business with offices located at One Microsoft Way, Redmond, Washington, 98052. The information to be disclosed by Microsoft and searched by the government is described in the following paragraphs and in Attachments A and B.

b. The email account [REDACTED] (hereafter "**Target Account 2**"), that is stored at premises owned, maintained, controlled, or operated by Google, Inc., a business with offices located at 1600 Amphitheatre Parkway, Mountain View, California, 94043. The information to be disclosed by Google and searched by the government is described in the following paragraphs and in Attachments C and D.

c. The iCloud account [REDACTED] associated with the Apple email account [REDACTED] (hereafter "**Target Account 3**"), that is stored at premises owned,

maintained, controlled, or operated by Apple, Inc., a business with offices located at 1 Infinite Loop, Cupertino, California 95014. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachment E and F.

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

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other 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 Accounts** contain communications relevant to 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 contribution ban) (the “Subject Offenses”).

5. On September 11, 2017, Chief Judge Beryl A. Howell of the District of Columbia issued a search warrant for Roger STONE’s [REDACTED] address, [REDACTED] (**Target Account 1**). On October 17, 2017, Chief Judge Howell issued a search warrant for STONE’s [REDACTED] address, [REDACTED] (**Target Account 2**). On or about March 14, 2018, Chief Judge Howell issued a search warrant for STONE’s iCloud account (**Target Account 3**). This

warrant seeks to search those accounts from the date each respective warrant was issued to the present.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. *Id.* §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States (including a magistrate judge of such a court) . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). The offense conduct included activities in Washington, D.C., as detailed below, including in paragraphs 14, 19, and 61.

SUMMARY

7. This application seeks authority to search, from the date of search warrants previously issued by the Court to the present, three accounts believed to be used by Roger STONE: **Target Account 1**, which is STONE’s Hotmail account; **Target Account 2**, which is STONE’s Gmail account; and **Target Account 3**, which is STONE’s iCloud account. As set forth herein, there is probable cause to believe that each of the Subject Accounts contains evidence of the Subject Offenses, including ongoing efforts to obstruct justice, tamper with witnesses, and make false statements.

8. For example, as set forth in more detail below, in recent months STONE has reached out to communicate with multiple witnesses he knew or had reason to believe were scheduled to testify before Congress about interactions with STONE during the 2016 presidential campaign or were scheduled to meet with the Special Counsel’s Office [REDACTED]. [REDACTED]. After STONE learned that one witness, Randy CREDICO, was prepared to contradict STONE’s congressional testimony, STONE repeatedly

urged CREDICO to assert the Fifth Amendment and decline to answer questions, and did so through multiple text messages. In June 2018, STONE instructed his private investigator to provide him with a full background investigation on another witness, [REDACTED] who had done information technology work for STONE during the campaign and [REDACTED]

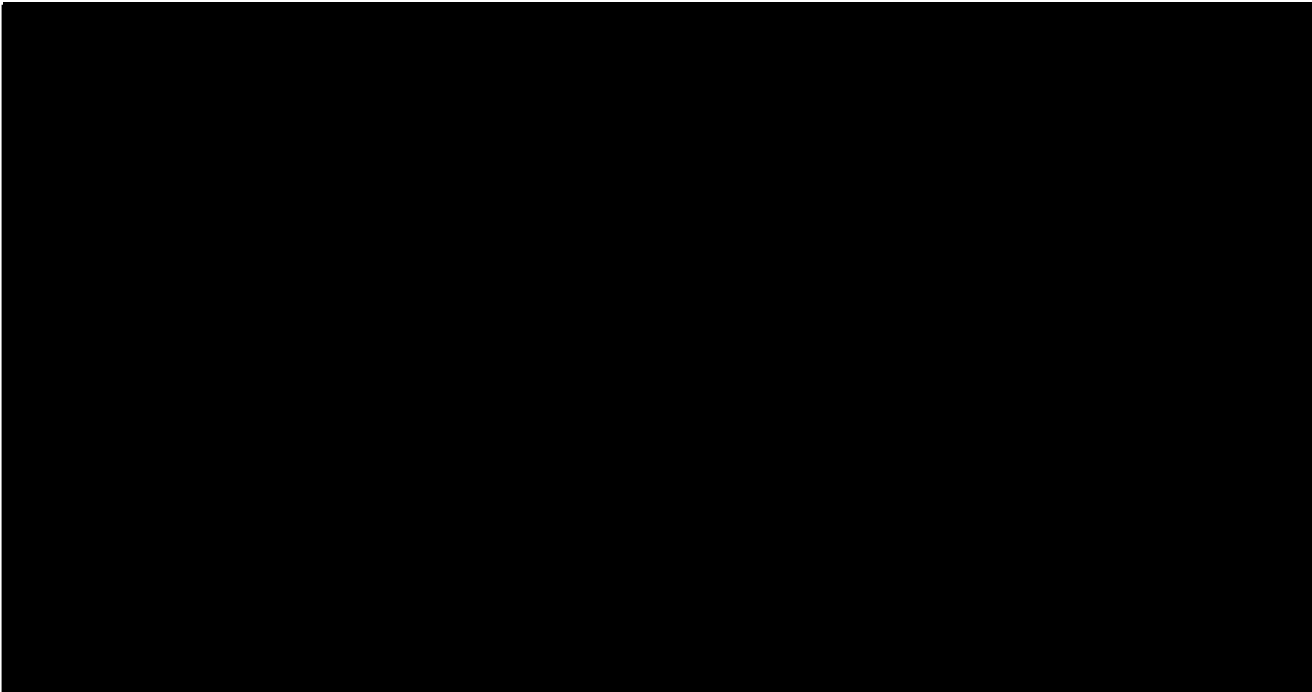
9. In September 2017, STONE released a statement he said he provided to Congress in which he denied having advance knowledge of “the source or actual content of the Wikileaks disclosures regarding Hillary Clinton.” He also stated publicly that when he tweeted during the campaign, on August 21, 2016, “it will soon the Podesta’s time in the barrel,” he was not referring to the hacking or publication of John Podesta’s emails, but rather to “Podesta’s business dealings with Russia.” Evidence obtained in the investigation, however, shows the following:

a. On or about July 25, 2016, Roger STONE emailed Jerome CORSI to “Get to Assange” at the Ecuadorian Embassy and “get pending WikiLeaks emails[.]” Julian ASSANGE is the founder of WikiLeaks. On or about July 31, 2016, STONE also instructed CORSI to have [REDACTED] contact ASSANGE. On or about August 2, 2016, CORSI responded to STONE that the “[w]ord is friend in embassy plans 2 more dumps. One shortly after I’m back. 2nd in Oct. Impact planned to be very damaging.... Time to let more than Podesta to be exposed as in bed w enemy if they are not ready to drop HRC.” After receipt of that message, on or about August 21, 2016, using @RogerJStoneJR, STONE tweeted: “Trust me, it will soon the Podesta’s time in the barrel. #CrookedHillary.”

b. Information disclosures subsequently occurred on or about the times CORSI predicted: On or about August 12, 2016, the day CORSI was scheduled to return to the United States (“shortly after I’m back”), Guccifer 2.0 released hacked information related to the

Democratic Congressional Campaign Committee (DCCC). On or about October 7, 2016, the day the Washington Post published a breaking story about an Access Hollywood videotape of then-candidate Trump making disparaging remarks about women, WikiLeaks released emails hacked from the account of John Podesta.

c. Furthermore, on the day of the Access Hollywood video disclosure, there were phone calls between STONE and CORSI after the Washington Post contacted STONE prior to publication. At approximately 11:00AM, the Washington Post received a tip regarding the Access Hollywood video. Approximately one hour later, shortly before noon, STONE received a call from the Washington Post. Approximately ninety minutes later, before 2:00PM, STONE called CORSI and they spoke. Approximately forty minutes later, CORSI called STONE and the two spoke again at length. At approximately 4:00PM, the Washington Post published its story regarding the Access Hollywood tape. By approximately 4:30PM, WikiLeaks tweeted out its first release of emails hacked from John Podesta.





PROBABLE CAUSE.

A. Background on Relevant Individuals

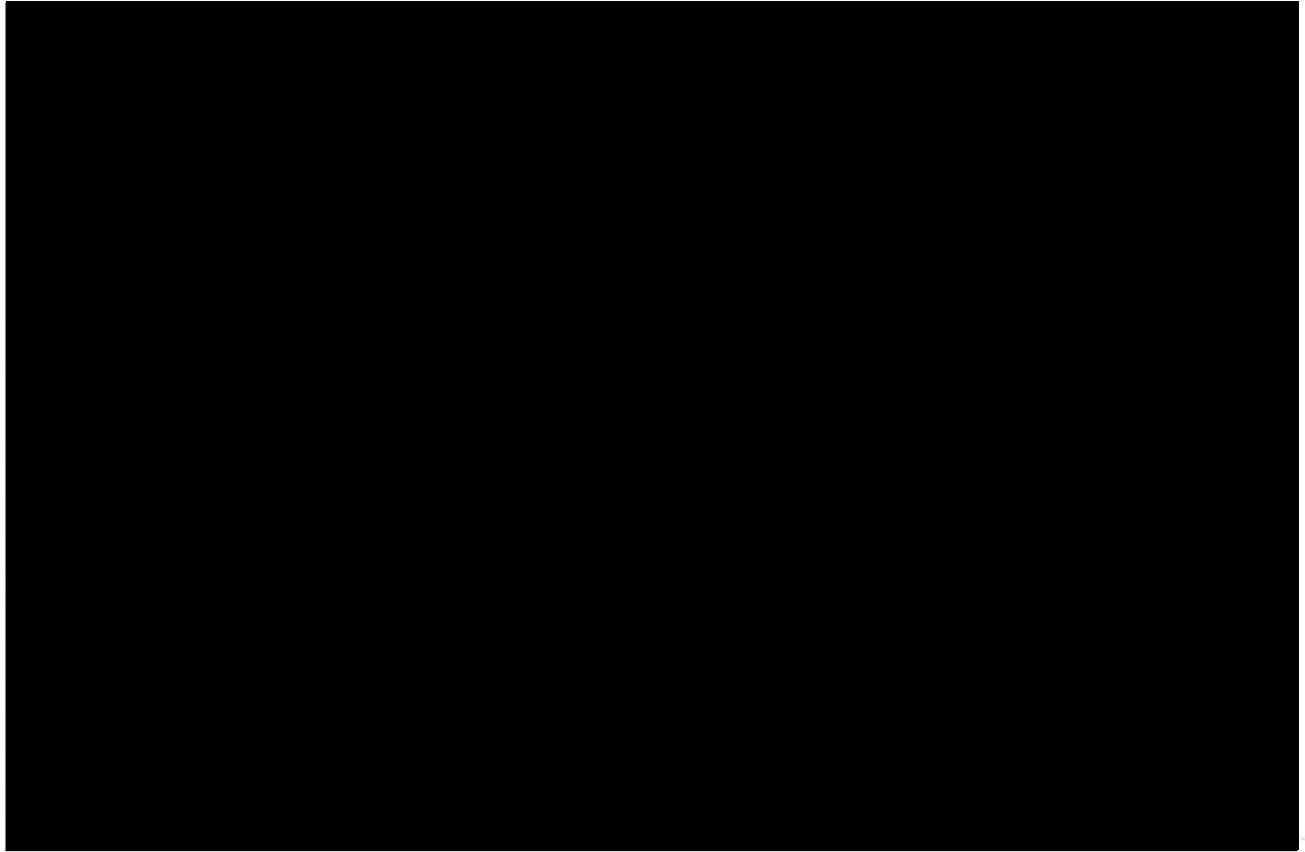
i. Roger STONE

10. 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

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





B. U.S. Intelligence Community Assessment of Russian Government-Backed Hacking Activity during the 2016 Presidential Election

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

a. The U.S. Intelligence Community (“USIC”) is confident that the Russian Government directed the recent compromises of emails from US persons and institutions, including from US political organizations. The recent disclosures of alleged hacked emails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts. These thefts and disclosures were

intended to interfere with the U.S. election process. Such activity is not new to Moscow—the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there. We believe, based on the scope and sensitivity of these efforts, that only Russia’s senior-most officials could have authorized these activities.

14. On January 6, 2017, theUSIC 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, theUSIC assessed the following:

a. “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.”

b. TheUSIC also described, at a high level, some of the techniques that the Russian government employed during its interference. TheUSIC 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.’”

c. With respect to “cyber activity,” theUSIC 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.” TheUSIC 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.” The GRU is the foreign military intelligence agency of the Russian Ministry of Defense, and is Russia’s largest foreign intelligence agency.

d. 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.”

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

C. Additional Hacking Activity by Individuals Associated with the GRU

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

16. 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.

17. 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 posted on DCLeaks.

18. 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.

19. On or about July 13, 2018, a grand jury in this District indicted eleven GRU officers for knowingly and intentionally conspiring to hack into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election, steal documents from those computers, and stage releases of stolen documents in order to interfere with the election. The victims of the hacking and releases included the DNC, the Democratic Congressional Campaign Committee (“DCCC”), and the chairman of the Clinton campaign (John Podesta). *See United States v. Viktor Borisovich Netyksho, et al.* (1:18-cr-215) (D.D.C.).¹

D. Roger STONE’s Public Interactions with Guccifer 2.0 and WikiLeaks

20. 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. 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.

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

¹ A twelfth defendant was charged with conspiring to infiltrate computers of organizations responsible for administering elections, including state boards of election, secretaries of state, and companies that supply software and other technology used to administer elections.

22. 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.”

23. On August 8, 2016, STONE addressed the Southwest Broward Republican Organization. During his speech, he was asked about a statement by 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.

24. 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.

25. 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.

26. 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.”

27. On August 18, 2016, Paul Manafort, STONE’s longtime friend and associate, resigned as Chairman of the Trump Campaign.

28. As noted above, 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.”

29. 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.”

30. On Saturday, October 1, 2016, using @RogerJStoneJr, STONE tweeted, “Wednesday @HillaryClinton is done. #WikiLeaks.”

31. On Sunday, October 2, 2016, MSNBC Morning Joe producer Jesse Rodriguez 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.”

32. 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.

33. 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.

34. 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.”

35. 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.”

E. STONE’s Private Twitter Direct Messages with WikiLeaks and ASSANGE

36. On August 7, 2017, Chief Judge Beryl A. Howell issued a search warrant for the Twitter account @RogerJStoneJr. Information recovered from the search of that account includes the following:

a. 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.”

b. 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.”

c. 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.”

d. 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."

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

f. 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."

F. STONE's Communications with STONE [REDACTED], and Others Regarding Forthcoming Leaks

37. As indicated above, on September 11, 2017, Chief Judge Howell issued a search warrant for STONE's [REDACTED] address, [REDACTED] (**Target Account 1**); on October 17, 2017, Chief Judge Howell issued a search warrant for STONE's [REDACTED] address, [REDACTED] (**Target Account 2**); and on or about March 14, 2018, Chief Judge Howell issued a search warrant for STONE's iCloud account (**Target Account 3**). In addition, on or about December 19, 2017, Chief Judge Howell issued a search warrant for [REDACTED] email account. Information recovered pursuant to those search warrants includes the following:

a. 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 **Target Account 1**, who replied to CORSI that, "May meet Manafort -guarantee nothing."

b. On or about May 18, 2016, CORSI emailed STONE at **Target Account 1** 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."

c. On July 25, 2016, STONE, using **Target Account 1**, 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.”

d. On or about July 31, 2016, STONE, using **Target Account 1**, 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.”

e. As noted above, on or about August 2, 2016 (approximately 19 days before STONE publicly tweeted about “Podesta’s time in the barrel”), CORSI emailed STONE at **Target Account 1**: “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.

f. On or about August 5, 2016, [REDACTED] an associate of STONE’s, emailed Stone at **Target Account 1**. 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

g. On or about August 15, 2016, CORSI emailed STONE at **Target Account 1**: “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.”

h. On or about August 31, 2016, CORSI emailed STONE at **Target Account 1**: “Did you get the PODESTA writeup.” STONE replied “[y]es.”

i. On or about August 31, 2016, CORSI messaged STONE at **Target Account 3**, “Podesta paid \$180k to invest in Uranium One – was hired by Rosatom in Giustra scandal. Podesta now under FBI investigation – tied to Ukraine Yanukovich – 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.”

j. On or about September 6, 2016, CORSI emailed STONE at **Target Account 1**: “Roger[,] Is NY Post going to use the Pedesta [sic] stuff?”

k. 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,

[REDACTED]

“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.

l. On or about October 3, 2016, an associate of STONE emailed STONE at **Target Account 2** and asked: “Assange – what’s he got? Hope it’s good.” STONE wrote back, “It is. I’d tell Bannon but he doesn’t call me back. My book on the TRUMP campaign will be out in Jan. Many scores will be settled.” The associate forwarded the email to Steve BANNON, 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.”

m. 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.

n. On or about October 4, 2016, CORSI messaged STONE at **Target Account 3**, “Assange made a fool of himself. Has nothing or he would have released it. Total BS hype.”

o. That same day, BANNON emailed STONE at **Target Account 2**, “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.”

p. 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.

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

38. 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.”

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

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

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

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

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

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

44. 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 on **Target Account 1**, "I expect that much of next dump focus, setting stage for Foundation debacle."

45. 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 **Target Account 2**, forwarded [REDACTED] message to CORSI without comment. STONE does not appear to have forwarded the email to any other individual.

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

46. On or about October 8, 2016, STONE, using **Target Account 3**, 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.”

47. On or about Wednesday, October 12, 2016, at approximately 8:17AM, STONE, using **Target Account 2**, emailed Corsi asking him to “send me your best podesta links.” STONE emailed CORSI at approximately 8:44AM, “need your BEST podesta pieces.” CORSI wrote back at approximately 8:54AM, “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?”

48. On or about that same day, October 12, 2016, Podesta accused STONE of having advance knowledge of the publication of his emails, as noted above. At approximately 3:25PM, CORSI emailed STONE at both **Target Account 1** and **2** with 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.”

49. 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 **Target Account 1**: “Got them and used them.”

50. On or about Thursday, October 13, 2016, CORSI emailed STONE at **Target Account 2**: “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

██████████ skimmed maybe billions off Skolkovo — Skolkovo kept their money with Metcombank[.] The Russians launched a criminal investigation[.] [web link] Once ██████████ 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[.]"

51. On or about Thursday, October 13, 2016, at approximately 6:30PM, CORSI sent STONE an email at **Target Account 2**, 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 ██████████, 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 ██████████, 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?"

52. On or about October 14, 2016, CORSI sent a message to STONE at **Target Account 3**, "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."

53. On or about October 17, 2016, CORSI messaged STONE at **Target Account 3**, “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.”

54. On or about October 17, 2016, CORSI emailed STONE at **Target Accounts 1 and 2** 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.”

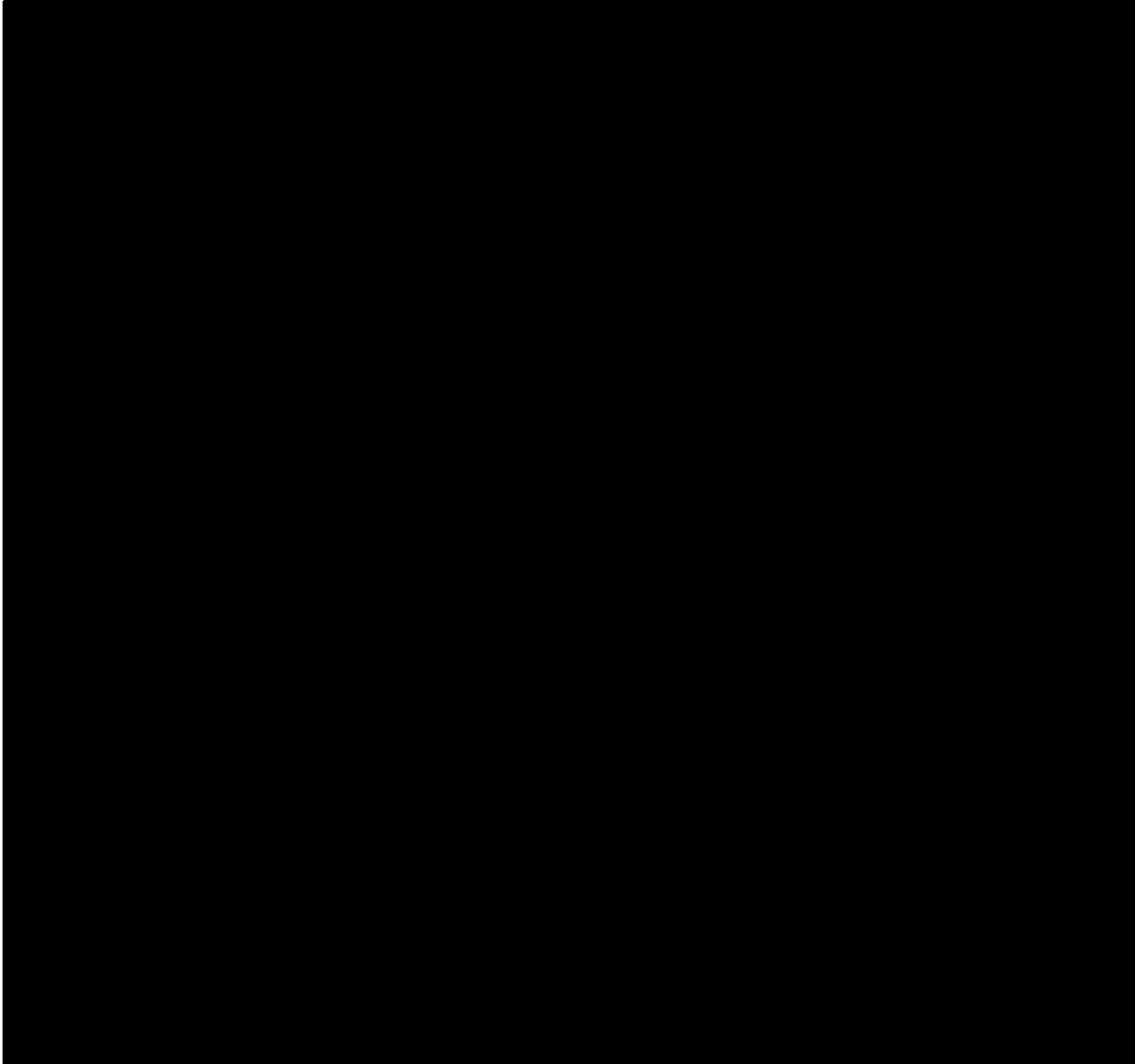
55. On or about October 18, 2016, CORSI messaged STONE at **Target Account 3**, “Pls call. Important.”

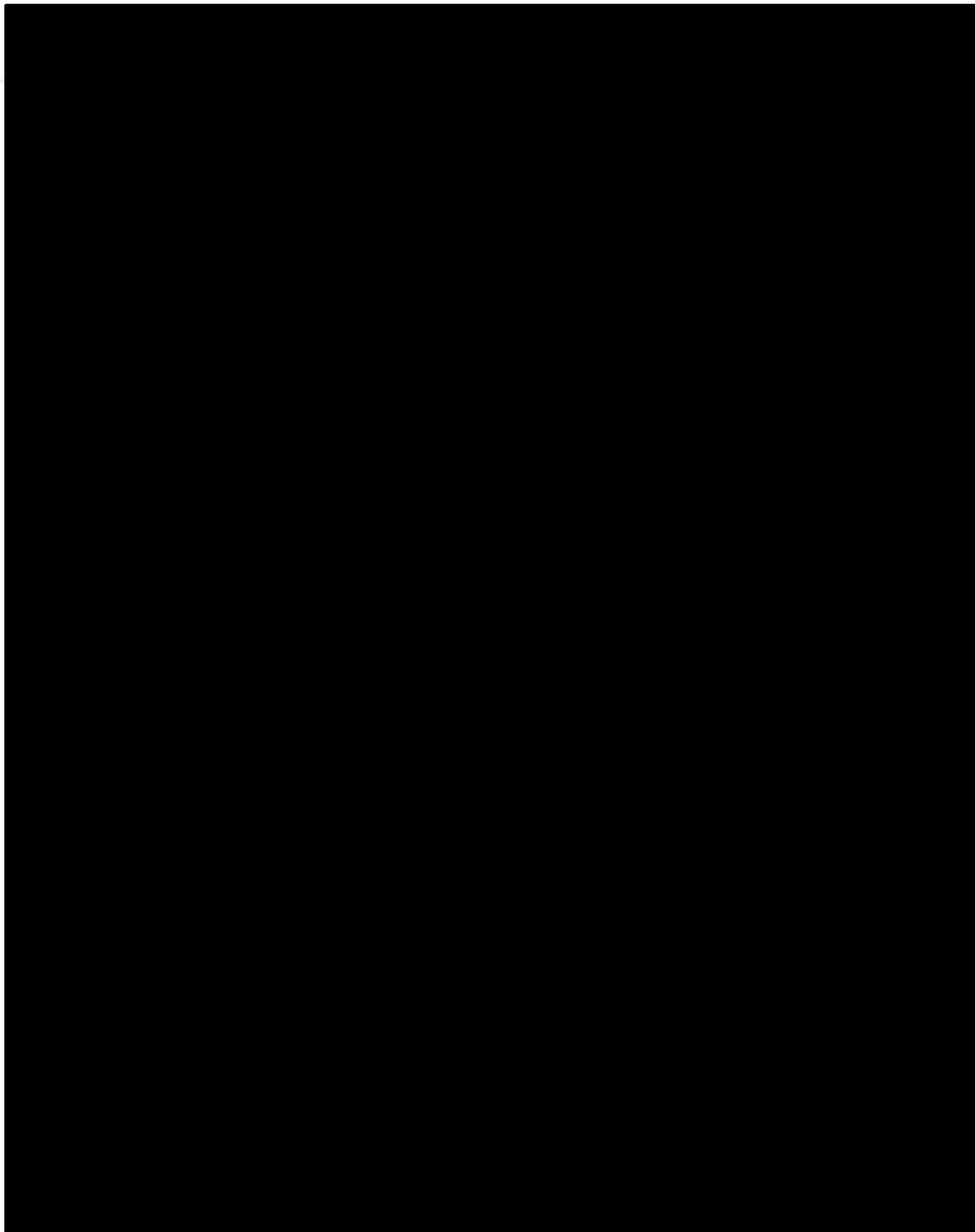
56. On or about October 19, 2016, STONE published an article on Breitbart.com in which he claimed he had “no advance notice of Wikileaks’ hacking of Podesta’s e-mails.” STONE stated, “I predicted that Podesta’s business dealings would be exposed. I didn’t hear it from Wikileaks, although Julian Assange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

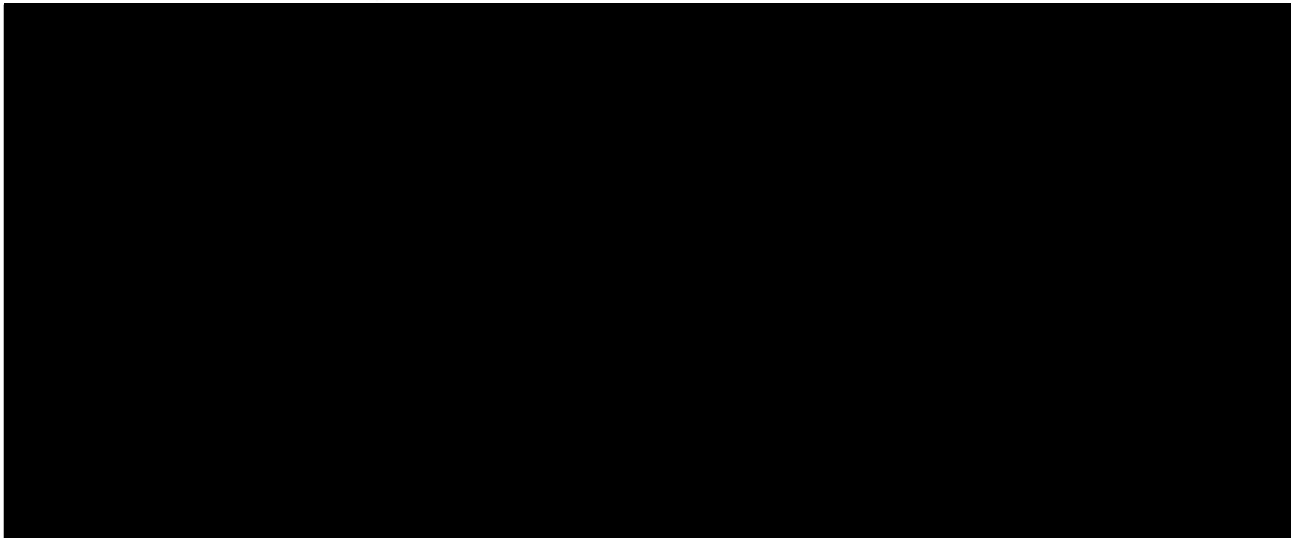
57. On or about November 8, 2016, the United States presidential election took place.

58. On or about November 9, 2016, CORSI messaged STONE at **Target Account 3**, “Congratulations, Roger. He could not have done it without you.”

59. On or about November 10, 2016, CORSI messaged STONE at **Target Account 3**, “Are you available to talk on phone?” Several minutes later, CORSI messaged, “I’m in London. Have some interesting news for you.”







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

61. 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.

62. 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.

63. 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.”

K. STONE’s Use of Target Account 3 to Message Randy CREDICO about STONE’s “Back channel”

64. On November 19, 2017, Randy CREDICO (who, as described further below, STONE publicly identified as his “intermediary” to ASSANGE), messaged STONE on **Target Account 3**, “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.”

65. On or about November 21, 2017, CREDICO messaged STONE on **Target Account 3**, “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??”

66. On or about November 24, 2017, STONE, using **Target Account 3**, 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 witchhunt [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[.]”

67. STONE and CREDICO continued to exchange messages via **Target Account 3**, and on November 24, 2017, CREDICO wrote to STONE, “Forensic evidence proves that there is no back Channel. So now you can relax.”

68. 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.

69. 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.”

70. On or about December 1, 2017, CREDICO messaged STONE on **Target Account 3**, stating, “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

⁴ Contrary to his statement, CREDICO has not provided any forensic evidence to the FBI.

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 trump [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[.]"

71. 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."

72. 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.

73. STONE and CREDICO continued to exchange messages via **Target Account 3**, 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."

74. On or about January 8, 2018, CREDICO messaged STONE on **Target Account 3** stating: “Embassy logs . . . + 17 other pieces of information prove that I did not have any conversations with Assange until September of last year.”

75. CREDICO and STONE continued to message each other, and on or about January 25, 2018, CREDICO wrote to STONE on **Target Account 3**: “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[.]”

76. 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

77. 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.

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/>

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.

L. STONE’s Use of the Target Accounts to Communicate with Individuals Related to the Investigation

78. On May 17, 2018, Chief Judge Howell issued an order for the use of pen-trap devices on **Target Account 1** and **Target Account 2**. The information obtained from that order, along with information obtained from toll records, revealed that STONE has continued to use **Target Account 1** and **Target Account 2**, and that he has used them to communicate with individuals related to the investigation.

79. For example, STONE and [REDACTED] communicated twice on May 28 and May 29, 2018 using **Target Account 1**. [REDACTED], a former associate of STONE’s, was interviewed by the Special Counsel’s Office on or about May 2, 2018. Toll records show that

[REDACTED] and STONE communicated multiple times on May 5, 2018, and STONE communicated with [REDACTED] using **Target Account 1** on June 1, 2018 and June 6, 2018. [REDACTED] a private investigator who had previously worked with STONE and who was hired by STONE to research individuals associated with this case (as described further below), communicated with STONE on **Target Account 1** at least four times between May 27, 2018 and July 12, 2018.

80. STONE has also used **Target Account 2** to communicate with individuals associated with this investigation.

a. For example, between May 23, 2018 and the present, STONE and CORSI exchanged at least five messages using **Target Account 2**. In the same time period, STONE exchanged at least 75 emails with CREDICO using **Target Account 2**.

b. Also in this same time period, STONE emailed [REDACTED] at least ten times using **Target Account 2**. [REDACTED] is a former employee of STONE. On May 9, 2018, FBI agents approached [REDACTED] and [REDACTED]. That day, and again on May 10, 2018, [REDACTED] communicated by phone with STONE. Overall, between May 23, 2018 and the present, STONE exchanged over 100 emails with [REDACTED] using **Target Account 2**. In addition, between on or about June 14, 2018 and June 17, 2018, [REDACTED] and STONE exchanged five emails using **Target Account 2**. [REDACTED]

81. STONE has also used a phone number associated with **Target Account 3** to communicate with [REDACTED], a private investigator hired by STONE. [REDACTED] was interviewed by investigators on June 7, 2018, and subsequently informed investigators that in June 2018, STONE instructed him to conduct a full background investigation on [REDACTED] who had been employed by STONE during the Campaign as an information technology specialist. [REDACTED]

[REDACTED] also told investigators that in June 2018, STONE instructed him to find an address for CREDICO that could be used to serve CREDICO with legal process.

[REDACTED] told investigators that his primary form of communication with STONE is by text message on **Target Account 3**.

BACKGROUND CONCERNING EMAIL

82. In my training and experience, I have learned the Providers provide a variety of on-line services, including electronic mail ("email") to the public. The Providers allow

subscribers to obtain email accounts at the domain names identified in the email address contained in Attachment A and C. Subscribers obtain an account by registering with the Providers. During the registration process, the Providers ask subscribers to provide basic personal information. Therefore, the computers of the Providers are likely to contain stored electronic communications (including retrieved and unretrieved email) for their subscribers and information concerning subscribers and their use of 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.

83. 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.

84. 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 Providers' 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.

85. In my training and experience, in some cases, email account users will communicate directly with an email service Providers 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 Providers' support services, as well as records of any actions taken by the Providers 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.

86. 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 Providers 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).

87. In my training and experience, information such as search history can help to show the state of mind of an individual at the time the search was made, as well as the individuals potential advance knowledge of events, as they search to see if the anticipated event has occurred.

INFORMATION REGARDING APPLE ID AND iCloud⁷

⁷ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; "Create and start using an Apple ID," available at <https://support.apple.com/en-us/HT203993>; "iCloud," available at <http://www.apple.com/icloud/>; "What does iCloud back up?," available at <https://support.apple.com/kb/PH12519>; "iOS Security," available at

88. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

89. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user

https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

90. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

91. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

92. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in 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 and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

93. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

94. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

95. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

96. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish 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.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

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

CONCLUSION

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

99. 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

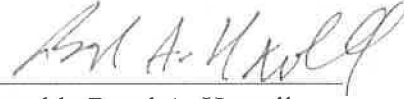
100. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation, the full nature and extent of which is not known to all of the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

Respectfully submitted,



Andrew Mitchell
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on this 31st day of August, 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 email address:



created or maintained between September 11, 2017 and present, 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

Particular Things to be Seized

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

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

- a. The contents of all e-mails, attachments and chat messages stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination e-mails sent addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All existing printouts from original storage of all of the electronic mail described above in Section I.A. above;
- c. All internet search data including all queries and location data;
- d. All transactional information of all activity of the account described above in Section I.A., including log files, dates, times, methods of connecting, ports, dial ups, and/or locations;
- e. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- f. Records or other information regarding the identification of the account described above in Section I.A, to include application, full name, physical address, telephone numbers and other identifiers, records of session times and durations, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, all screen names associated with subscribers and/or accounts, all account names associated with the subscriber,
- g. All records indicating the services available to subscribers of the electronic mail address described above in Section I.A.;

II. Information to be Seized by Law Enforcement Personnel

Any and all records that relate in any way to the accounts described in Attachment A which consists of evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 2 (aiding and abetting), 18 U.S.C. § 3 (accessory after the fact), 18 U.S.C. § 4 (misprision of a felony), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 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 contribution ban) from June 1, 2015 to 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, or any individual associated with the Trump Campaign;
- c. All images, messages, communications, calendar entries, search terms, "address book" entries and contacts, including any and all preparatory steps taken in furtherance of the above-listed offenses;
- d. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier concerning the messages identified above, including records about their identities and whereabouts;
- e. Evidence of the times the account was used;
- f. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
- g. Passwords and encryption keys, and other access information that may be necessary to access the account and other associated accounts;
- h. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;

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

ATTACHMENT C

Property to be Searched

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



created or maintained between October 17, 2017 and the present, that is stored at premises owned, maintained, controlled, or operated by Google, Inc., a business with offices located at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT D

Particular Things to be Seized

I. Files and Accounts to be produced by Google, Inc.

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

- a. The contents of all e-mails, attachments and chat messages stored in the account, including copies of e-mails sent to and from the account, draft e-mails, the source and destination e-mails sent addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All existing printouts from original storage of all of the electronic mail described above in Section I.A. above;
- c. All internet search data including all queries and location data;
- d. All transactional information of all activity of the account described above in Section I.A, including log files, dates, times, methods of connecting, ports, dial ups, and/or locations;
- e. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- f. All records or other information regarding the identification of the account described above in Section I.A, to include application, full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, all screen names associated with subscribers and/or accounts, all account names associated with the subscriber, methods of connecting, log files, means and source of payment (including any credit or bank account number), and detailed billing records;
- g. All records indicating the services available to subscribers of the electronic mail address described above in Section I.A.;
- h. Google+ subscriber information, circle information, including name of circle and members, contents of posts, comments, and photos, to include date and timestamp;

- i. Google Drive files created, accessed or owned by the account;
- j. YouTube subscriber information, private videos and files, private messages, and comments;
- k. Google+ Photos contents to include all images, videos and other files, and associated upload/download date and timestamp;
- l. Google Talk and Google Hangouts conversation logs associated with the account.

II. Information to be Seized by Law Enforcement Personnel

Any and all records that relate in any way to the accounts described in Attachment C 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 contribution ban), from June 1, 2015 to 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, or any individual associated with the Trump Campaign;
- c. All images, messages, communications, calendar entries, search terms, "address book" entries and contacts, including any and all preparatory steps taken in furtherance of the above-listed offenses;
- d. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier concerning the messages identified above, including records about their identities and whereabouts;
- e. Evidence of the times the account was used;
- f. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
- g. Passwords and encryption keys, and other access information that may be necessary to access the account and other associated accounts;
- h. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;
- i. All existing printouts from original storage which concern the categories identified in subsection II.a

ATTACHMENT E

Property to be Searched

This warrant applies to information associated with the following Apple DSID:



created or maintained between March 14, 2018 and the present, that is stored at premises owned, maintained, controlled, or operated by Apple, Inc., located at One Apple Park Way, Cupertino, California 95014.

ATTACHMENT F

Particular Things to be Seized

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

To the extent that the information described in Attachment E is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment E:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

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

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be Seized by Law Enforcement Personnel

Any and all records that relate in any way to the accounts described in Attachment A which consists of evidence, fruits, or instrumentalities of violations of 18 U.S.C. § 2 (aiding and abetting), 18 U.S.C. § 3 (accessory after the fact), 18 U.S.C. § 4 (misprision of a felony), 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 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 contribution ban), from June 1, 2015 to 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, or any individual associated with the Trump Campaign;
- c. All images, messages, communications, calendar entries, search terms, "address book" entries and contacts, including any and all preparatory steps taken in furtherance of the above-listed offenses;
- d. Communication, information, documentation and records relating to who created, used, or communicated with the account or identifier concerning the messages identified above, including records about their identities and whereabouts;
- e. Evidence of the times the account was used;
- f. All images, messages and communications regarding wiping software, encryption or other methods to avoid detection by law enforcement;
- g. Passwords and encryption keys, and other access information that may be necessary to access the account and other associated accounts;
- h. Credit card and other financial information, including but not limited to, bills and payment records evidencing ownership of the subject account;
- i. All existing printouts from original storage which concern the categories identified in subsection II.a