

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)*

SAMSUNG GALAXY S5
[REDACTED]

) Case No. 1:17-mj-793
) Assigned to: Chief Judge Beryl A. Howell
) Date Assigned: 10/27/2017
) Description: Search and 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 _____ District of _____ Columbia
(identify the person or describe the property to be searched and give its location):

See Attachment A incorporated herein.

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 incorporated herein.

YOU ARE COMMANDED to execute this warrant on or before _____ *(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 _____ **Beryl A. Howell, Chief 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)*

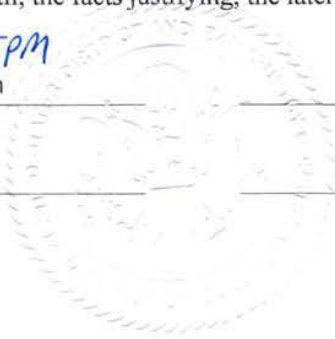
for 30 days *(not to exceed 30)* until, the facts justifying, the later specific date of _____

Date and time issued: 10/27/2017 ^{3:35 PM} ~~6:00 am~~


Judge's signature

City and state: Washington, D.C.

Beryl A. Howell, Chief Judge
Printed name and title



ATTACHMENT A

DEVICE TO BE SEARCHED

The property to be searched is a **SAMSUNG GALAXY S5 SMARTPHONE, IMEI No.**

 hereinafter the TARGET DEVICE.

The TARGET DEVICE will be located within the District of Columbia.

ATTACHMENT B

ITEMS TO BE SEIZED

The items, information, and data to be seized are fruits, evidence, information relating to, contraband, or instrumentalities of violations of 18 U.S.C. § 641, including, but not limited to:

1. text messages, call logs, phone books, photographs, voice mail messages, images, video, and any other stored electronic data;
2. items, information, and data relating to any reporter or news outlet, including any that reveal or relate to any contact or relationship between James A. Wolfe and any reporter or news outlet;
3. items, information, and data containing, constituting, or referring to sensitive U.S. government information or classified National Security Information;
4. evidence of user attribution showing who used or owned the TARGET DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
5. evidence of the attachment to the TARGET DEVICE to other electronic storage devices or similar containers for electronic evidence;
6. passwords, encryption keys, and other devices that may be necessary to access the TARGET DEVICE;
7. records of, or information about, the TARGET DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” and “data” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

FILED

OCT 27 2017

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

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

IN THE MATTER OF THE SEARCH OF:
SAMSUNG GALAXY S5

IMEI No. [REDACTED]
[REDACTED]

Case No. _____

Case No. 1:17-mj-793

Assigned to: Chief Judge Beryl A. Howell

Date Assigned: 10/27/2017

Description: Search and Seizure Warrant

ORDER

The United States has filed a motion to seal the above-captioned warrant and related documents, including the application and affidavit in support thereof and all attachments thereto and other related materials (collectively, the "Warrant").

The Court finds that the United States has established that a compelling governmental interest exists to justify the requested sealing, and that there is reason to believe that disclosure of the Warrant would jeopardize the investigation by providing the subject of the investigation an opportunity to destroy evidence or flee and jeopardize the investigation by disclosing the details of facts known to investigators, the identities of witnesses, and the investigative strategy.

The Court further finds that a sufficient showing of good cause has been made for the continued sealing of the Classified Annex to the Search Warrant Affidavit, which the FBI shall maintain in its secure files after review by the Court *in camera*, in order to help ensure the protection of classified information and the integrity of the government's investigation.

It is, therefore, this 27th day of October 2017,



1. IT IS ORDERED that the motion is hereby GRANTED, and that the warrant, the application and affidavit in support thereof, all attachments thereto and other related materials, the instant motion to seal, and this Order be SEALED until further order of the Court, except as necessary to facilitate the enforcement of criminal law, including the execution of the arrest warrants, or to any federal official to assist the official receiving the information in the performance of that official's duties.

IT IS FURTHER ORDERED that the Classified Annex shall be maintained, under seal, in the FBI's secure files, on behalf of the Court, as a part of the record.

IT IS FURTHER ORDERED that the Clerk of the Court shall provide the United States Attorney's Office with three certified copies of this application and Order upon request, and shall provide copies of this Order to the Agency upon request.


BERYL A. HOWELL
CHIEF JUDGE

Copy to:


Assistant United States Attorney
United States Attorney's Office
555 4th Street NW, 11th Floor
Washington, D.C. 20530


FILED

OCT 27 2017

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

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF:
SAMSUNG GALAXY S5



Case No. 1:17-mj-793
Assigned to: Chief Judge Beryl A. Howell
Date Assigned: 10/27/2017
Description: Search and Seizure Warrant

Filed Under Seal

ORDER

The United States has filed a motion to delay notification of the above-captioned Warrant pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3).



The Court finds that the United States has established that there is reasonable cause to believe that providing immediate notification of the execution of the Warrant as required by Federal Rule of Criminal Procedure 41(f), may have an adverse result on the ongoing covert investigation, as defined in 18 U.S.C. § 2705.

It is, therefore, this 27th day of October 2017,

IT IS ORDERED that the Government's motion is be GRANTED and the United States may delay notice until 30 days from the date of the execution of the Warrant.


BERYL A. HOWELL
CHIEF JUDGE

Copy to:


Assistant United States Attorney
United States Attorney's Office
555 4th Street NW, 11th Floor
Washington, D.C. 20530


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)*
SAMSUNG GALAXY S5



Case No. 1:17-mj-793
Assigned to: Chief Judge Beryl A. Howell
Date Assigned: 10/27/2017
Description: Search and Seizure Warrant

APPLICATION FOR A SEARCH WARRANT

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

See Attachment A incorporated herein and included as part of the Affidavit in Support of this Application for a Search Warrant

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

See Attachment B incorporated herein and included as part of the Affidavit in Support of this Application for a Search Warrant

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

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

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 641	Theft/conversion of government property

The application is based on these facts:
See Attached Affidavit

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

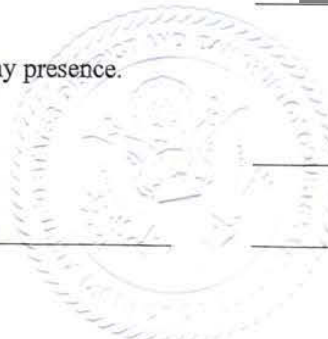
 Applicant's signature

 Printed name and title

Sworn to before me and signed in my presence.

Date: 10/27/2017

City and state: Washington, D.C.



Judge's signature

Beryl A. Howell, Chief Judge
 Printed name and title

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

**IN THE MATTER OF
THE SEARCH OF:
SAMSUNG GALAXY S5**

Case No. 1:17-mj-793
Assigned to: Chief Judge Beryl A. Howell
Date Assigned: 10/27/2017
Description: Search and Seizure Warrant

UNDER SEAL

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER
RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

I, [REDACTED] being first duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this Affidavit in support of an Application under Rule 41 of the Federal Rules of Criminal Procedure for a Search Warrant authorizing the examination of property – a digital device as described in **Attachment A** – and the extraction from that property of electronically stored information as described in **Attachment B**.

2. I am “an investigative or law enforcement officer” of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States or of a state or political subdivision thereof, who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

3. I have been a Special Agent with the Federal Bureau of Investigation (“FBI”) since [REDACTED] assigned since [REDACTED] to the Counterintelligence Division of the Washington Field Office (“WFO”). Prior to my appointment as a Special Agent, I worked as an

Investigative Specialist with the FBI for [REDACTED] years, addressing surveillance matters regarding counterintelligence and counterterrorism investigations. As a Special Agent, I am responsible for investigating offenses involving espionage, illegal agents of foreign powers, media leaks of classified national security information, and the unauthorized retention and disclosure of classified national security information, including defense-related information.

4. I am familiar with the facts and circumstances set forth below from my personal participation in this investigation, my review of documents and other evidence, as well as publicly-available information, and my conversations with other law enforcement officers. Because this Affidavit is being submitted for the limited purpose of supporting an Application for a Search Warrant, I am setting forth only those facts and circumstances necessary for that purpose. Unless otherwise indicated, all written and oral statements referred to herein are set forth in substance and in part, rather than verbatim.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. On the basis of my knowledge concerning this investigation, and on the basis of other information which I have reviewed and determined to be reliable, I allege the following facts to show that there is probable cause to believe that the SAMSUNG GALAXY S5, IMEI [REDACTED] smartphone bearing number [REDACTED] (the "TARGET DEVICE"), which is described in **Attachment A**, has data that furthers the investigation into potential violations of 18 U.S.C. § 641 (conversion of U.S. government property), and other crimes. Specifically, there is probable cause to believe that the TARGET DEVICE contains evidence, fruits, and instrumentalities of violations of the aforementioned offense, as more fully described in **Attachment B**.

PROBABLE CAUSE

6. I believe that the facts and circumstances set forth below establish probable cause to believe that since at least December 1, 2016, and through the present, James A. WOLFE, Director of Security for the Senate Select Committee on Intelligence (“SSCI”) has used, and continues to use, his personal smartphone bearing number [REDACTED] – the TARGET DEVICE – to disclose or facilitate the disclosure of sensitive information that is the property of the United States government, and on occasion classified national security information (“NSI”), including NSI related to the national defense, to a news reporter, referred to herein as “REPORTER.”

7. Pursuant to Executive Order 13526, NSI shall be classified at the TOP SECRET level when its unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to the national security. NSI shall be classified at the SECRET level when its unauthorized disclosure reasonably could be expected to cause serious damage to the national security.

UNITED STATES SENATE SELECT COMMITTEE ON INTELLIGENCE (SSCI)

8. The SSCI was created by the Senate to “oversee and make continuing studies of the intelligence activities and programs of the United States Government,” to “submit to the Senate appropriate proposals for legislation and report to the Senate concerning such intelligence activities and programs,” and to “provide vigilant legislative oversight over the intelligence activities of the United States to assure that such activities are in conformity with the Constitution and laws of the United States.” S. Res. 400, 94th Cong., 2d Sess. (1976) (as amended). In the course of executing its duties, SSCI receives classified national security

information from Executive Branch intelligence community agencies, including the FBI. According to the Rules of Procedure of the Select Committee on Intelligence, “access to classified information supplied to the Committee shall be limited to those Committee staff members with appropriate security clearances and a need-to-know”

JAMES A. WOLFE

9. James A. WOLFE, [REDACTED] is a United States national who became employed by SSCI in or about May 1987. Prior to that, he served for approximately four years on active duty with the U.S. Army, assigned to [REDACTED] U.S. Army Intelligence Command (“INSCOM”) at Ft. Meade, Maryland, and was honorably discharged as a Staff Sergeant in or about March 1987. He became Director of Security for SSCI in or about 1990 and remains so employed.

10. In his capacity as the SSCI Director of Security, WOLFE is responsible for receiving, maintaining, and managing the classified NSI provided to SSCI by Executive Branch intelligence community agencies, and for making authorized dissemination of such NSI to SSCI members and staff. He is also responsible for managing the SSCI facilities used in connection with such information, including the SSCI’s Sensitive Compartmented Information Facility (“SSCI SCIF”).

11. [REDACTED] granted WOLFE an initial TOP SECRET clearance with access to Sensitive Compartmented Information (“TS/SCI”) on August 23, 1988, following a security background investigation conducted by the FBI. Subsequent periodic background investigations on WOLFE were successfully completed in or about 1997, 2002, 2008, and 2014. [REDACTED]

[REDACTED] Based on my experience, I know that an individual who is granted a security clearance, [REDACTED] must in each case sign a form certifying that he understands the restrictions on handling and communicating classified information, and the criminal penalties for violating those restrictions, including 18 U.S.C. § 641.

12. According to an individual who has personal knowledge of the SSCI SCIF, with whom I have spoken, WOLFE's office is located within the SSCI SCIF [REDACTED] [REDACTED] Electronic devices such as personal smartphones are not permitted within a SCIF and must be left outside the SCIF. At the entrance to the SSCI SCIF, there are boxes where a person may secure such an electronic device before entering the SCIF.

13. [REDACTED]

[REDACTED]

14. WOLFE uses the moniker [REDACTED]

[REDACTED]

15. Verizon Wireless subscriber information confirms that WOLFE has been the subscriber of telephone number [REDACTED] since December 14, 2007.

REPORTER¹

16. REPORTER, born in [REDACTED], is a United States national who, [REDACTED] [REDACTED] graduated from university with a B.A. in journalism in [REDACTED]. According to published news reports, [REDACTED] REPORTER served as an intern with a national news outlet (“News Outlet #1”) in Washington, D.C., working with two other reporters. REPORTER assisted in the publication of a number of articles in 2013 and 2014, and one of the news articles that was published with REPORTER’s assistance on March 4, 2014, was entitled “Probe: Did the CIA spy on the U.S. Senate?” The article reported on a dispute between the CIA and SSCI over the SSCI report on the CIA’s secret detention and interrogation program; the article cited sources saying that the CIA monitored computers that Senate aides used to prepare the report. According to the article itself, the article was based on information “provided by people with knowledge of the dispute being fought in the seventh-floor executive offices of the CIA’s headquarters in Langley, Va., and the [Senate Intelligence] committee’s high-security work spaces on Capitol Hill.” According to a separate published news profile of REPORTER, News Outlet #1’s article was “the direct result of tips she received through unnamed sources with whom she has developed trusting relationships since she began reporting for [News Outlet #1] in May 2013.” The News Outlet #1 team, including REPORTER, was nominated for the 2015 Pulitzer Prize for Investigative Journalism.

¹ REPORTER’s true identity is set forth in the Classified Annex to this Affidavit, as are the true names of News Outlets #1, #2, #3, and #4. See the “Classified Annex” section below.

17. [REDACTED]

18. [REDACTED]

from October 2014 to October 2015, REPORTER was employed by an online news service (“News Outlet #2”) in Washington, D.C.; from November 2015 to May 2017, she was employed by a different online news service (“News Outlet #3”) in Washington, D.C.; and in May 2017 she became, and remains, employed as an investigative reporter with “News Outlet #4.” During the course of this investigation, I have reviewed numerous news articles published by REPORTER from 2013 to the present, and for all four employers, REPORTER has reported mainly on national security and intelligence matters, and particularly on activities of the SSCI. [REDACTED]

[REDACTED] Based on the content of her reporting, I believe that numerous articles published by REPORTER contain information which could only have been provided by a person, or persons, with intimate inside knowledge of SSCI’s activities, including those involving sensitive U.S. government information [REDACTED]

19. [REDACTED]

[REDACTED]

RELATIONSHIP BETWEEN WOLFE AND REPORTER

20. Based on REPORTER's work covering SSCI's handling of classified NSI of the CIA, from mid-2013 through early 2014, and the fact that WOLFE was the Director of Security for SSCI during that period, I believe WOLFE was acquainted with, and may have served as an unauthorized source for, REPORTER as early as mid-2013.

21. Toll records for WOLFE's personal smartphone bearing number [REDACTED] – the TARGET DEVICE – for the period from December 1, 2016, through October 10, 2017, show that the TARGET DEVICE and a particular phone number exchanged 25,751 "Short Message Service" ("SMS") messages – also known as text messages – (accounting for 67% of WOLFE's total text messages) and 556 phone calls (accounting for 21% of WOLFE's total phone calls). Thus, for the period from December 1, 2016, through October 11, 2017, WOLFE exchanged communications with that particular phone number a total of more than 26,000 times, or an average of more than 83 times per day – far exceeding the total of WOLFE's remaining personal cellphone communications. In 2011, REPORTER identified that particular phone number as her phone number, [REDACTED]. Recent investigation has confirmed that that particular phone number is currently REPORTER's personal cellphone number.

22. A pen register and trap and trace device activated on the TARGET DEVICE on October 20, 2017, shows that the TARGET DEVICE and REPORTER's personal cellphone

remain in regular, frequent contact through the date of this Affidavit. My review of the toll records for WOLFE's personal smartphone – the TARGET DEVICE – also indicates that he is using a web-based application called [REDACTED]. I am aware that this application can be installed on a computer and can allow an individual to access and send SMS messages through his or her cellphone from the computer by use of the application. This application would allow, for example, [REDACTED]

[REDACTED] (Electronic devices such as personal cellphones are not permitted inside SCIF space, and must be left outside.) I have been made aware by Verizon that the application may download SMS messages onto both the computer and the cellphone, and that the web-based application would likely contain some or all of the SMS messages used by the application, depending on the user's settings.

23. [REDACTED]

24. [REDACTED]

25.

26.

27.




DISCLOSURE #1

28. In early March 2017, there was intense public interest in an ongoing FBI investigation into alleged Russian influence in the 2016 general election. The then-Director of the FBI provided classified oral briefings to the leadership of the Senate and the House of Representatives, including SSCI and the House Permanent Select Committee on Intelligence (“HPSCI”) (referred to collectively herein as “the Senate and House leadership”).

29. In March 2017, the Senate and House leadership requested that a particular agency of the Executive Branch furnish a copy of a specific classified document (“the Classified Document”) for their review. The Classified Document was classified TOP SECRET overall because it contains both SECRET and TOP SECRET information. The nature of the Classified Document itself is classified at the SECRET level. A specific SECRET fact (“the Classified Fact”²) is the identity of an individual who was implicated in an earlier espionage investigation

² The Classified Document and the Classified Fact are identified in the Classified Annex to this Affidavit. See the “Classified Annex” section below.

involving Russia, and who was alleged to have met with a Russian intelligence officer. The paragraph in the Classified Document containing the Classified Fact was clearly marked “S//NF”, indicating that the information was classified at the SECRET level and not for dissemination to any foreign government. The Classified Fact was, and remains, classified at the SECRET level. The DOJ agreed to provide copies of the Classified Document to the Senate and House leadership on a “read-only” basis.

30. On March 17, 2017, the Classified Document was transported to the SSCI SCIF and was read by numerous members of the Senate and House leadership and their staff. This was the first time that the Classified Fact was disclosed to any SSCI members and staff and other Senate and House leadership and their staff.

31. On April 3, 2017, at a particular time of the evening known to me, News Outlet #2 published an online article, under REPORTER’s byline, that contained the Classified Fact. This was the first published news report of the Classified Fact.

32. Although the News Outlet #2 article cited the individual who is the subject of the Classified Fact as a source “confirming” the Classified Fact, I believe that REPORTER already knew the Classified Fact, and thereafter, on the day the article was published, reached out to the individual to seek such confirmation. Furthermore, based on information developed in this investigation, I submit there is probable cause to believe that WOLFE disclosed the Classified Fact to REPORTER.

a. According to WOLFE’s personal smartphone toll records, the TARGET DEVICE and REPORTER’s personal cellphone exchanged 82 SMS communications during March 17, 2017. In addition, on the evening of March 17, 2017, there occurred a

28-minute phone call between the TARGET DEVICE and REPORTER's personal cellphone.

b. On the night of April 3, 2017 – the date of the REPORTER's publication of the Classified Fact – at a particular time known to me, REPORTER appeared on a national cable television show and engaged in the following exchange:

REPORTER: I had been doing a lot of reporting on it so I know that it was him in the document, and when I asked him about it he said, "Yes"

Host: So you were able to figure this out before you got the confirmation from him. Obviously, the icing on the cake is him saying, "Yeah, it's me."

REPORTER: Mmmm-hmmm. [Nodding her head up and down affirmatively.]

I believe this exchange unequivocally indicates that REPORTER knew, before obtaining confirmation from the individual himself, the individual's identification as contained in the Classified Fact.

c. According to WOLFE's personal smartphone toll records, the TARGET DEVICE and REPORTER's personal cellphone exchanged 124 SMS communications during April 3, 2017. In addition, on April 3, 2017, there occurred a phone call between the TARGET DEVICE and REPORTER's personal cellphone lasting 7 minutes at approximately 20 minutes after her News Outlet #2 article was published, and another lasting 15 minutes at approximately 90 minutes after her cable television show appearance.

d. On April 4, 2017, REPORTER posted on [REDACTED] a photo of herself, smiling, from the national cable television show broadcast, with the

caption: “when u ask if he met with a Russian spy but you’ve already got those receipts.”

According to my research, the term “receipts” in this context likely means “proof.” I believe that this posting also indicates that REPORTER knew the Classified Fact before seeking confirmation from the individual.

DISCLOSURE #2

33. In October 2017, News Outlet #4 published an online article, under REPORTER’s byline, reporting that a particular individual had informed SSCI that he will not be cooperating with any requests to appear before the panel and “would plead the Fifth, according to a source familiar with the matter.” The article also stated: “The intelligence committee declined to comment.”

34. Based on the aforementioned facts establishing the relationship between WOLFE and REPORTER, I believe it is highly likely that the “source familiar with the matter” cited by REPORTER was WOLFE.

OTHER INDICIA OF REPORTER’S SOURCE WITHIN SSCI

35. On the night of Monday, September 18, 2017, according to WOLFE’s personal smartphone toll records, there occurred phone calls between the TARGET DEVICE and REPORTER’s personal cellphone lasting approximately 28 minutes, followed immediately by another lasting approximately 23 minutes and a third lasting approximately 15 minutes. In addition they exchanged 42 SMS communications during that day. On the morning of Tuesday, September 19, 2017, there occurred a phone call lasting approximately 15 minutes, and they exchanged 80 SMS communications during that day. [REDACTED] on September 19, 2017, REPORTER commented:

a. "Senate Intel has been soo frustrated in recent weeks by the constant dribble of leaks about who's testifying to them, when."

b. "There was a real come-to-Jesus at SSCI in June, after leaks out of the Comey hearing TI;dr [sic] was, stop leaking or you'll screw everything up."

c. "So this constant barrage of 'this person is appearing before SSCI this day' or release of testimony has majorly irked them. On all sides."

d. "The SSCI read is, Trumpster lawyers will leak info about upcoming appearances blame the committee, then use as a pretext not to cooperate."

e. "After Cohen started sending talking [sic] to the media over the last few day [sic], SSCI had had enough."

f. "Cancelling & forcing him to testify openly is a very clear signal flare to the rest of Team Trump. And its been a loooooong time coming."

36. On October 3, 2017, REPORTER posted [REDACTED] that: "SSCI negotiated for MONTHS to get access to Russia stuff. It is so, so close hold that even among most highly-cleared, access is limited."

37. In the late afternoon of October 25, 2017, at a particular time known to me, REPORTER posted on [REDACTED] "did we know Cohen's getting interviewed by SSCI today? Michael Cohen's getting interviewed by SSCI today. (Still. Going on like 6 hours)." According to the pen register on WOLFE's personal smartphone, on that same day, WOLFE and REPORTER exchanged 18 SMS communications between mid-afternoon and late at night, including 7 SMS communications within the hour before REPORTER's [REDACTED]

38. There is probable cause to believe that the TARGET DEVICE contains fruits, evidence, information, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 18 U.S.C. § 641 (conversion of government property) and other crimes.

39. The TARGET DEVICE to be searched, as further described in **Attachment A**, is the personal smartphone of WOLFE, which is believed to be generally carried on his person. In furtherance of this investigation, the FBI anticipates scheduling a meeting, which WOLFE would attend, on or about Monday, October 30, 2017, within the District of Columbia. The meeting will be arranged by the FBI, in part, to create an opportunity to gain surreptitious access to the TARGET DEVICE for purposes of executing this Warrant, if approved. It is anticipated that WOLFE will be required to leave the TARGET DEVICE unattended during the meeting, which will enable agents to surreptitiously execute the requested Warrant and thereafter enable WOLFE to retrieve the TARGET DEVICE without knowledge of the Warrant's execution.

CLASSIFIED ANNEX

40. I represent to the Court that the Classified Annex to this Affidavit, which is incorporated herein by reference and which identifies the true names of REPORTER and of News Outlets #1, #2, #3, and #4, as well as the true nature of the Classified Document and the Classified Fact, is classified at the SECRET level because (1) the true names of REPORTER and of News Outlets #1, #2, #3, and #4, when read together with the information contained in this Affidavit, would reveal classified information at the SECRET level, and (2) the true nature of the Classified Document and the Classified Fact remain classified at the SECRET level. When separated from the Classified Annex, this Affidavit is not classified. After providing the Court with this Affidavit, including the Classified Annex, *in camera* for the Court's review for

purposes of the Application for a Search Warrant, I request that the FBI be permitted to maintain the Classified Annex in its files, on behalf of the Court as part of the record. I further request that the Court order that this Affidavit, including the Classified Annex, remain under seal, except that the agents and other personnel, including prosecutors, involved in execution of the requested Warrant, who have the necessary security clearance, will review the Classified Annex in the course of their duties. In addition, the Affidavit, including the Classified Annex, may be disclosed as necessary to accomplish the Special Search Procedures set forth below.

TECHNICAL TERMS

41. Based on my training and experience, and information acquired from other law enforcement officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. “Digital device,” as used herein, includes the following terms and respective definitions:

i. A “computer” means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

ii. “Digital storage media,” as used herein, means any storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks (“DVDs”), USB flash drives, flash memory cards, and internal and external hard drives.

b. “Wireless telephone” (or smartphone, mobile telephone, or cellular telephone), a type of digital device, is a handheld wireless device used for voice and data communication at least in part through radio signals and also often through “wi-fi” networks. When communicating via radio signals, these telephones send signals through networks of transmitters/receivers, enabling communication with other wireless telephones, traditional “land line” telephones, computers, and other digital devices. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of applications and capabilities. These include, variously: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages, e-mail, and other forms of messaging; taking, sending, receiving, and storing still photographs and video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; global positioning system (“GPS”) locating and tracking technology, and accessing and downloading information from the Internet.

c. “Computer passwords and data security devices” means information or items designed to restrict access to or hide computer software, documentation, or data.

Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

d. “Computer software” means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

e. An Internet Protocol (“IP”) Address is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 149.101.1.32). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static – that is, long-term – IP addresses, while other computers have dynamic – that is, frequently changed – IP addresses.

f. The “Internet” is a global network of computers and other electronic devices that communicate with each other using numerous specified protocols. Due to

the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

42. Based on my training, experience, and research, I know that the TARGET DEVICE has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, and SMS messenger. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, and sometimes by implication who did not, as well as evidence relating to the commission of the offense under investigation.

**COMPUTERS, ELECTRONIC/MAGNETIC STORAGE,
AND FORENSIC ANALYSIS**

43. As described above and in **Attachment B**, this application seeks permission to search for information that might be found within the TARGET DEVICE. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that there is probable cause to believe that the records and information described in **Attachment B** will be stored in the TARGET DEVICE for at least the following reasons:

a. Individuals who engage in criminal activity, including violations of 18 U.S.C. § 641, use digital devices, like the TARGET DEVICE, to access websites to facilitate illegal activity and to communicate online; to store on digital devices, like the TARGET DEVICE, documents and records relating to their illegal activity, which can include logs of online “chats”; email correspondence; text or other SMS messages;

contact information, including telephone numbers, email addresses, identifiers for instant messaging and social medial accounts; and store stolen data for future exploitation.

b. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often “back up” or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

c. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person “deletes” a file on a digital device such as a home computer, a smartphone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are

replaced with more recently viewed Internet pages. Thus, the ability to retrieve “residue” of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer, smartphone, or other digital device habits.

44. As further described in **Attachment B**, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this Affidavit, but also for forensic electronic evidence or information that establishes how the TARGET DEVICE was used, the purpose of its use, who used it (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in the TARGET DEVICE at issue here because:

a. Although some of the records called for by this Warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the TARGET DEVICE are, as described further in **Attachment B**, called for by this Warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the TARGET DEVICE not currently associated with any file, can provide

evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smartphone, or other digital device was in use. Computer, smartphone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. I know that when an individual uses a digital device to commit a violation of 18 U.S.C. § 641, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

METHODS TO BE USED TO SEARCH DIGITAL DEVICES

45. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

For these reasons, there is a reasonable necessity that the digital data from TARGET DEVICE be seized in order to conduct the requested search.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Recovery of “residue” of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement

laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting “keyword” search techniques

and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format (“PDF”), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

e. Analyzing the contents of mobile devices can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running

IOS 7, deployed a type of sophisticated encryption known as “AES-256 encryption” to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, “Hide It Pro,” disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching the TARGET DEVICE for the information, records, or evidence pursuant to this Warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, I request permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this Warrant. In addition, the assistance of other government agencies may be sought in order to successfully retrieve and review the data.

g. In searching for information, records, or evidence, further described in **Attachment B**, law enforcement personnel executing this Warrant will employ the following procedures:

i. The TARGET DEVICE, and/or any digital images thereof created by law enforcement in aid of the examination and review, will be examined and reviewed by law enforcement personnel, sometimes with the aid of a technical expert, including an expert from another government agency, in an appropriate setting, in order to extract and seize the information, records, or evidence described in **Attachment B**.

ii. The analysis of the contents of the TARGET DEVICE may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by “opening,” reviewing, or reading the images or first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic “keyword” searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

iii. In searching the TARGET DEVICE, the forensic examiners may examine as much of the contents of the device as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in **Attachment B**. In addition, the forensic examiners may search for and attempt to recover “deleted,” “hidden,” or encrypted data to determine whether the contents fall within the items to be seized as described in **Attachment B**. Any search techniques or protocols used in searching the contents of the TARGET DEVICE will be specifically chosen to identify the specific items to be seized under this Warrant.

SPECIAL SEARCH PROCEDURES

46. Notwithstanding the foregoing, I have been informed by the prosecutors overseeing the investigation in this matter that they have decided to adopt special procedures in light of the possibility that the TARGET DEVICE contains materials that are protected by the Speech or Debate Privilege, U.S. Const. art I., § 6, cl. 1 (“the Privilege”). Accordingly, before the procedures set forth in the immediately foregoing section entitled “Methods to be Used” are executed, the following will occur.

47. Special search procedures will be employed with respect to the TARGET DEVICE to assure that an appropriate opportunity is afforded to the Senator serving as Chairman of SSCI to either waive or assert the Privilege, before employees or agents of the

Executive Branch conduct any review of the contents of the TARGET DEVICE.³ These special search procedures are as follows:

a. As soon as practicable after the agents executing the Warrant obtain an image of the contents of the TARGET DEVICE, but before any contents are reviewed, the Department of Justice (“DOJ”) will contact the SSCI Chairman to inform him of the Warrant.

b. Before conducting any review of the contents of the TARGET DEVICE, DOJ will request that the SSCI Chairman waive the Privilege and consent to the search of the TARGET DEVICE pursuant to the Warrant. If the SSCI Chairman agrees to waive the Privilege, the agents will be authorized to search the TARGET DEVICE for evidence, fruits, and instrumentalities of the criminal violations set forth in this Affidavit, using the procedures set forth above.

c. Because there is no practical way to segregate contents of the TARGET DEVICE without reviewing the contents, if the SSCI Chairman declines to waive the privilege, the agents will, without reviewing the contents of the TARGET DEVICE, provide the contents to the SSCI Chairman for a privilege review.

d. If the SSCI Chairman elects to conduct a privilege review, the SSCI Chairman will have 30 days to review the contents of the TARGET DEVICE and provide the U.S. Attorney’s Office for the District of Columbia (“USAO”) with a log of the

³ The United States Court of Appeals for the District of Columbia has held that even incidental review of Speech or Debate privileged material by agents during the execution of a search of the office of a Member of Congress violates the Privilege unless the Member is provided an opportunity to review and assert the Privilege. *United States v. Rayburn House Office Building, Room 2113*, 497 F.3d 654, 662 (D.C. Cir. 2007).

records contained on the TARGET DEVICE over which the Privilege is being asserted. That log will identify each record by date, recipient, sender, and subject matter, if such information is available. As needed, the USAO will request that the District Court review the records over which the SSCI Chairman has asserted the Privilege, in order for the Court to make a final determination whether they contain privileged information.

e. Alternatively, if the SSCI Chairman elects to conduct a privilege review, the SSCI Chairman may complete such review within 30 days by working together with agents assigned to the investigation, to jointly review the contents of the TARGET DEVICE.

f. If the SSCI Chairman elects to conduct a privilege review, and fails to complete such review within 30 days, the government will provide the contents of the TARGET DEVICE to the District Court for its review.

48. In summary, neither the USAO nor the agents executing the Warrant – nor any other employee or agent of the Executive Branch – will review the contents of the TARGET DEVICE until: (1) the SSCI Chairman waives the Privilege, as set forth in section b. of the foregoing numbered paragraph; (2) the SSCI Chairman identifies non-privileged material from the TARGET DEVICE that can be reviewed, as set forth in section d. of the foregoing numbered paragraph; (3) the SSCI Chairman and law enforcement agents jointly review the contents of the TARGET DEVICE, as set forth in section e. of the foregoing numbered paragraph; or (4) pursuant to further order of the Court.

REQUEST FOR DELAYED NOTIFICATION

49. Based on information developed in the course of this investigation, beginning as early as December 1, 2016, and continuing to the present, WOLFE has used, and continues to use, his personal smartphone bearing number [REDACTED] - the TARGET DEVICE - in communicating with REPORTER, and there is probable cause to believe that WOLFE has used, and continues to use, the TARGET DEVICE to transmit and facilitate the transmission to REPORTER of sensitive information that is the property of the U.S. government, and on occasion classified NSI, including NSI related to the national defense.

50. This investigation is covert and on-going. We are currently using traditional investigative techniques as well as conducting court-authorized electronic surveillance to uncover the full scope of WOLFE's illegal activities. Given the sensitive nature of the criminal activities under investigation, as well as the additional anticipated investigation steps, it is likely that the investigation will continue for at least a 30-day period.

51. There is reasonable cause to believe that providing immediate notice of the execution of the warrant requested herein as required by Federal Rule of Criminal Procedure 41(f) prior to the conclusion of this investigation may lead to numerous adverse results as defined in 18 U.S.C. § 3103a(b)(1) (incorporating by reference 18 U.S.C. § 2705):

a. Based on my training and experience, I know that providing notice of the execution of the warrant requested herein, prior to the conclusion of this investigation, would seriously jeopardize the ongoing investigation as such a disclosure would give WOLFE an opportunity to change patterns of behavior and destroy evidence.

b. If WOLFE were notified that law enforcement searched the TARGET DEVICE, it is reasonable to believe he would immediately terminate communicating with REPORTER. This in turn, would foreclose any possibility of a continued covert investigation into the above-described criminal activity by WOLFE.

c. Finally, there is reasonable cause to believe that providing notice of the execution of the Warrant requested herein, prior to the conclusion of this investigation, would likely lead to the destruction of valuable evidence. As described above, there is probable cause to conclude that WOLFE's criminal activity is conducted using his facilities, including computers, at SSCI as well as his personal smartphone and other communications devices. If this investigation were to become known to WOLFE, he would have the access and means to destroy or conceal evidence.

52. Accordingly, I request authorization under 18 U.S.C. § 3103a to delay any notice otherwise required by Federal Rule of Criminal Procedure 41(f), so that investigators will not be required to leave a copy of the Warrant or inventory of items at the location where the TARGET DEVICE is acquired for the purpose of executing the requested search. In order to satisfy the notification and delayed notice requirements of Federal Rule of Criminal Procedure 41(f) and 18 U.S.C. § 3103a, I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the Warrant to delay notice until 30 days after the execution of the Warrant has been completed.

CONCLUSION

53. I submit that this Affidavit supports probable cause for a warrant to search the TARGET DEVICE described in **Attachment A** and to seize the items described in **Attachment B**.

Respectfully submitted,



OCT 27 2017

Subscribed and sworn to before me
on October 27, 2017

A handwritten signature in blue ink that reads "Beryl A. Howell".

Beryl A. Howell
UNITED STATES DISTRICT COURT
CHIEF JUDGE



00 79 79



ATTACHMENT A

DEVICE TO BE SEARCHED

The property to be searched is a **SAMSUNG GALAXY S5 SMARTPHONE, IMEI No.**

 hereinafter the TARGET DEVICE.

The TARGET DEVICE will be located within the District of Columbia.

ATTACHMENT B

ITEMS TO BE SEIZED

The items, information, and data to be seized are fruits, evidence, information relating to, contraband, or instrumentalities of violations of 18 U.S.C. § 641, including, but not limited to:

1. text messages, call logs, phone books, photographs, voice mail messages, images, video, and any other stored electronic data;
2. items, information, and data relating to any reporter or news outlet, including any that reveal or relate to any contact or relationship between James A. Wolfe and any reporter or news outlet;
3. items, information, and data containing, constituting, or referring to sensitive U.S. government information or classified National Security Information;
4. evidence of user attribution showing who used or owned the TARGET DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
5. evidence of the attachment to the TARGET DEVICE to other electronic storage devices or similar containers for electronic evidence;
6. passwords, encryption keys, and other devices that may be necessary to access the TARGET DEVICE;
7. records of, or information about, the TARGET DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” and “data” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

CLASSIFIED ANNEX TO AFFIDAVIT

REPORTER:



NEWS OUTLET #1: McClatchy DC News

NEWS OUTLET #2: Huffington Post

NEWS OUTLET #3: BuzzFeed News

NEWS OUTLET #4: Politico

CLASSIFIED DOCUMENT #1:

(U//FOUO) (~~S//NF/FISA~~) Application for surveillance on Carter Page pursuant to the Foreign Intelligence Surveillance Act (FISA).

CLASSIFIED FACT #1:

(U//FOUO) (~~S//NF/FISA~~) "Male-1" referred to in the Carter Page FISA Application is Carter Page.