

EXHIBIT 12

AO 106 (SDNY Rev. 01/17) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

19 MAG 8467

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

See Affidavit and Attachment A

Case No. S1 17 Cr. 548 (PAC)

APPLICATION FOR A SEARCH AND SEIZURE 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 Affidavit and Attachment A

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

See Attached Affidavit and its Attachment A

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(s)</i>	<i>Offense Description(s)</i>
18 U.S.C. §§ 793, 1030, and 2252A	Unlawful disclosure of classified information, unauthorized computer access, and illegal acts related to child pornography, as well as conspiracies and attempts to violate these provisions and aiding and abetting these offenses.

The application is based on these facts:

See Attached Affidavit and its Attachment A

- Continued on the attached sheet.
- Delayed notice of 5 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

Christian Jensen, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 09/09/2019

Judge's signature

The Honorable James L. Cott, U.S.M.J.

Printed name and title

City and state: New York, NY

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States Of America for a Search and Seizure Warrant for a Huawei Nexus 6P cellular telephone with IMEI Number 867980020596552

TO BE FILED UNDER SEAL

**Agent Affidavit in Support of
Application for Search and Seizure
Warrant**

SOUTHERN DISTRICT OF NEW YORK) ss.:

CHRISTIAN JENSEN, being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I am a Special Agent of the Federal Bureau of Investigation (“FBI”) and have been so employed since 2017. I am currently assigned to a squad responsible for counterintelligence matters. In the course of my duties as a Special Agent, I have been involved in investigating offenses involving espionage and related violations of law, including unauthorized retention, gathering, transmitting or losing classified documents or materials; unauthorized removal and retention of classified documents or materials; illegally acting in the United States as a foreign agent; and other national security offenses. As a result of my involvement in those investigations, as well as my training in counterintelligence operations, I am familiar with some of the tactics, methods, and techniques of United States persons who possess, or have possessed a United States Government security clearance and may choose to harm the United States by misusing their access to classified information. I am also familiar, though my training and experience with the use of computers in criminal activity and the forensic analysis of electronically stored information.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the electronic device specified below (the

“Subject Device”) for the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information (“ESI”). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Device

3. The Subject Device is a Huawei Nexus 6P cellular telephone with IMEI Number 867980020596552. The Subject Device is located in the Southern District of New York and will be located in the Southern District of New York at the time of the execution of the proposed warrant.

4. Based on my training, experience, and research, I know that the Subject Device has capabilities that allow it to serve as, among other things, a wireless telephone, a digital camera, a video recorder, a portable media player, a GPS navigation device, and a calendar. I also know that the Subject Device is a so-called “smartphone” in that it is Internet capable and can access the Internet through cellular and WiFi networks and that through user-installed applications, the Subject Device is capable of accessing and storing Internet-based content, including email, digital storage accounts, social media accounts, bank and credit card accounts, and almost any other manner of service or platform otherwise accessible through the Internet. Moreover, the Subject Device has an internal storage capacity that allows the Subject Device to store all manner of electronic data, including data obtained from the various Internet-based platforms I have identified above.

5. Based on my training, experience, and conversations with other law enforcement officers, I know that the International Mobile Equipment Entity (“IMEI”) is an identifying number unique to a particular cellular telephone—in other words, although the call number assigned to a specific phone may change, the IMEI assigned to a specific phone does not.

C. The Subject Offenses

6. I respectfully submit that probable cause exists to believe that the Subject Device contains evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 793 (unlawful disclosure of classified information), 1030 (unauthorized computer access), and 2252A (illegal acts related to child pornography), as well as conspiracies and attempts to violate these provisions and aiding and abetting these offenses (the “Subject Offenses”).

II. Probable Cause

A. WikiLeaks’ Publication of Classified Information and Related Charges Against Joshua Adam Schulte

7. Based on my conversations with others, my training and experience, and my review of publicly available material on the Internet, including on the website wikileaks.org (“WikiLeaks”), I know that, between on or about March 7, 2017 and November 17, 2017, WikiLeaks made 26 separate online disclosures of materials (the “WikiLeaks Disclosures”). The WikiLeaks Disclosures included classified information about sensitive cyber-tools from the Central Intelligence Agency (the “CIA Information”), the disclosure of which significantly damaged the national security of the United States by, among other things, revealing certain CIA intelligence-gathering methods.

8. Based on my training, experience, participation in this investigation, and conversations with others, I know, among other things, that Joshua Adam Schulte was employed by the CIA as a computer engineer from in or about May 2010 through on or about November 10,

2016, when he resigned from the CIA. During Schulte's more than six years working in the CIA, his responsibilities included, among other things, developing computer code for specific projects, including projects explicitly described in the WikiLeaks Disclosures. Schulte also had a skill set that enabled him to write computer code designed to clandestinely copy data from computers.

9. Based on my training, experience, and participation in this investigation, I also know, among other things, that on or about October 31, 2018, a grand jury in this District returned Superseding Indictment S2 17 Cr. 548 (PAC) (the "Superseding Indictment"), attached as Exhibit A and incorporated by reference, charging Schulte with, among other things the Subject Offenses, specifically:

a. Three counts of violating 18 U.S.C. § 793 (Counts One through Three) and four counts of violating 18 U.S.C. §§ 641 and 1030 (Counts Five through Eight), in connection with Schulte's unlawful theft and transmittal of the CIA Information in or about 2016 (the "WikiLeaks Charges"). As the Superseding Indictment reflects, the WikiLeaks Charges stem from Schulte's theft of the CIA Information using CIA computer systems in or about 2016 and his transmission of that information to WikiLeaks.

b. Another count of violating Section 793 (Count Four), in connection with Schulte's unlawful disclosure and attempted disclosure of classified information from the Metropolitan Correctional Center ("MCC") between in or about December 2017 and in or about October 2018 (the "MCC Leak Charge"). The MCC Leak Charge stems from, among other things, Schulte's illegal use of cellphones in the MCC to transmit and attempt to transmit classified information to other individuals.

c. Three counts of violating 18 U.S.C. § 2252A (Counts Twelve to Fourteen), in connection with Schulte's receipt, possession, and transportation of child pornography (the

“Child Pornography Charges”). The Child Pornography charges relate to Schulte’s possession, on his home computer, of approximately thousands of images and videos of child pornography from at least in or about 2009, up to and including in or about March 2017. Schulte was initially charged by complaint with the Child Pornography Charges in August 2017. The Complaint detailing some of the evidence against Schulte related to the Child Pornography Charges is attached as Exhibit B and incorporated by reference.¹

B. Schulte’s Use of the Subject Device

10. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, following the initial WikiLeaks Disclosure on March 7, 2017, Schulte repeatedly initiated contact, via telephone and text messages, with multiple of his former CIA colleagues. Those colleagues have reported that contact to government and law enforcement officials.

a. In those communications with his former colleagues, Schulte repeatedly asked about the status of the investigation into the disclosure of the Classified Information.

b. Schulte requested more details on the information that was disclosed.

c. Schulte inquired of his colleagues’ personal opinions regarding who, within the CIA, each believed was responsible for the disclosure of the Classified Information. Schulte also asked what other former CIA Group colleagues were saying about the disclosure.

d. Schulte denied being involved in the disclosure of the Classified

¹ The Superseding Indictment also charged Schulte with (i) two counts of violating 18 U.S.C. §§ 1001 and 1503, in connection with false statements Schulte made to the FBI during its investigation of the WikiLeaks Disclosures; (ii) one count of violating 18 U.S.C. § 401(3), in connection with Schulte’s willful violation of a protective order entered by the Court in this case in 2017; and (iii) one count of violating 18 U.S.C. § 2319, in connection with Schulte’s criminal violation of copyrights.

Information.

e. Schulte indicated at the time (before the FBI had publicly identified Schulte as a subject of its investigation) that he believed that he was a suspect in the investigation of the leak of CIA Information.

11. Furthermore, I know that Schulte made at least some of the communications above using the so-called Google Voice feature associated with a particular Google account with the email address joshschulte1@gmail.com (the "Schulte Gmail Address"). I know from my training and experience, and my participation in this investigation, that Google Voice is a service which provides users the ability to, among other things, make voice calls, send text messages, forward calls, and receive voicemails via their Google accounts. In this case, the Google account in question is the account associated with the Schulte Gmail address and which has the subscriber name "Josh Schulte" (the "Schulte Google Account"). Specifically, for example:

a. Based on my review of documents and conversations with others, I know that on or about March 7, 2017, when WikiLeaks made the first of the WikiLeaks Disclosures, Schulte used the Google Voice feature associated with the Schulte Google Account to send messages to multiple of his former colleagues at the CIA.

b. Schulte, using the Google Voice feature associated with the Schulte Google Account, also had phone calls with former CIA colleagues, including one telephone call with a former colleague during which he, among other things, inquired about the former colleague's personal opinions regarding who was responsible for the disclosure of the Classified Information and what the person's motivation might be. Schulte indicated that he believed that the person responsible was a contractor who disclosed the Classified Information for fame.

c. During a call on or about March 8, 2017 using the telephone number

associated with the Schulte Google Account with the same former colleague,² Schulte denied his involvement in the disclosure of the CIA Information, indicated his belief that many people suspected him of the disclosure, and relayed a conversation with another acquaintance during which Schulte had denied involvement in the disclosure of the CIA Information, but was dissatisfied with the acquaintance's reaction to Schulte's denial.

12. I know, from my review of records, including emails from the Schulte Google Account, and my conversations with others, that Schulte purchased the Subject Device in or about September 2016 and that it was delivered to him on or about September 21, 2016. I also know from my review of records and conversations with others that around the time the Subject Device was delivered to Schulte, Schulte signed into the Schulte Google Account on the Subject Device via Google's Android feature.³ That is, the Subject Device's unique IMEI number (as well as other identifiers, such as the Subject Device's device ID, MEID, and serial number) was listed among the identifying features of the telephone associated with the Schulte Google Account. I also know that the same subscription information listed the Schulte Gmail address as the user of the Subject Device.

² The telephone number associated with the Schulte Google Account is listed in the subscriber information for the account under the category "SMS."

³ Based on my conversations with other law enforcement agents and others, and my review of documents, I know that Android is a mobile operating system developed by Google, and it is used on a variety of touchscreen mobile devices, such as smartphones and tablet computers. Google retains information related to the Android device associated with an account, including the IMEI, MEID (the Mobile Equipment Identifier), device ID, and/or serial number of the devices. Each of those identifiers uniquely identifies the device used. One device may be associated with multiple different Google and Android accounts, and one Google or Android account may be associated with multiple devices.

C. The First Search of the Subject Device and the Request to Search the Subject Device Again

13. Based on my training, experience, participation in this investigation, review of documents, and conversations with others, I know, among other things, the following:

a. On or about March 15, 2017, FBI agents approached Joshua Adam Schulte in New York, New York and seized the Subject Device pursuant to a subpoena. The Subject Device has been in the FBI's control since that day.

b. On or about March 21, 2017, Schulte, along with two of his then-attorneys, participated in a voluntary, non-custodial interview with prosecutors and FBI agents in Manhattan. During that interview, and in the presence of his counsel, Schulte consented to the search of the Subject Device and agreed to unlock the phone so that the FBI could conduct a forensic examination of the device.⁴

c. After Schulte unlocked the phone, FBI personnel attempted to forensically image the Subject Device so that the FBI could review its contents. However, because the Subject Device rebooted during that process, the FBI was able to obtain only a logical forensic image of the Subject Device (the "Logical Forensic Image"). Although the Logical Forensic Image contains some content from the Subject Device, the Logical Forensic Image does not contain all data that may be on the Subject Device, including deleted information and data from applications. The data and information from the Subject Device that is missing from the Logical Forensic Image would likely be captured on a complete forensic image of the phone ("Complete Forensic Image"). However, in March 2017, the FBI was unable to obtain a Complete Forensic Image of the Subject

⁴ On or about March 16, 2017, the FBI submitted an application for a search warrant for the Subject Device, which was granted. Based on my participation in this investigation, I have learned that, the FBI, however, did not execute that search warrant, because the Subject Device was locked, and thus inaccessible, when the FBI obtained it on or about March 15, 2017.

Device because the Subject Device locked after it rebooted and the FBI did not know the password to unlock the phone again to attempt to obtain a Complete Forensic Image.

d. On or about August 12, 2019, FBI personnel involved in this investigation successfully unlocked the Subject Device using a portion of a password identified during the course of the investigation ("Password-1"). Forensic examiners with the FBI believe that they will be able to obtain a Complete Forensic Image of the Subject Device using Password-1.

e. After unlocking the Subject Device using Password-1, an FBI agent promptly contacted the Assistant United States Attorneys involved in this investigation to inform them of this development, and the decision was made to seek a warrant to search the Subject Device for evidence, fruits, and instrumentalities of the Subject Offenses.

14. Based on the foregoing, I respectfully request authorization to search the Subject Device again in an effort to obtain a Complete Forensic Image. I respectfully submit that there is probable cause to believe that a Complete Forensic Image of the Subject Device will contain some or all of the following:

a. The phone number associated with the Subject Device, as well as call log information of phone numbers of incoming and outgoing, and missed or unanswered calls to and from the Subject Device;

b. Address books and contact lists stored on the Subject Device or its memory card(s);

c. Voicemail messages, opened or unopened, related to the Subject Offenses;

d. Evidence concerning the identity or location of the owner(s) or user(s) of the Subject Device when the Subject Offenses were committed;

e. Evidence concerning the identity and/or location of the individual(s)

involved in the commission of the Subject Offenses;

f. Evidence of communications among, or concerning, participants in or witnesses to the commission of the Subject Offenses;

g. Contact information of co-conspirators and witnesses to the commission of the Subject Offenses, including telephone numbers, email addresses, and identifiers for instant messaging and social media accounts;

h. Text, data, “chats,” MMS (“Multimedia Messaging Service”) messages, SMS (“Short Message Service”) messages, FaceTime messages, and e-mail messages, any attachments to those messages, such as digital photographs and videos, and any associated information, such as the phone number or e-mail address from which the message was sent, pertaining to the Subject Offenses;

i. Digital photographs and videos related to the commission of the Subject Offenses;

j. Browsing history, websites visited, and internet searches conducted on the Subject Device; and

k. Any Global Positioning Satellite (“GPS”) entries, Internet Protocol connections, and location entries to include Cell Tower and WiFi entries.

15. Like individuals engaged in any other kind of activity, individuals who engage in the Subject Offenses store records relating to their illegal activity and to persons involved with them in that activity on electronic devices such as the Subject Device. Such records can include, for example logs of online “chats” with co-conspirators; email correspondence; contact information of co-conspirators, including telephone numbers, email addresses, and identifiers for instant messaging and social medial accounts; stolen financial and personal identification data, including bank account numbers, credit card numbers, and names, addresses, telephone numbers,

and social security numbers of other individuals; and/or records of illegal transactions using stolen financial and personal identification data. Individuals engaged in criminal activity often store such records in order to, among other things, (i) keep track of co-conspirator's contact information; (ii) keep a record of illegal transactions for future reference; (iii) keep an accounting of illegal proceeds for purposes of, among other things, dividing those proceeds with co-conspirators; and (iv) store stolen data for future exploitation.

16. Computer files or remnants of such files can be recovered months or even years after they have been created or saved on an electronic device such as the Subject Device. Even when such files have been deleted, they can often be recovered, depending on how the hard drive has subsequently been used, months or years later with forensics tools. The ability to retrieve from information from the Subject Device depends less on when the information was first created or saved than on a particular user's device configuration, storage capacity, and computer habits.

17. Accordingly, in light of the foregoing, I respectfully submit that there is probable cause to believe that the Subject Device contains evidence, fruits, and contraband relating to the Subject Offenses.

III. Procedures for Searching ESI

A. Review of ESI

18. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained on the Subject Device for information responsive to the warrant.

19. In conducting this review, law enforcement may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

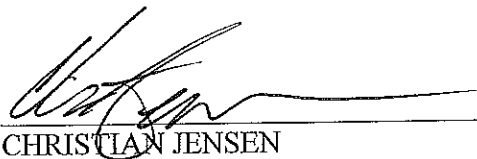
- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by “opening” or reading the first few “pages” of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- “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 the existence and location of search terms related to the subject matter of the investigation. (Keyword searches alone are typically inadequate to detect all information subject to seizure. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.)

20. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement may need to conduct a complete review of all the ESI from the Subject Device to locate all data responsive to the warrant.

IV. Conclusion and Ancillary Provisions

21. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant. Because the Subject Device is in the possession of the FBI, I also respectfully request permission to execute the search warrant at any time in the day or night.

22. The Government also respectfully requests permission to delay notice of the execution of the warrant for five days so that if the search reveals any potential co-conspirators, the Government can investigate those leads before disclosure is made to the defendant.



CHRISTIAN JENSEN
Special Agent
Federal Bureau of Investigation

Sworn to before me on
September 9, 2019



THE HONORABLE JAMES L. COTT
UNITED STATES MAGISTRATE JUDGE

Attachment A

I. Device Subject to Search and Seizure

The device to be seized and searched (the “Subject Device”) is a Huawei Nexus 6P cellular telephone with IMEI Number 867980020596552.

II. Execution of the Warrant

Law enforcement agents are permitted to execute the search warrant at any time in the day or night. Upon the execution of this warrant, notice will be provided at or as soon as possible after the execution of the search.

III. Review of Electronically Stored Information (“ESI”) on the Subject Device

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained on the Subject Device for evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 793 (unlawful disclosure of classified information), 1030 (unauthorized computer access), and 2252A (illegal acts related to child pornography), as well as conspiracies and attempts to violate these provisions and aiding and abetting these offenses (the “Subject Offenses”) as described below. Law enforcement personnel will use reasonable efforts to limit the search of the Subject Device for ESI dated on or after September 21, 2016.

1. The phone number associated with the Subject Device, as well as call log information of phone numbers of incoming and outgoing, and missed or unanswered calls to and from the Subject Device;
2. Address books and contact lists stored on the Subject Device or its memory card(s);
3. Voicemail messages, opened or unopened, related to the Subject Offenses;

4. Evidence concerning the identity or location of the owner(s) or user(s) of the Subject Device;

5. Evidence concerning the identity and/or location of the individual(s) involved in the commission of the Subject Offenses;

6. Evidence of communications among, or concerning, participants in or witnesses to the commission of the Subject Offenses;

7. Contact information of co-conspirators and witnesses to the commission of the Subject Offenses, including telephone numbers, email addresses, and identifiers for instant messaging and social media accounts;

8. Text, data, "chats," MMS ("Multimedia Messaging Service") messages, SMS ("Short Message Service") messages, FaceTime messages, and e-mail messages, any attachments to those messages, such as digital photographs and videos, and any associated information, such as the phone number or e-mail address from which the message was sent, pertaining to the Subject Offenses;

9. Digital photographs and videos related to the commission of the Subject Offenses;

10. Browsing history, websites visited, and internet searches conducted on the Subject Device; and

11. Any Global Positioning Satellite ("GPS") entries, Internet Protocol connections, and location entries to include Cell Tower and WiFi entries.

[REMAINING PAGES INTENTIONALLY OMITTED]