

**EXHIBIT 7**

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In re: Warrant and Order For  
Prospective and Historical Location  
Information and/or Pen Register  
Information for the Cellphones  
Assigned Call Numbers 917-553-3691,  
917-319-5188, and 703-400-2172

17 MAG

2462

17 MAG 2462

AGENT AFFIDAVIT

\_\_\_\_ Mag. \_\_\_\_

**Agent Affidavit in Support of Warrant and Order  
for Cellphone Location and Pen Register Information**

STATE OF NEW YORK     )  
  ) ss.  
COUNTY OF NEW YORK    )

SARA E. LANGENDERFER, Special Agent with the Federal Bureau of Investigation,  
being duly sworn, deposes and states:

**I. Introduction**

1. I am a Special Agent with the Federal Bureau of Investigation (the “FBI” or the “Investigating Agency”). As such, I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I am assigned to the FBI’s New York Field Office, and have been employed by the FBI since 2016. Prior to that, for four years I was an Intelligence Analyst assigned to a task force with the Drug Enforcement Administration (“DEA”). I am currently assigned to a squad responsible for counterespionage matters and have worked in the field of counterintelligence from January 2017 to present. In the course of my duties as a Special Agent, I am responsible for 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; other national security offenses; and the making of false statements. As a result of my involvement in espionage investigations and investigations involving the unauthorized disclosure or retention of classified information, as well as my training in counterintelligence operations, I am familiar with 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, through my training and experience with the use of computers and telephones in criminal activity and the forensic analysis of electronically stored information.

2. **Requested Information.** I respectfully submit this Affidavit pursuant to 18 U.S.C. §§ 2703(c) and (c)(1)(A) and the applicable procedures of Federal Rule of Criminal Procedure 41; 18 U.S.C. §§ 2703(d) & 2705; and 18 U.S.C. §§ 3121-3126, in support of a warrant and order for prospective location information, historical location information, toll records, and/or pen register information, for the Target Cellphones identified below (collectively, the “Requested Information”).

3. **Basis for Knowledge.** This Affidavit is based upon my participation in the investigation, my examination of reports and records, and my conversations with other law enforcement agents and other individuals, as well as my training and experience. Because this Affidavit is being submitted for the limited purpose of obtaining the Requested Information, it does not include all the facts that I have learned during the course of this 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. In addition, unless otherwise indicated, statements by others referenced in this Affidavit were not necessarily made

to me, but may have been provided to me by someone else to whom I have spoken or whose report I have read (and who in turn may have had either direct or indirect knowledge of the statement). Similarly, unless otherwise indicated, information in this Affidavit resulting from surveillance does not necessarily set forth my personal observations, but may have been provided to me by other law enforcement agents who observed the events, and to whom I have spoken or whose report I have read.

**4. Target Cellphones, Subscriber, Target Subject, and Service Providers.** The Target Cellphones referenced in this Affidavit are as follows:

a. Target Cellphone-1 is the cellphone assigned call number 917-553-3691. The subscriber of Target Cellphone-1 is currently unknown. JOSHUA ADAM SCHULTE is believed to use Target Cellphone-1 and is a Target Subject of this investigation. Virgin Mobile USA, LLC is the Service Provider for Target Cellphone-1.

b. Target Cellphone-2 is the cellphone assigned call number 917-319-5188. The subscriber of Target Cellphone-2 is currently unknown. JOSHUA ADAM SCHULTE is believed to use Target Cellphone-2 and is a Target Subject of this investigation. AT&T is the Service Provider for Target Cellphone-2.

c. Target Cellphone-3 is the cellphone assigned call number 703-400-2172. Target Cellphone-3 was subscribed to in the name of Joshua Schulte, 45897 Peach Oak Terrace, Sterling Virginia 20166 (the "Subscriber"), until service was cancelled to Target Cellphone-3 on or about March 12, 2017. JOSHUA ADAM SCHULTE was believed to have used Target Cellphone-3 and is a Target Subject of this investigation. Sprint is the Service Provider for Target Cellphone-3.

**5. Precision Location Capability.** Cellphone service providers have technical capabilities that allow them to collect at least two kinds of information about the locations of the cellphones to which they provide service: (a) precision location information, also known as E-911 Phase II data, GPS data, or latitude-longitude data, and (b) cell site data, also known as “tower/face” or “tower/sector” information. Precision location information provides relatively precise location information about a cellphone, which a provider can typically collect either via GPS tracking technology built into the phone or by triangulating the device’s signal as received by the provider’s nearby cell towers. Cell site data, by contrast, reflects only the cell tower and sector thereof utilized in routing any communication to and from the cellphone, as well as the approximate range of the cellphone from the tower during the communication (sometimes referred to as “per-call measurement” (“PCM”) or “round-trip time” (“RTT”) data). Because cell towers are often a half-mile or more apart, even in urban areas, and can be ten or more miles apart in rural areas, cell site data is typically less precise than precision location information. Based on my training and experience, I know that the Service Providers have the technical ability to collect precision location information from any cellphone on its network, including by initiating a signal on the Service Providers’ network to determine the phone’s location. I further know that cell site data is routinely collected by the Service Providers in the course of routing calls placed to or from any cellphone on its network.<sup>1</sup>

**6. Successor Service Provider.** Because it is possible that the Target Subject may change cellphone service provider during the course of this investigation, it is requested that the warrants

---

<sup>1</sup> Toll records are sometimes necessary or helpful in order to obtain or interpret historical cell site data and are therefore also requested herein.

and investigative orders requested apply without need for further order to any Successor Service Provider who may provide service to the Target Cellphones during the time frames at issue herein.

## **II. Facts Establishing Probable Cause**

7. Although I understand that probable cause is not necessary to obtain all of the Requested Information, I respectfully submit that probable cause exists to believe that the Requested Information will lead to evidence of the crimes of (i) the unauthorized possession and, *inter alia*, the communication of national defense information to someone not entitled to receive it, in violation of Title 18, United States Code, Section 793(d); (ii) the unlawful retention of national defense information, in violation of Title 18, United States Code, Section 793(e); (iii) exceeding authorized access to a computer in order to obtain national defense information with reason to believe that information could be used to the injury of the United States and the advantage of a foreign nation and willfully transmitting that information to a person not entitled to receive it, in violation of Title 18, United States Code, Section 1030(a)(1); (iv) intentionally exceeding authorized access and thereby obtaining information from a department or agency of the United States, in violation of Title 18, United States Code, Section 1030(a)(2)(B); and (v) transmitting computer code to intentionally damage a protected computer, in violation of Title 18, United States Code, Section 1030(a)(5)(A) (collectively, the “Target Offenses”), as well as the identification and locations of the Target Subject who is engaged in the Target Offenses.

### **WikiLeaks Publication of Classified CIA Information**

8. Based on my review of publicly available material on the Internet, including on the website wikileaks.org (“WikiLeaks”), I know that, on March 7, 2017, WikiLeaks published what it claimed were more than 8,000 documents and files that contained classified information (the “Classified Information”) belonging to the Central Intelligence Agency (“CIA”). In its press release accompanying the Classified Information, WikiLeaks further claimed that:

a. The public dissemination of the Classified Information was “the largest ever” unauthorized publication of classified CIA documents.

b. The Classified Information constituted the “first full part” of a series—thus indicating that there would be subsequent publications of additional sensitive CIA information.<sup>2</sup>

c. The “collection” obtained by WikiLeaks amounted to “more than several hundred million lines of code” and revealed the “entire hacking capacity” of the CIA, including various malware, viruses, and other tools used by the CIA.

9. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that:

a. The information that WikiLeaks claimed was classified CIA information—that is, the Classified Information—was at the time of its disclosure, in fact, classified CIA information.

b. Specifically, the Classified Information was created and maintained by one specific group within the CIA which is responsible for various computer engineering activities, including the development of computer code (the “CIA Group”). That CIA Group exists within a larger CIA component (the “CIA Component”). In March 2016, less than 200 employees were assigned to the CIA Group.

c. The Classified Information was maintained by the CIA Group on an isolated local-area computer network (the “LAN”).<sup>3</sup> Only employees of the CIA Group had

---

<sup>2</sup> On or about March 24, 2017, WikiLeaks released twelve additional documents that it claimed were also obtained from the CIA. On or about March 31, 2017, WikiLeaks released a third batch of documents that it claimed were also obtained from the CIA.

<sup>3</sup> In its press release announcing the publication of the Classified Information, WikiLeaks stated that the Classified Information originated from “an isolated, high-security network.”

access to the LAN on which the Classified Information was stored.<sup>4</sup>

i. An isolated network, such as the CIA Group's LAN, is a network-security structure by which the isolated network is physically separated (or "air-gapped") from unsecured networks, such as the public Internet.

ii. Accordingly, such isolated networks, like the LAN, cannot be accessed from the public Internet, but rather only through those computers which are physically connected to the isolated network.

iii. The CIA Group's LAN, and each of its component parts, was maintained in heavily physically secured governmental facilities, which include multiple access controls and various other security measures.

d. Based on a preliminary analysis of the timestamps associated with the Classified Information reflecting the latest (or most recent) creation or modification date associated with the Classified Information, it appears that the Classified Information was copied from the LAN in or about March 2016.

e. The duplication and removal from the LAN of the Classified Information and its subsequent public dissemination via WikiLeaks was not authorized by the United States government.

---

<sup>4</sup> Prior search warrant applications in connection with this investigation set forth that a preliminary analysis had concluded that the Classified Information was likely copied from a back-up server to which the same three systems administrators likely had access. The information that the Classified Information was likely recovered from an automated back-up file which only systems administrators likely had access to was first received by the FBI on or about March 22, 2017. As set forth herein, an investigation is ongoing as to whether the stolen data was in fact back-up data taken from the automated back-up. But, nevertheless, the current assessment remains that the copying of the data, regardless of the data's original location, would likely have required systems administrator access of the type maintained by TARGET SUBJECT JOSHUA ADAM SCHULTE. Accordingly, we respectfully submit, that the precise location from where the Classified Information was taken—whether from an automated back-up file or from a non-back-up computer file—does not affect the probable cause underlying the prior search warrant applications.



f. The unauthorized disclosure of the Classified Information could—at a minimum—reasonably be expected to cause serious damage to the national security of the United States. *See* Executive Order 13526; 18 C.F.R. § 3a.11(a)(2).

g. The Classified Information is national defense information and its disclosure could reasonably be expected to be used to the injury of the United States and to the advantage of a foreign nation. *See* 18 U.S.C. § 793(d) & (e).

10. I know, based on my conversations with other law enforcement agents and others, that TARGET SUBJECT JOSHUA ADAM SCHULTE was employed as a computer engineer by the CIA—specifically in the CIA Group—from in or about May 2010 through on or about November 10, 2016, when he resigned from the CIA.

a. During SCHULTE’s more than six years working in the CIA Group, his responsibilities included, among other things, developing computer code for specific projects, including projects explicitly described in the Classified Information. SCHULTE had a skill set that enabled him to write computer code designed to clandestinely copy data from computers.

b. As part of his responsibilities with the CIA Group in or about March and early April 2016, SCHULTE was one of three system administrators for the LAN. Among other things, that meant that he was one of three employees responsible for maintaining the LAN, and for controlling the access of other CIA Group employees.

c. These three systems administrators also had “super-user” access to the LAN which allowed them broader access to programs, files and servers.

11. Preliminary analysis indicates—but does not conclusively demonstrate—that the wholesale access to, and subsequent copying of, the Classified Information would likely have

required systems administrator access of the type described above.<sup>5</sup>

a. The publicly released Classified Information originally published by WikiLeaks, based on a preliminary review, appears to contain the names and/or pseudonyms of, *inter alia*, multiple CIA employees—including two of the three aforementioned LAN systems administrators. SCHULTE's name, on the other hand, was not apparently published in the Classified Information. Thus, SCHULTE was the only one of the three systems administrators who was not publicly identified via WikiLeaks's first publication of the Classified Information.

b. The other two individuals who served in March 2016 as systems administrators for the CIA Group's LAN remain employed by the CIA. SCHULTE resigned from the CIA in November 2016, as described in detail below.

12. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that SCHULTE has alleged that, on or about March 1, 2016, another CIA Group co-worker had made a threat against him. Thereafter, the CIA conducted an investigation into the incident. SCHULTE expressed deep unhappiness about the way that CIA responded to the alleged threat.

a. He threatened legal action against the CIA for its handling of the situation, and repeatedly stated that he felt that he was being punished by CIA management for reporting the alleged threat incident.

b. SCHULTE informed CIA security that, if "forced into a corner" he would

---

<sup>5</sup> Analysis of the precise origin of the Classified Information is ongoing. While there may have been multiple mechanisms to gain access to the Classified Information, the preliminary assessment is that the most likely routes to acquiring that information would have required systems administrator access. But even if true, it is, of course, also possible that an employee who was not a designated systems administrator could find a way to gain access to the Classified Information. For example, such an employee could steal and use—without legitimate authorization—the username and password of a designated systems administrator. Or an employee lacking systems administrator access could, at least theoretically, gain access to the Classified Information by finding a "back-door" to it.

proceed with a lawsuit against the CIA. He also repeatedly threatened that he or his lawyer would go to the media.

c. In addition, CIA security learned that SCHULTE had removed an internal CIA document from CIA facilities that regarded his complaints to the CIA concerning its handling of the alleged threat, despite being told multiple times by CIA security officials not to do so.

13. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, on or about April 4, 2016, SCHULTE and the other CIA employee were each reassigned to different offices within the CIA Group in response to the workplace dispute discussed above in Paragraph 12.

14. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, around the time of his reassignment to another branch within the CIA Group, and at least in part because of his new responsibilities, many of SCHULTE's administrator privileges on the LAN were revoked, and he was no longer permitted to serve as a systems administrator in the CIA Group's LAN.

15. At the same time, on or about April 4, 2016, SCHULTE's computer access to a specific developmental project ("Project-1") was also revoked. Until his reassignment, SCHULTE had been the CIA Group employee with principal responsibility for Project-1. Upon that transfer, principal responsibility for Project-1 was transferred to another CIA Group employee, who received computer access to Project-1.<sup>6</sup> I know from my review of publicly available material on the Internet, including WikiLeaks.org, that Project-1 was one of a small

---

<sup>6</sup> SCHULTE retained read-only access to Project-1 (but not the ability to alter the code) and the ability to copy the computer code associated with it in order to support another project for which he had responsibility.

group of CIA projects and capabilities that WikiLeaks highlighted explicitly by name in its March 7, 2017 press release that accompanied the online publication of the Classified Information.

16. On or about March 14, 2017, pursuant to a search warrant authorized by the Honorable Barbara Moses, Google, Inc., produced information, including a history of TARGET SUBJECT JOSHUA ADAM SCHULTE's Google searches (the "Google Search(es)" or "Search(es)").

17. Based on my review of those Google Searches, and conversations with law enforcement agents and others, as well as my own training and experience, I know that on or about April 4, 2016, SCHULTE conducted a Google Search that led him to visit a webpage entitled in part "Detecting USB insertion/Removal in C++ non-GUI application."<sup>7</sup> I understand, based on my training, experience, and conversations with others, that "Detecting USB insertion/[r]emoval" likely relates to the function by which a computer recognizes—or does not recognize—that an external device has been connected to it via its USB port. (A USB port is a standard connection interface used to connect devices to a computer, including—among numerous other peripheral items—a portable computer storage device.)

18. Based on my conversations with other law enforcement agents and others, and my review of documents, I understand that, one week later, on or about April 11, 2016, SCHULTE unilaterally, and without authorization, logged onto the CIA Group's LAN and reinstated his own administrator privileges.

---

<sup>7</sup> Both C++ and non-GUI (which stands for graphical user interface) are references to standard types of computer programming language or code, used, inter alia, by aspects of the LAN.

19. On or about April 12, 2016, in the evening<sup>8</sup> SCHULTE conducted Google Searches apparently designed to gather information about copying a large quantity of data from one computer storage device to another, including:

- a. “windows command line copy all files subdirectories”;
- b. “windows copy all files and subdirectories”; and
- c. “windows back files xcopy or robocopy” (4/13/16)

i. I understand, based on my training, experience, and conversations with others, that “robocopy” and “xcopy” each refer to computer commands that allow a user to copy multiple computer files—or entire computer directories (and all their contents)—from one computer storage location to another. For example, this command would be used to copy files and folders, *en masse*, from one network to another, from one computer to another, or from a computer network onto an portable hard drive.

ii. According to Microsoft, the “robocopy” function would allow a user “to mirror the contents of an entire folder hierarchy across local volumes or over a network. . . . Robocopy is a powerful tool, capable of moving, copying, and deleting files and folders faster than you can say ‘Whoops.’” In addition, the Robocopy command allows a user to copy an entire file storage directory sporadically, rather than all at one time. It does that by enabling the copying process to proceed in increments and re-start from where it left off, rather than requiring a user to start the copying process over again from the beginning.

20. On the following day, April 13, 2016, SCHULTE conducted Google Searches apparently designed to gather information about the speed of various portable, external computer

---

<sup>8</sup> The Google search warrant returns list the times of the searches in “UTC” or coordinated universal time, which is the same as Greenwich Mean Time. Accordingly, the dates and times enumerated herein have been adjusted to Eastern Standard Time.

hard drives, such as “thumb drives” and “flash drives,” which are computer memory storage devices that connect to a computer typically via a USB port.

a. Those Google Searches included:

- i. “thumbdrive copy speed”;
- ii. “flash drive transfer rate”; and
- iii. “flash drive read speeds”

b. On the same day, April 13, 2016, within minutes of conducting these Searches regarding portable hard drive speeds, SCHULTE also conducted another Google Search apparently designed to identify the most efficient way to copy units of computer data: “optimal reading chunk size c++”. I know, based on my training, experience and conversations with others, that:

i. Computers store, read and write data in units that are sometimes referred to as “blocks” or “chunks.” When data is copied, each block or chunk is separately read, copied and written from the original storage location to the destination storage location. These data blocks or chunks can be of varying sizes. Accordingly, the speed and efficiency of copying data can be affected by the size of each block or chunk of data.

ii. After conducting the above-mentioned Google Search (“optimal reading chunk size c++”), SCHULTE visited websites relating to issues such as “what is the ideal memory block size to use when copying.”

21. On or about April 14, 2016, CIA Group management discovered that SCHULTE had personally re-instituted his administrator privileges to the LAN without permission.

22. The following day, on or about April 15, 2016, SCHULTE conducted the following Google Search relating specifically to software running on the CIA Group’s LAN: “[

admin view restricted pages.”<sup>9</sup> After conducting the search, SCHULTE visited websites that related to ways to restrict the ability of even other Systems Administrators to view aspects of the LAN. (SCHULTE conducted the same search again thirteen days later, on or about April 28, 2016.)

23. On or about April 18, 2016, approximately three days later, SCHULTE received notice regarding CIA policies against personnel restoring their own access to privileges or computer networks after those accesses have been revoked. SCHULTE signed an acknowledgment that he understood that “individuals are not permitted to personally attempt and/or renew their previous authorizations [including administrator privileges] to any particular [computer] system.” That notice further instructed SCHULTE: “do not attempt to restore or provide yourself administrative rights to any project and/or system for which they have been removed.”

24. Also on or about April 18, 2016, SCHULTE conducted various Google Searches regarding copying files on a computer network, including “copying multiple [] large files.” After conducting this search, SCHULTE visited a website titled, in part, “how to copy a large number of files quickly between two servers.”

25. Less than a week later, on or about April 24, 2016, SCHULTE conducted a Google Search for a “SATA adapter.” Based on my training, experience and conversations with others, I understand that such an adapter is used to connect a computer hard drive to a computer externally, via USB connection. In other words, by connecting an internal drive to another

---

<sup>9</sup> The brackets redact out the proprietary name of the specific commercially available software program that was running on the CIA Group’s LAN.



computer via that computer's external USB port, a SATA adapter allows an internal computer hard drive to be used instead as a portable, external memory drive.

26. On or about April 24, 2016, SCHULTE conducted multiple Google Searches for how to "partition" or divide a computer hard drive up, in order to move files from one storage location on the computer to a separate drive or portioned location.

27. On or about April 28, 2016, SCHULTE again conducted a Google Search relating specifically to software running on the CIA Group's LAN: "[ ] admin view restricted pages," which was identical to the Search, described above, he conducted on April 15, 2016—four days after restoring his own administrator access to that very software program without authorization.

28. On the evening of Saturday, April 30, 2016, SCHULTE conducted numerous Google Searches apparently relating to the deletion of computer data, including possibly (and ineffectively) his own Google Searches.

a. These searches included the following:

- i. "google history";
- ii. "google view browsing history";
- iii. "western digital disk wipe utility"; and
- iv. "Samsung ssd wipe utility"

b. I know, based on my training, experience and conversations with others, that "[W]estern [D]igital" is the name of one of the largest providers of computer storage hardware (such as portable hard drives), and that "wipe utility," or wipe drive utilities are, based on the description on Western Digital's website, designed to "erase all the data on a hard drive."



c. I further know, based on my training, experience and conversations with others, that Samsung SSD is a reference to a brand (Samsung) of solid-state drives, which is a type of portable computer hard drive.

d. On March 15, 2017, the Honorable Barbara C. Moses issued a search warrant for a Manhattan apartment, in which SCHULTE has resided since shortly after his resignation from the CIA in November 2016. Pursuant to the search conducted on that same day, law enforcement officers recovered, among other things, the following, numerous computer storage devices with the capacity to store at least more than ten terabytes of data, including multiple Western Digital hard disk drives (themselves totaling multiple terabytes<sup>10</sup> of storage space) and at least one Samsung SSD solid state external hard drive.<sup>11</sup> As noted immediately above, these are the two brands of hard drive which SCHULTE specifically searched for “wipe utilities”—programs designed to completely erase data from the drives—on the evening of April 30, 2016.<sup>12</sup>

29. Approximately five hours after conducting the Google Searches regarding the wiping of hard drives—at approximately 3:20 a.m. in the early morning hours of May 1, 2016—SCHULTE visited a website entitled in part “how can I verify that a 1tb file transferred

---

<sup>10</sup> I know, based on my training, experience and conversations with others, that one terabyte of data is roughly equivalent to one-thousand gigabytes of data or one-million megabytes of data. Put differently, one terabyte of data is roughly equivalent to more than 85 million word processing pages.

<sup>11</sup> Those computer devices are in the process of being analyzed.

<sup>12</sup> In addition, pursuant to the search, agents recovered from SCHULTE’s apartment, internal correspondence from the CIA that appears, based on a preliminary analysis, to contain classified information (though *not* the Classified Information), including, *inter alia*, the names of CIA employees, and code names of specific CIA Group programs. I know, based on my training, experience and conversations with others, that removing and storing classified information in one’s own home is generally prohibited.

correctly.” I know, based on my training, experience and conversations with others, that “1tb” likely refers to 1 terabyte of data.

30. Three days later, on or about May 4, 2016, SCHULTE again conducted multiple Google Searches apparently related to the permanent deletion of data from a computer storage device, including “western digital disk wipe utility” and “can you use dban on ssd.” Based on my training, experience and conversations with others, I understand that:

- a. “SSD” is an acronym for “solid-state drive” a kind of computer memory storage device.
- b. “dban” is an acronym that stands for “Darik’s Boot and Nuke,” a computer software program that is designed, according to various websites selling the software, to “securely wipe[] the hard disks of most computers. DBAN is appropriate for bulk or emergency data destruction.” According to one popular technology website, CNET.com: “use DBAN only if you want to completely eradicate any trace of data on a hard drive. This is the ultimate in data shredding—there’s no recovery once you’ve used it.”

31. Starting two days later, May 6, 2016, and again on May 8, 2016, SCHULTE conducted multiple Google Searches apparently designed to research the anonymous transmission of data on the internet, through the use of “private trackers” which are non-public Internet sites set up to privately transfer large quantities of data from one computer to another, as well as via through “The Onion Router” or “TOR” which allows for anonymous communications on the Internet via a worldwide network of linked computer servers, and multiple layers of data encryption.

- a. On May 6, 2016, SCHULTE conducted multiple Google Searches apparently relating to ways to transfer data between computers anonymously, including searches

for “trackers,” “trackers torrent,” and “private trackers.” Based on my training, experience and conversations with others, I understand that trackers or torrent trackers are computer code (or a “protocol”) that connects computers on the Internet to each other in order to facilitate the transfer of large files over the Internet. I further understand that “private trackers” are trackers that are not publicly accessible, but rather that require authorization by an administrator to use the tracker to share files. After conducting the Google Search for “private trackers,” SCHULTE visited a website entitled “opentrackers.org” that claims that its private tracker can be used “to avoid detection & bypass anti-piracy/site blocking.”<sup>13</sup>

b. On May 8, 2016, SCHULTE conducted multiple Google Searches apparently related to the use of The Onion Router (or TOR) to anonymously transfer encrypted data on the Internet. For example, SCHULTE searched for “setup for relay,” “test bridge relay,” and “tor relay vs bridge.” Each of these searches returned information regarding the use of interconnected computers (or relays) on TOR to convey information, or the use of a computer to serve as the gateway (or bridge) into the TOR network of relays.

32. Less than three weeks later, on May 26, 2016, and notwithstanding the warnings described above, SCHULTE made an official request that he again be given full access to Project-1. Before receiving a response to that request, SCHULTE requested access from another employee who, apparently without proper vetting, granted SCHULTE the requested full access to Project-1. On the same day, SCHULTE used that newly obtained access to, unilaterally and without authorization, revoke the computer access permissions of all other CIA Group

---

<sup>13</sup> Trackers and torrent trackers are often used in the transfer of large media files, including video and audio. The investigation to date has indicated that, in addition to the activity set forth herein, SCHULTE also appears to have been engaged in the sharing of large media files, including movies and music. Accordingly, it is at least possible that certain of these searches, as well as others described herein, could relate to those activities.

employees to work on Project-1. Once this conduct was discovered, SCHULTE was issued a letter of warning that stated, “You were aware of the policy for access and your management’s lack of support for you to retain administrative privileges, but nonetheless you took steps to deliberately violate that policy and gain those privileges.” It continued by warning SCHULTE that any future violations would result in “further administrative action of a more severe nature.” After receiving the letter of warning, SCHULTE disagreed with some of its conclusions and consequently refused to sign the form.

33. A review of the Google Search history that has been obtained for SCHULTE indicates that for the approximately six years between at least August 2010, until August 3, 2016, he conducted no searches for WikiLeaks. But, beginning on August 4, 2016, SCHULTE initiated numerous Google Searches for WikiLeaks and related terms, and visited more than 200 pages that he apparently found as a result of those searches.

a. Between August 4 and August 22, 2016, SCHULTE conducted Searches for “wikileaks” at least eleven times. Pursuant to those Google Searches, he read dozens of articles regarding WikiLeaks, though he appears never to have actually visited the WikiLeaks.org Internet website.<sup>14</sup>

b. Between August 2016 and March 14, 2017, he searched “wikileaks” at least a dozen additional times, and read hundreds of online articles and publications regarding WikiLeaks. He apparently first visited the WikiLeaks.org website on March 7, 2017—the date of the release of the Classified Information.

---

<sup>14</sup> I know, based on my training, experience, and conversations with others, that, among many other reasons, one reason a person might search for “wikileaks” but never visit the website is because the act of visiting a website can leave a trail that a particular IP address visited the website. Accordingly, one reason (perhaps among many) for repeatedly searching “wikileaks” but not visiting the WikiLeaks.org website, would be to avoid leaving behind a footprint of one’s visit.

c. In addition to the numerous searches for “wikileaks” which commenced on August 4, 2016, SCHULTE also conducted multiple related Searches, including: prior to the March 7, 2017 release of the Classified Information, “assange” (Julian Assange is the founder and “editor-in-chief” of WikiLeaks.org), “snowden its time,” “wikileaks code,” and “wikileaks 2017”—and after the March 7, 2017 release of the Classified Information, “wikileaks public opinion,” and “officials were aware before the WikiLeaks release of a loss of sensitive information.”

34. On August 1, 2016, SCHULTE conducted a Google Search for “create temporary email,” and, three seconds later, visited the website [www.throwawaymail.com](http://www.throwawaymail.com). Based on my training, experience, conversations with others, and review of documents, I know that “throwawaymail.com” is an Internet website that randomly generates an anonymous email address for a user without any registration; that random and anonymous email address can immediately receive and send emails, but automatically expires within a very short period of time (approximately 48 hours).

35. On August 10, 2016, SCHULTE conducted a Search for “tails,” and then, two seconds later, visited the website “<https://tails.boum.org>.” I know, based on my training, experience, conversations with others, and review of that website, that “tails” is an acronym for “the Amnesic Incognito Live System,” that works in conjunction with TOR (described above) to ensure anonymous connections on the Internet and therefore will leave no digital footprint of the internet websites visited by someone using the system.<sup>15</sup> The WikiLeaks.org website also lists

---

<sup>15</sup> News reporting indicates that Edward Snowden used the tails system in connection with his transfer of allegedly classified documents to various news outlets. *See Out in the Open: Inside the Operating System Edward Snowden Used to Evade the NSA*, Wired, April 14, 2014, *available at* <https://www.wired.com/2014/04/tails/> (last accessed Mar. 31, 2017); *The ultra-secure Tails OS beloved by Edward Snowden gets a major upgrade*, PC World, Jan. 27, 2016, *available at* <http://www.pcworld.com/article/3026721/linux/the-ultra-secure-os-beloved-by-edward-snowden-gets-a-major-upgrade.html> (last accessed Mar. 31, 2017).

“tails” as one of its “partner organizations.”

36. Between mid-August and early September, SCHULTE conducted numerous searches regarding the following:

a. On August 14, 2016, filing a lawsuit against one’s boss (*e.g.* “can you sue your boss”), one’s employer (*e.g.* can i sue my employer for unfair treatment”), and the “EEOC.” (Less than an hour after conducting those Searches, SCHULTE searched “tor.”)

b. On September 1 and 5, 2016, SCHULTE repeatedly searched, “what is a mole.” I know, based on my training and experience that, among other meanings, a “mole” generally refers to a spy working inside a country’s security, military or intelligence services.

37. In approximately August 2016, as part of a standard background reinvestigation of SCHULTE for the purpose of renewing his security clearances, the CIA conducted interviews of multiple CIA Group colleagues. Among other things:

a. Some (but not all) colleagues independently reported that SCHULTE’s demeanor with his management and colleagues, and his commitment to his work, changed markedly for the worse in or around February 2016.

b. Multiple colleagues stated that SCHULTE had indicated that he felt aggrieved by the CIA in a number of respects. Some also reported that they believed SCHULTE to be untrustworthy and potentially subject to outside coercion. (Other colleagues made no such report and, indeed affirmatively reported that they believed that SCHULTE was, in fact, trustworthy.)

c. Some (but not all) colleagues also reported that SCHULTE’s security practices were lax, and that SCHULTE tended not to abide by security guidelines he deemed

inconvenient—particularly guidelines concerning when and what kinds of media or data (such as external drives) could be connected or uploaded to CIA computer systems.<sup>16</sup>

38. Based on my conversations with other law enforcement agents and others, my review of documents, and my training and experience, I know that, in connection with and preceding SCHULTE's November 2016 resignation from the CIA, he sent the following communications, among others:

a. Approximately one month prior to his resignation, on October 12, 2016, SCHULTE, using his CIA email account, sent an email to another CIA Group employee at that employee's official email account. The subject line of the email stated, "ROUGH DRAFT of Resignation Letter \*EYES ONLY\*." The email contained a letter entitled "Letter of Resignation 10/12/16" and addressed to "To whomever it may concern" ("Draft Resignation Letter"). I know from reviewing the Draft Resignation Letter, which spanned approximately three single-spaced pages, the following:

i. SCHULTE began the letter by stating, in substance and in part, that he had "always been a patriot" and would "obviously continue to support and defend this country until the day that I die," but that "from this day forward" he would "no longer do so as a public servant."

ii. SCHULTE claimed that he believed that the CIA Group management had unfairly "veiled" CIA leadership from various of SCHULTE's previously expressed concerns, including concerns about the network security of the CIA Group's LAN. SCHULTE continued: "That ends now. From this moment forward you can no longer claim

---

<sup>16</sup> As described herein, external drives can be connected to computers and files in order to allow users to move files from the computers onto the portable external drives.



ignorance; you can no longer pretend that you were not involved.”

iii. SCHULTE explained that he was resigning from the CIA because CIA Group management had, among other things, “ignored” issues he had raised about “security concerns” and had attempted to “conceal these practices from senior leadership,” including that the CIA Group’s LAN was “incredibly vulnerable” to the theft of sensitive data. He claimed that one named CIA Group manager had ignored his security concerns and “later attempt[ed] to evade responsibility and blame the decentralized and insecure [CIA Group computing] environment entirely on me.”<sup>17</sup>

iv. Specifically, SCHULTE wrote that inadequate CIA security measures had “left [the CIA Group’s LAN] open and easy for anyone to gain access and easily download [from the LAN] and upload [sensitive CIA Group computer code] in its entirety to the [public] internet.”

b. It appears that SCHULTE did not, in fact, submit the Draft Resignation Letter.

c. On his last day with the CIA (November 10, 2016), SCHULTE did, however, send an internal email to the CIA Office of the Inspector General (OIG) advising that office that he had been in contact with the United States House of Representatives’ Permanent Select Committee on Intelligence regarding his complaints about the CIA (the “OIG Email”).

i. In the OIG Email, which SCHULTE labeled “Unclassified,” SCHULTE raised many of the same complaints included in the draft “Letter of Resignation 10/12/16,” described above, including the CIA’s treatment of him and its failure to address the

---

<sup>17</sup> SCHULTE went on to describe other complaints he had about managers at the CIA. Among other things, SCHULTE described his complaints about the way in which CIA Group management had handled various personnel and disciplinary issues.



“security concerns” he had repeatedly raised in the past.

ii. Shortly thereafter, CIA security learned that one of SCHULTE’s colleagues had witnessed SCHULTE printing the OIG Email, placing it in a folder, and exiting the CIA Component facility where SCHULTE worked. Notwithstanding SCHULTE’s labeling of the email as “Unclassified,” the CIA subsequently determined that the OIG Email which SCHULTE removed from the CIA without authorization did, in fact, contain classified information.

39. The FBI recovered a copy of the November 10, 2016 OIG Email, which contained classified information and which SCHULTE labeled “Unclassified” and removed from a CIA facility, from his residence during the March 15, 2017 search.

**SCHULTE’s Use of the Target Cellphones**

40. On or about March 15, 2017, law enforcement officers seized a cellular telephone (“Phone-1”) from SCHULTE pursuant to a search warrant signed by the Honorable Barbara C. Moses. After officers seized Phone-1, SCHULTE was observed by law enforcement officers conducting surveillance going into a convenience store (the “Store”). After SCHULTE left the Store, Law enforcement officers subsequently went into the convenience store and confirmed with a cashier that SCHULTE had purchased a cellular telephone from the Store. After SCHULTE purchased the cellular telephone from the Store, he placed a call to his current employer in New York, New York (the “Employer”). Subsequently, the Employer informed the FBI that SCHULTE had contacted the Employer using Target Cellphone-2.

41. Based on my conversations with law enforcement officers involved in conducting surveillance of SCHULTE on or about March 17, 2017, I have learned, among other things, that during the evening of March 17, 2017, SCHULTE was observed entering an electronics store in

Manhattan. While inside the electronics store, SCHULTE was observed purchasing an item or items from a cashier (the "Cashier"). Law enforcement officers subsequently spoke with the Cashier who stated, among other things, that SCHULTE had purchased Target Cellphone-1. Specifically, the Cashier was able to confirm through documentation the phone number associated with Target Cellphone-1 and that the Service Provider for Target Cellphone-1 is Virgin Mobile USA LLC.

42. Based on my review of toll records for Target Cellphone-1 and Target Cellphone-2, I have learned, among other things, that both cellphones have been regularly used since their purchase on March 15, 2017 (Target Cellphone-2) and March 17, 2017 (Target Cellphone-1), respectively.

43. On or about March 16, 2017, FBI agents interviewed one of SCHULTE's former colleagues ("Individual-1") who works at the CIA. Following that interview, Individual-1 provided FBI agents with the number for Target Cellphone-3 as the number that he used to communicate with SCHULTE.

44. Based on my review of records provided by Sprint, I have learned, among other things, that Target Cellphone-3 is subscribed to in the name of SCHULTE; that Target Cellphone-3 was active between at least in or about January 2016 and in or about March 12, 2017; and that Sprint is the Service Provider for Target Cellphone-3. Based on my review of Phone-1, I have learned, among other things, that the number for Target Cellphone-3 is one of the numbers associated with Phone-1.

45. For these reasons, I submit that there is probable cause to believe that SCHULTE is using Target Cellphone-1 and Target Cellphone-2 and that the Requested Information will assist law enforcement in monitoring his whereabouts, including when he travels to Texas. Moreover,

prospective location information (and historical location information) concerning Target Cellphone-1 and Target Cellphone-2 will likely assist law enforcement agents in identifying individuals that SCHULTE meets with and locations that SCHULTE frequents potentially in furtherance of the Subject Offenses.


46. For the foregoing reasons, I also submit that there are reasonable grounds to believe that the historical location information for Target Cellphone-3 is relevant and material to an ongoing criminal investigation. Specifically, historical location information for Target Cellphone-3 will likely assist law enforcement agents in identifying past locations that SCHULTE frequented potentially in furtherance of the Subject Offenses. Historical location information will also help to identify SCHULTE's whereabouts at times when the Classified Information may have been removed from the Agency and/or distributed to third parties.

### **III. Request for Warrant and Order**

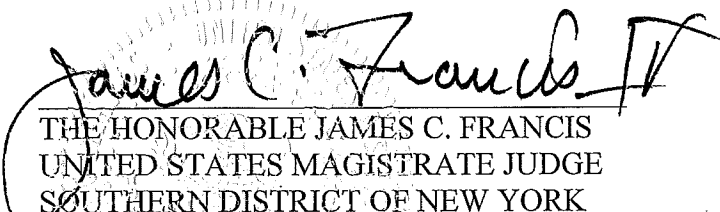
47. Based on the foregoing I respectfully request that the Court require the Service Providers to provide the Requested Information as specified further in the Warrant and Order proposed herewith, including prospective precision location and cell site data for Target Cellphone-1 and Target Cellphone-2 for a period of 45 days from the date of this Order; historical cell site data and toll records (i) for Target Cellphone-1 and Target Cellphone-2 for the period from March 15, 2017 to the present and (ii) for Target Cellphone-3 for the period from January 1, 2016 through March 12, 2017; and pen register information for Target Cellphone-1 and Target Cellphone-2 for a period of 60 days from the date of this Order.

48. **Nondisclosure.** The existence and scope of this ongoing criminal investigation are not publicly known. As a result, premature public disclosure of this affidavit or the requested Warrants and Orders could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation.

Accordingly, I respectfully request that the Providers be directed not to notify the subscriber or others of the existence of the Warrants and Orders for a period of 180 days, and that the Warrant and Order and all supporting papers be maintained under seal until the Court orders otherwise, as specified in the Application submitted in conjunction with this Affidavit.

  
\_\_\_\_\_  
SARA E. LANGENDERFER  
Special Agent  
Federal Bureau of Investigation

Sworn to before me this  
31st day of March, 2017

  
\_\_\_\_\_  
THE HONORABLE JAMES C. FRANCIS  
UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF NEW YORK