

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the
District of Massachusetts

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

1841 Maple Street, North Dighton, MA 02764 and any
electronic devices found within as
Described in Attachment B

Case No. 23-4242-DHH

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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-1 attached hereto and incorporated herein for all purposes.

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

See Attachment B attached hereto and incorporated herein by reference for all purposes.

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

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

The search is related to a violation of:

Table with 2 columns: Code Section, Offense Description. Row 1: 18 U.S.C. §§ 793(b), 793(d), 793(e), and 18 U.S.C. § 1924; Unauthorized removal, retention, and transmission of classified documents or material

The application is based on these facts:
See attached affidavit of SA Victoria Horne

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

Victoria Horne / SA
Applicant's signature
Victoria Horne, FBI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephone (specify reliable electronic means).

Date: 04/13/2023

David H. Hennessy
Judge's signature
Hon. David H. Hennessy, U.S. Magistrate Judge
Printed name and title
[Seal of the United States District Court, District of Massachusetts]

City and state: Boston, Massachusetts

**AFFIDAVIT OF SPECIAL AGENT VICTORIA HORNE IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Victoria Horne, state:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation and have been since April 2021. As a Special Agent, I have received training at the FBI Academy located in Quantico, Virginia, including training on investigative methods and training specific to counterintelligence and espionage investigations. I am currently assigned to a squad at the FBI Washington Field Office, Counterintelligence Division, where I primarily investigate counterintelligence and espionage matters. During the course of these investigations, I have conducted or participated in witness and subject interviews, service of subpoenas, the execution of search and arrest warrants, physical surveillance, the seizure of evidence, including computer, electronic, and email evidence, as well as requested and reviewed pertinent records. Based on my experience and training, I am familiar with the requirements for the handling of classified documents and information. I am also familiar with the methods used by individuals engaged in the unlawful use or disclosure of classified information, including national defense information.

2. I am currently investigating Jack Douglas Teixeira (“TEIXEIRA”) for the Unauthorized Removal, Retention, and Transmission of Classified Documents or Material, in violation of 18 U.S.C. § 793(b), (d), and (e) and/or 18 U.S.C. § 1924 (the “SUBJECT OFFENSES”).

3. This affidavit is being submitted in support of applications for warrants to search the premises known as 1841 Maple Street, North Dighton, MA 02764 (“SUBJECT PREMISES 1”) further described in Attachment A-1; the premises known as 106 Walker Street, North

Dighton, MA 02764 (“SUBJECT PREMISES 2”), further described in Attachment A-2; a 2016 Chevrolet Colorado with Massachusetts plate number 2BFD25 (the “SUBJECT VEHICLE”), further described in Attachment A-3; a Motorola Ultra 108MP cellular phone further described in Attachment A-4, and the contents of any additional electronic devices found in the locations in Attachments A-1 and A-2 and A-3, for the records and items described in Attachment B.

4. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested search warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE TO BELIEVE THAT A FEDERAL CRIME WAS COMMITTED

Statutory Authorities and Definitions

5. Pursuant to 18 U.S.C. § 793(b), “[w]hoever . . . copies, takes, makes, or obtains, or attempts to copy, take, make or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense” shall be fined or imprisoned not more than ten years, or both.

6. Pursuant to 18 U.S.C. § 793(d), “[w]hoever, lawfully having possession of, access to, control over, or being entrusted with any document . . . or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or

willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it” shall be fined or imprisoned not more than ten years, or both.

7. Pursuant to 18 U.S.C. § 793(e), “[w]hoever having unauthorized possession of, access to, or control over any document . . . relating to the national defense . . . willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted” or attempts to do or causes the same “to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it” shall be fined or imprisoned not more than ten years, or both.

8. Pursuant to 18 U.S.C. § 1924, it is illegal for any officer, employee, contractor, or consultant of the United States, who, by virtue of his/her office, employment, position, or contract, becomes possessed of documents or materials containing classified information, to knowingly remove such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location.

9. Under Executive Order 13526, the unauthorized disclosure of material classified at the “TOP SECRET” level (“TS”), by definition, “reasonably could be expected to cause exceptionally grave damage to the national security” of the United States. Exec. Order 13526 § 1.2(a)(1), 75 Fed. Reg. 707, 707–08 (Jan. 5, 2010). The unauthorized disclosure of information classified at the “SECRET” level (“S”), by definition, “reasonably could be expected to cause serious damage to the national security” of the United States. Exec. Order 13526 § 1.2(a)(2). The unauthorized disclosure of information classified at the “CONFIDENTIAL” level (“C”), by definition, “reasonably could be expected to cause damage to the national security” of the United States. Exec. Order 13526 § 1.2(a)(3).

10. Sensitive Compartmented Information (“SCI”) means classified information concerning or derived from intelligence sources, methods, or analytical processes, which is further restricted, with the requirement that it be handled within formal access control systems established by the Director of National Intelligence.

11. Classified information may be marked as “Not Releasable to Foreign Nationals/Governments/Non-US Citizens,” abbreviated “NOFORN,” to indicate information that may not be released in any form to foreign governments, foreign nationals, foreign organizations, or non-U.S. citizens without permission of the originator.

12. Classified information may also be marked as “Originator Controlled,” abbreviated “ORCON.” This marking indicates that dissemination beyond pre-approved U.S. entities requires originator approval.

13. Classified information of any designation may be shared only with persons determined by an appropriate United States Government official to be eligible for access, and who possess a “need to know.” Among other requirements, for a person to obtain a security clearance allowing that person access to classified United States Government information, that person is required to and must agree to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations. If a person is not eligible to receive classified information, classified information may not be disclosed to that person. In order for a foreign government to receive access to classified information, the originating United States agency must determine that such release is appropriate.

14. Pursuant to Executive Order 13526, classified information contained on automated information systems, including networks and telecommunications systems that collect, create, communicate, compute, disseminate, process, or store classified information must be maintained in a manner that: (1) prevents access by unauthorized persons; and (2) ensures the integrity of the information.

15. 32 C.F.R. Parts 2001 and 2003 regulate the handling of classified information. Specifically, 32 C.F.R. § 2001.43, titled “Storage,” regulates the physical protection of classified information. This section prescribes that SECRET and TOP SECRET information “shall be stored in a GSA-approved security container, a vault built to Federal Standard (FHD STD) 832, or an open storage area constructed in accordance with § 2001.53.” It also requires periodic inspection of the container and the use of an Intrusion Detection System, among other things.

Overview

16. The FBI is currently investigating the unauthorized disclosure of more than 40 images on internet sites including a U.S. social media platform (“Social Media Platform 1”)¹, which contain various classification markings, including documents marked at the “TOP SECRET” level, and which appear to depict U.S. Government classified national defense information (the “Government Information”).

17. As set forth in further detail below, TEIXEIRA is a current employee of the United States Air Force National Guard (“USAFNG”) who possesses a security clearance at the TS//SCI level by virtue of his employment with USAFNG. TEIXEIRA is stationed at Otis Air

¹ Social Media Platform 1 is a VOIP and instant messaging social platform. Users of Social Media Platform 1 have the ability to communicate with voice calls, video calls, text messaging, and can post media and files in private chats or as part of communities called “servers.” A Social Media Platform 1 server is a collection of persistent chat room and voice channels, which can be accessed via invitation.

National Guard Base in Massachusetts, where he has access to classified information systems. According to badge access logs, TEIXEIRA badged into the base as recently as April 12, 2023.

18. As described further below, there is probable cause to believe that TEIXEIRA posted Government Information onto Social Media Platform 1 (“Server 1”) from approximately December 2022 to March 2023. Specifically, there is probable cause to believe that TEIXEIRA uploaded an image of a classified document (the “Government Document”) to Server 1 using a particular username associated with TEIXEIRA (the “TEIXEIRA Username”). The Government Document describes the status of the Russia-Ukraine conflict, including troop movements, on a particular date. The Government Document is based on sensitive U.S. intelligence, gathered through classified sources and methods and contains national defense information. A subject matter expert has confirmed that the Government Document is classified at the TS//SCI level.

TEIXEIRA’S Background

19. TEIXEIRA is currently serving as an E-3/Airman First Class in the USAFNG and is stationed at Otis Air National Guard Base. TEIXEIRA has held that rank since May 2022 and enlisted in the Air National Guard in September 2019 as an E-1 rank. As of February 2023, TEIXEIRA’s title was Cyber Defense Operations Journeyman.

20. As required for this position, TEIXEIRA holds a Top Secret security clearance, which was granted in 2021. Based on my training and experience, I know that to acquire his security clearance, TEIXEIRA would have signed a lifetime, binding non-disclosure agreement in which he would have had to acknowledge that the unauthorized disclosure of protected information could result in criminal charges.

21. In addition to TEIXEIRA's Top Secret clearance, he maintained sensitive compartmented access (SCI) to other highly classified programs. He has also had this access since 2021.

22. TEIXEIRA's security clearance paperwork lists his primary address as SUBJECT PREMISES 1. TEIXEIRA's security clearance paperwork also indicates that he lived at SUBJECT PREMISES 2, while his parents lived together until approximately 2009. As recently as April 13, 2023, FBI surveillance personnel witnessed TEIXEIRA entering and exiting SUBJECT PREMISES 1. Additionally, TEIXEIRA was seen departing from the driveway of SUBJECT PREMISES 2 on April 13, 2023.

23. TEIXEIRA's security clearance paperwork lists his phone number as 508-822-2006. According to the Massachusetts Department of Motor Vehicles, TEIXEIRA resides at SUBJECT PREMISES 1 and drives a vehicle with Massachusetts license plate number 2BFD25. Additionally, FBI agents observed TEIXEIRA driving the SUBJECT VEHICLE as recently as April 13, 2023. Your affiant believes that TEIXEIRA currently has his primary residence at SUBJECT PREMISES 1 because he listed that address in his Record of Emergency Data with his employer, has this address listed with the Massachusetts Department of Motor Vehicles, and FBI Surveillance observed TEIXEIRA at the Maple Street residence as recently as April 13, 2023. In addition, agents executed an arrest outside of SUBJECT PREMISES 1 on that same date.

TEIXEIRA Transmits National Defense Information on Social Media Platform 1

24. On or about April 10, 2023, the FBI interviewed another user of Social Media Platform 1 ("User 1"). According to User 1, an individual began posting purportedly classified information on Social Media Platform 1 on or about December 2022 on a specific server

(“Server 1”). Social Media Platform 1 users can create a “server” for free and then invite other users to join the server to communicate with each other. A server can be configured as public, meaning anyone can join, or it can be configured to be private. To participate in a private server, a user must be invited by another user who already belongs to that private server.

25. Server 1 had approximately 50 members, and User 1 indicated that the purpose of Server 1 was to discuss geopolitical affairs and current and historical wars.

26. According to User 1, an individual using the TEIXEIRA Username began posting paragraphs of text on Server 1 in December 2022, which contained information about the war in Ukraine. In or around January 2023, the TEIXEIRA Username began posting pictures of documents on Server 1 that contained U.S. classification markings.

27. According to User 1, User 1 spoke to the individual using the TEIXEIRA Username at various times using a video chat application, voice calls, or the chat function on Server 1. User 1 described the user of the TEIXEIRA Username as an individual named Jack who lived in Massachusetts and stated that Jack was in the USAFNG. User 1 further described the individual as a white male who was clean cut and between 20 and 30 years old.

28. On April 13, 2023, User 1 identified TEIXEIRA’s Department of Motor Vehicles photo from a photo lineup, and identified TEIXEIRA as the individual who User 1 communicated with on multiple occasions by video, voice, and computer chats on Social Media Platform 1, who used the TEIXEIRA Username in question, and who admitted to posting documents on Social Media Platform 1.

29. User 1 also recalled that, during one of the conversations with TEIXEIRA on Social Media Platform 1, TEIXEIRA, using the TEIXEIRA username, explained that he had become concerned that he may be discovered making the transcriptions of text in the workplace,

which is why TEIXEIRA began taking the documents to his residence and posting photographs of the documents on Server 1, instead of posting the paragraphs of text.

30. On or about April 12, 2023, Social Media Platform 1 provided the FBI with records pursuant to legal process, which included records related to User 1's Social Media Platform 1 Account as well as the subscriber information for the administrator of Server 1 to which User 1 belonged. According to Social Media Platform 1 Records, the administrator of Server 1 is the individual using the TEIXEIRA Username. Additionally, according to Social Media Platform 1, the billing name for the TEIXEIRA Username is Jack Teixeira with a billing address of SUBJECT PREMISES 1. As a result, there is probable cause to believe that the individual using the TEIXEIRA Username is TEIXEIRA.

31. The Government Document was accessible to TEIXEIRA by virtue of his employment with USAFNG. According to a U.S. Government Agency ("USG Agency 1"), which has access to logs of certain documents TEIXEIRA accessed, TEIXEIRA accessed the Government Document in February 2023. A subject matter expert reviewed information in the Government Document and determined that certain of the information is classified at the TOP SECRET//SCI level. As described above, TOP SECRET information "reasonably could be expected to cause exceptionally grave damage to the national security" of the United States. Exec. Order 13526 § 1.2(a)(1), 75 Fed. Reg. 707, 707-08 (Jan. 5, 2010).

32. By virtue of his access to Server 1, where the Government Information was originally posted, User 1 had access to the Government Document and subsequently reposted the Government Document on a separate social media website ("Social Media Platform 2").

33. User 1 also recalled that TEIXEIRA shared a video of himself shooting a Tokarev. Your affiant knows that a Tokarev is an out-of-production Soviet semi-automatic

pistol that was used throughout World War II. Your affiant also knows that another resident of SUBJECT PREMISES 1 is a collector of historical weaponry.

34. As part of my investigation, I also reviewed the original images of Government Information that were reposted by User 1 on Social Media Platform 2. In the background of one of those original images – behind the photograph of the Government Information – I observed a pamphlet with information about a spotting scope, a type of scope typically used for hunting, that I know to be sold by a specific online retailer of gun optics, night vision devices, and trail cameras, among other items. Your affiant has reason to believe that such a hunting scope may, therefore, be in the possession of TEIXEIRA.

THE PREMISES CONTAINS EVIDENCE, FRUITS, AND INSTRUMENTALITIES

35. I also have probable cause to believe that the premises to be searched contain fruits, evidence, and instrumentalities of violations of the federal statutes listed above, as described in Attachment B.

36. On April 13, 2023, Social Media Platform 1 provided the FBI subscriber information for a particular User ID associated with the TEIXEIRA Username, which belonged the administrator for the Server 1, jointly utilized by User 1. The billing name for that User ID was “JACK TEIXEIRA” and the billing street was listed as 1841 Maple Street, North Dighton, Massachusetts (SUBJECT PREMISES 1).

37. Additionally, on April 13, 2023, the FBI conducted surveillance on TEIXEIRA. During the course of the surveillance, TEIXEIRA drove his vehicle, a 2016 red Chevrolet Colorado bearing Massachusetts license plate 2BFD25 (MA-2BFD25), to SUBJECT PREMISES 1. TEIXEIRA parked MA-2BFD25 in the vicinity of SUBJECT PREMISES 1 and subsequently entered SUBJECT PREMISES 1. Earlier in the day, the FBI surveillance team witnessed

TEIXEIRA leaving the driveway of SUBJECT PREMISES 2.

38. In addition, Massachusetts's Department of Motor Vehicles returns reflect that JACK DOUGLAS TEIXEIRA's mailing address was 1841 Maple Street, North Dighton, Massachusetts, 02764, the address associated with SUBJECT PREMISES 1.

39. Further, the owner of record of 106 Walker Street, North Dighton, MA 02764, the address associated with SUBJECT PREMISES 2 is a person with the same legal name as TEIXEIRA. TEIXERA was observed leaving the driveway of SUBJECT PREMISES 2 on April 13, 2023 before driving to SUBJECT PREMISES 1, where he was subsequently arrested. Since the time of that arrest, law enforcement has secured SUBJECT PREMISES 1 in anticipation of a search warrant. Additionally, law enforcement has been surveilling SUBJECT PREMISES 2 in anticipation of a search warrant.

40. After TEIXEIRA was arrested on April 13, 2023, law enforcement spoke with an occupant of SUBJECT PREMISES 1. That individual consented to law enforcement retrieval of three cellular telephones from SUBJECT PREMISES 1. The individual identified the cellular telephone described in Attachment A-4 as belonging to TEIXEIRA.

SEIZURE OF COMPUTER EQUIPMENT AND DATA

41. From my training, experience, and information provided to me by other agents, I am aware that individuals frequently use computers to create and store records of their actions by communicating about them through e-mail, instant messages, and updates to online social-networking websites; drafting letters; keeping their calendars; arranging for travel; storing pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online.

42. Based on my training, experience, and information provided by other law enforcement officers, I know that many cell phones (which are included in Attachment B's definition of "hardware"), including iPhones, can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications that reveal or suggest who possessed or used the device.

43. I am aware of a report from the United States Census Bureau that shows that in 2016, among all households nationally, 89 percent had a computer, which includes smartphones, and 81 percent had a broadband Internet subscription. Specifically, in 2016, when the use of smartphone ownership was measured separately for the first time, 76 percent of households had a smartphone and 58 percent of households had a tablet, and 77 percent of households had a desktop or laptop computer. Further, according to the Pew Research Center, as of 2019, 96 percent of adult Americans own a cellphone, and 81 percent own a cellphone with significant computing capability (a "smartphone"). The percentage of adults that own a smartphone is even higher among younger demographic groups: 96 percent of 18-29 year olds, 92 percent of 30-49 year olds, and 79 percent of 50-64 year olds owned smartphones in 2019.

44. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

- a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.
- b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media -- in particular, computers’ internal hard drive -- contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.
- d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed

Internet pages or if a user takes steps to delete them.

e. Data on a storage medium 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 traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords.

Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

f. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the

computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the

computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

g. 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.

h. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium 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, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

i. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a

particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

45. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

- a. The volume of evidence: storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.
- b. Technical requirements: analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer

hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even “hidden,” deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a “booby trap.”

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

46. The premises may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner’s knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

47. The law enforcement agents will endeavor to search and seize only the computer

equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B because they are associated with (that is used by or belong to) TEIXEIRA . If however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

CONCLUSION

48. Based on the information described above, I have probable cause to believe that TEIXEIRA has violated 18 U.S.C. § 793(b), (d), and (e) and 18 U.S.C. § 1924.

49. Based on the information described above, I also have probable cause to believe that evidence, fruits, and instrumentalities of these crimes, as described in Attachment B, are contained within the premises described in Attachments A-1, A-2, A-3, and A-4.

50. Additionally, the government requests permission to execute the searches at any time of the day or night. Specifically, the government believes there is good cause based upon on User 1's representation that TEIXEIRA took classified information home to photograph it. As a result, there is reason to believe that additional classified information is currently being stored in an unsecure manner at SUBJECT PREMISES 1 and/or SUBJECT PREMISES 2. Based upon a review of what appears to be Government Information containing classification portion markings which has been disseminated by User 1 and which User 1 states originated with TEIXEIRA, and a review of source documents, there is reason to believe that TEIXEIRA accessed larger amounts of classified national defense information and only disseminated select pages of larger documents. Although certain information has been posted on various social

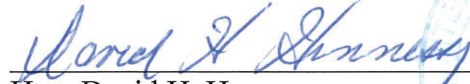
media sites, there is good cause to believe that additional, highly sensitive documents containing classified U.S. national defense information will be found at the SUBJECT PREMISES.

Sworn to under the pains and penalties of perjury,


Victoria Horne Special Agent, Federal
Bureau of Investigation

Subscribed and sworn to before me via telephone on April 13, 2023.

10:52 PM


Hon. David H. Hennessy
United States Magistrate Judge

