

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF GEORGIA
AUGUSTA DIVISION

IN THE MATTER OF THE SEARCH OF:)
)
1957 BATTLE ROW,)
AUGUSTA, GA 30904 and)
A LIGHT COLOR NISSAN CUBE WITH)
VIN JN8AZ2KR0CT254476, and the person)
of REALITY LEIGH WINNER)

Case No. 1:17mj24

Filed Under Seal

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

I, Justin C. Garrick, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 1957 Battle Row, Augusta, GA 30904, hereinafter "PREMISES," further described in Attachment A; a light-colored Nissan Cube with VIN JN8AZ2KR0CT254476, hereinafter "VEHICLE"; and the person of REALITY LEIGH WINNER, hereinafter "WINNER," for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") assigned to the Atlanta division, and have been since 2008. During this time, I have received training at the FBI Academy located at Quantico, Virginia, specific to counterintelligence and espionage investigations. I currently am assigned to investigate counterintelligence and espionage matters. Based on my experience and training, I am familiar with efforts used to unlawfully collect and disseminate sensitive government information, including national defense information.

3. There is probable cause to believe that the PREMISES, VEHICLE, and WINNER's

person contain evidence, contraband, fruits, and/or other items illegally possessed in violation of 18 U.S.C. § 793(e).

4. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation, and information from other FBI and U.S. Government personnel. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

STATUTORY AUTHORITY AND DEFINITIONS

5. For the reasons set forth below, I believe that there is probable cause to believe that the PREMISES, VEHICLE, and WINNER's person contain evidence, contraband, fruits, and/or other items illegally possessed in violation of Title 18, United States Code, Section 793(e) (the "Subject Offense").

6. Under 18 U.S.C. § 793(e), "whoever having unauthorized possession of, access to, or control over any document . . . 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 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.

7. Under Executive Order 13526, information in any form may be classified if it: (1) is owned by, produced by or for, or is under the control of the United States Government; (2) falls

within one or more of the categories set forth in the Executive Order [Top Secret, Secret, and Confidential]; and (3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security.

8. Where such unauthorized disclosure could reasonably result in damage to the national security, the information may be classified as "Confidential" and must be properly safeguarded. Where such unauthorized disclosure could reasonably result in serious damage to the national security, the information may be classified as "Secret" and must be properly safeguarded. Where such unauthorized disclosure could reasonably result in exceptionally grave damage to the national security, the information may be classified as "Top Secret" and must be properly safeguarded.

9. 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, in order 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.

10. 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.

11. 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.

PROBABLE CAUSE

12. As set forth in further detail below, WINNER is under investigation for printing and improperly removing and transmitting classified material from an Intelligence Community Agency (the “U.S. Government Agency”) on or about May 9, 2017, and passing the classified material to an online news outlet (the “News Outlet”). WINNER is a contractor with Pluribus International Corporation assigned to a U.S. Government Agency facility in Georgia. She has been employed at the facility since on or about February 13, 2017. From January 2013 until her employment with Pluribus International Corporation, WINNER was an active duty member of the U.S. Air Force and held a Top Secret clearance.

13. On June 1, 2017, the FBI was notified by the U.S. Government Agency that the U.S. Government Agency had been contacted by the News Outlet on May 30, 2017, regarding an upcoming story. The News Outlet informed the U.S. Government Agency that it was in

possession of what it believed to be a classified document authored by the U.S. Government Agency. The News Outlet provided the U.S. Government Agency with a copy of this document. Subsequent analysis by the U.S. Government Agency confirmed that the document in the News Outlet's possession is intelligence reporting dated on or about May 5, 2017 (the "intelligence reporting"). This intelligence reporting is classified at the Top Secret level, indicating that its unauthorized disclosure could reasonably result in exceptionally grave damage to the national security, and is marked as such. The U.S. Government Agency has since confirmed that the reporting contains information that was classified at that level at the time that the reporting was published on or about May 5, 2017, and that such information currently remains classified at that level.

14. The U.S. Government Agency examined the document shared by the News Outlet and determined the pages of the intelligence reporting appeared to be folded and/or creased, suggesting they had been printed and hand-carried out of a secured space.

15. The U.S. Government Agency conducted an internal audit to determine who accessed the intelligence reporting since its publication. The U.S. Government Agency determined that six individuals printed this reporting. These six individuals included WINNER. A further audit of the six individuals' desk computers revealed that WINNER had e-mail contact with the News Outlet. The audit did not reveal that any of the other individuals had e-mail contact with the News Outlet.

16. The U.S. Government Agency determined that WINNER had e-mail communication with the News Outlet on or about March 30, 2017, and March 31, 2017. The first e-mail was from WINNER, using e-mail address da3re.fitness@gmail.com, to the News Outlet.

In it, WINNER appeared to request transcripts of a podcast. The second e-mail was from the News Outlet to da3re.fitness@gmail.com and confirmed WINNER's subscription to the service. The da3re.fitness@gmail.com account is a personal e-mail account not sponsored by or affiliated with the U.S. Government Agency.

17. On or about May 9, 2017, four days after the publication of the classified report, WINNER conducted searches on the U.S. Government Agency's classified system for certain search terms, which led WINNER to identify the intelligence reporting. On or about May 9, 2017, WINNER also printed the intelligence reporting. A review of WINNER's computer history revealed she did not print any other intelligence report in May 2017.

18. At all times relevant to this affidavit, WINNER has maintained an active Top Secret clearance. The U.S. Government Agency confirmed that although WINNER had the required access to search for and view the intelligence reporting, the information contained in the intelligence reporting is unrelated to her job duties, and WINNER therefore does not possess a "need to know."

19. On or about May 24, 2017, a reporter for the News Outlet (the "Reporter") contacted another U.S. Government Agency affiliate with whom he has a prior relationship. This individual works for a contractor for the U.S. Government (the "Contractor"). The Reporter contacted the Contractor via text message and asked him to review certain documents. The Reporter told the Contractor that the Reporter had received the documents through the mail, and they were postmarked "Augusta, Georgia." WINNER resides in Augusta, Georgia. The Reporter believed that the documents were sent to him from someone working at the location where WINNER works. The Reporter took pictures of the documents and sent them to the Contractor.

The Reporter asked the Contractor to determine the veracity of the documents. The Contractor informed the Reporter that he thought that the documents were fake. Nonetheless, the Contractor contacted the U.S. Government Agency on or about June 1, 2017, to inform the U.S. Government Agency of his interaction with the Reporter. Also on June 1, 2017, the Reporter texted the Contractor and said that a U.S. Government Agency official had verified that the document was real. When questioned about what intelligence report number was associated with the images on his phone, the Contractor supplied the reporting number associated with the intelligence reporting at issue.

20. On May 27 to 29, 2017, WINNER traveled outside the United States to Belize in Central America. WINNER provided notice to the U.S. Government Agency in March 2017 of her intent to travel to Belize in May 2017. The purpose of WINNER's travel and her activities while abroad are unknown.

21. WINNER resides at the PREMISES, as verified on June 2, 2017, by her Driver's License address and two utility billing addresses. Additionally, WINNER owns and drives a light-colored Nissan Cube with VIN JN8AZ2KR0CT254476, as verified by the vehicle registration information. Agents viewed a light-colored Nissan Cube parked at the PREMISES on June 2, 2017, and witnessed WINNER traveling in the VEHICLE in Augusta, Georgia, on June 3, 2017. I confirmed on June 2, 2017, that WINNER has a cellular phone serviced by Cingular/AT&T. In my training and experience, people typically store their electronics and correspondence (including letters or printed emails) in their homes and transport them in their vehicles. I also know that people typically carry small electronic storage devices and communication devices, such as thumb drives and cellular phones, on their person. There is thus

probable cause to believe that intelligence reporting and evidence of correspondence between WINNER and the News Outlet, among other items of evidentiary value, may be found inside the PREMISES and the VEHICLE, as well as on storage and communication devices on WINNER's person. Moreover, there is probable cause to believe that evidence of communications between WINNER and the News Outlet, among other items of evidentiary value, will be found on WINNER's electronic devices at the PREMISES, in the VEHICLE, and on WINNER's person.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

22. As described in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in the VEHICLE, and on WINNER's person, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

23. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, in the VEHICLE, or on WINNER's person, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when 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.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, that is, in space on the storage medium that is not currently being used by an active file .. for long periods of time before they are overwritten. 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 drives - contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic 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. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

24. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe

that this forensic electronic evidence will be on any storage medium in the PREMISES, in the VEHICLE, or on WINNER's person because:

- a. Data on the 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, e-mail 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.
- b. 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).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a 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.
- e. 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.

25. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises or vehicle for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises or vehicle, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.
- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

26. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

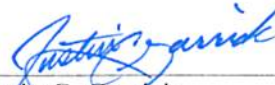
CONCLUSION

27. I submit that this affidavit supports probable cause for a warrant to search the PREMISES, the VEHICLE, and the PERSON described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING

28. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation and the FBI has not yet identified all potential criminal confederates nor located all evidence related to its investigation. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness by allowing criminal parties an opportunity to flee, destroy evidence (stored electronically and otherwise), change patterns of behavior, and notify criminal confederates.

Respectfully submitted,



Justin C. Garrick
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on June 3, 2017:



THE HONORABLE BRIAN K. EPPS
UNITED STATES MAGISTRATE JUDGE