UNITED STATES DISTRICT COURT

for the
District of Minnesota

In the Matter of the Search of:

THE OFFICE LOCATED AT THE MINNEAPOLIS-ST. PAUL INTERNATIONAL AIRPORT IN ROOM G-1141-07

SEALED BY ORDER OF THE COURT

Case No. 17-MJ-670 (DTS)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

THE OFFICE LOCATED AT THE MINNEAPOLIS-ST. PAUL INTERNATIONAL AIRPORT IN ROOM G-1141-07

located in the State and District of Minnesota, there is now concealed: **See attached list of items to be seized, Attachment B.**

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:

Code Section	*Offense Description*
Title 18 United States Code, Section 793(e)	Unauthorized Possession of, Access to, or Control Over Any Document or Information;
Title 18 United States Code, Section 1924	Removal of Documents Without Authority by Officer of the United States

The application is based on these facts: **See attached Affidavit.**

X Continued on the attached sheet.

Applicant's Signature

Matthew T. Pietropola, Special Agent, FBI
Printed Name and Title

Sworn to before me and signed in my presence.

Date: 8/28/17

Judge's Signature

City and State: Minneapolis, MN

The Honorable David T. Schultz, United States Magistrate Judge
Printed Name and Title

ATTACHMENT B

Property to be seized

1. All documents and records relating to violations of 18 U.S.C. § 793(e) (gathering, transmitting or losing defense information), and 18 U.S.C. § 1924 (unlawful removal or retention of classified information), including:

a. Notebooks or documents, records, or papers containing information relating to the national defense and/or classified information;

b. Information pertaining to others who possess classified information, including information pertaining to their location;

c. Information pertaining to any others who conspired with Terry James Albury to release, communicate, or transmit national defense information and/or classified information;

d. Computer hardware, computer software, passwords and data security devices, cameras (including digital and video), telephones, handheld devices, computer related documentation, and other digital and electronic media, including storage devices that may have been used to store or transmit classified information.

e. Records or documents evidencing ownership or use of computer hardware, computer software, telephones, cameras, handheld devices, electronic media

and electronic storage devices, including sales receipts, bills for Internet access, and handwritten notes.

f. Miscellaneous papers, magazines, books, or any other pocket litter, especially that which may contain handwriting, computer-generated text or highlighted sections.

g. Items containing potential passwords or passphrases;

h. Information identifying persons or entities, who have been involved in violations of 18 U.S.C. § 793(e) (gathering, transmitting or losing defense information), and 18 U.S.C. § 1924 (unlawful removal or retention of classified information), including communications, financial transactions, and data exchange with or between such persons, or photographs of such persons.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords,

documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA
Case No. 17-MJ-670 (DTS)

IN THE MATTER OF THE SEARCH INVOLVING TERRY ALBURY	))))	**SEALED BY ORDER OF THE COURT**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Matthew T. Pietropola, being first duly sworn, hereby depose and state as follows:

I

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been since August 2008. Since that time, I have worked in the Counterintelligence Division at the Washington Field Office and at FBI Headquarters. I have investigated various types of offenses against the United States, including numerous investigations into espionage and the unlawful retention or disclosure of sensitive and classified government information, including national defense information. I have received training in the preparation, presentation, and service of criminal complaints and arrest and search warrants. I have executed arrest warrants and search warrants in previous cases.

II

PURPOSE OF THE AFFIDAVIT

2. I make this affidavit in support of an application for a warrant to search the following locations or things:

a. [redacted], hereinafter "PREMISES";

b. A blue Dodge Charger owned by the Federal Bureau of Investigation and used by Terry James Albury, with VIN 2C3CDXJG35111, hereinafter "VEHICLE";

c. The office located at the Minneapolis-St. Paul International Airport in room G-1141-07, hereinafter "OFFICE";

d. The person of Terry James Albury, hereinafter "ALBURY"

further described in Attachment A, for the things described in Attachment B.

3. This affidavit is made in support of an application for a search warrant under Rule 41 of the Federal Rules of Criminal Procedure. Specifically, this affidavit is made in support of a request for a warrant to search the above locations for items listed in Attachment B. 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.

III

STATUTORY AUTHORITY AND DEFINITIONS

4. For the reasons set forth below, I believe that there is probable cause to believe that the PREMISES, VEHICLE, OFFICE, and ALBURY's person contain evidence, contraband, fruits, and/or other items illegally possessed in violation of Title 18,

United States Code, Section 793(e), and Title 18, United States Code, Section 1924 (the "Subject Offenses").

5. Under 18 U.S.C. § 793(e), "[w]hoever 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.

6. Under 18 U.S.C. § 1924 "[w]hoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined under this title or imprisoned for not more than one year, 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. Access to information at any level may be further restricted through compartmentation in secure compartmented information categories (SCI).

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.

IV

PROBABLE CAUSE

12. TERRY JAMES ALBURY ("ALBURY") began his career with the FBI in the summer of 2000 in its Honors Intern Program, during which he worked at FBI Headquarters on matters related to crimes against children. In August 2001, ALBURY was hired as a full time FBI employee conducting surveillance operations. ALBURY

became an FBI Special Agent in April 2005 and is currently assigned to the FBI Minneapolis Field Office.

13. While employed by the FBI, ALBURY has worked in various positions and on various projects. For his current assignment, ALBURY is assigned as an airport liaison working counterterrorism and other matters. ALBURY maintains a Top Secret security clearance with access to Sensitive Compartmented Information (SCI) and has access to various systems that contain classified information.

14. FBI records reflect that ALBURY was first issued a Top Secret/SCI security clearance in or about June 2000. On June 6, 2000, and again on October 22, 2001, ALBURY signed a "CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT" that stated, among other things:

> Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security...
>
> I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or-violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, *952 and 1924, Title 18, United States Code...

15. Also on October 22, 2001, ALBURY signed an "EMPLOYMENT AGREEMENT" that stated, among other things:

> As consideration for employment in the Federal Bureau of Investigation (FBI), United States Department of Justice, and as a condition for continued

employment, I hereby declare that I intend to be governed by and I will comply with the following provisions:

> (1) That I am hereby advised and I understand that Federal Law including statutes, regulations issued by the Attorney General and Orders of the President of the United States prohibit loss, misuse or unauthorized disclosure or production of information in the files of the FBI.
>
> (2) I understand that unauthorized disclosure of information in the files of the FBI or information I may acquire as an employee of the FBI could result in impairment of national security, place human life in jeopardy, or result in the denial of due process to a person or persons who are subjects of an FBI investigation, or prevent the FBI from effectively discharging its responsibilities. I understand the need for this secrecy agreement; therefore, as consideration for employment I agree that I will never divulge, publish, or reveal either by word or conduct, or by other means disclose to any unauthorized recipient without official written authorization by the Director of the FBI or his delegate, any information from the investigatory files of the FBI or any information relating to material contained in the files, or disclose any information or produce any material acquired as a part of the performance of my official duties or because of my official status…
>
> (4) That I understand unauthorized disclosure may be a violation of Federal law and prosecuted as a criminal offense…

16. More recently, on July 28, 2015, April 14, 2016, and June 5, 2017, ALBURY completed Information Security Awareness online training that established rules of behavior for general users of FBI information technology and information systems, which stated, among other things:

> I understand that I am to use FBI systems only for lawfully authorized purposes as set forth in Title 5 CFR Parts 2635 and 3801 (Federal Ethics Regulations), 28 CFR 45.4 (de minimis personal use), and as further outlined in this document and other FBI policy directives. Even where granted access, I must access the system files and information only on a need-to-know basis and only in furtherance of authorized tasks or mission related-functions. To remain compliant with applicable statutes, orders,

regulations, and directives, the FBI will update this form. It is my responsibility to maintain current knowledge of the FBI IT/IS Rules of Behavior for General Users.

As an authorized user of FBI IT/IS, I acknowledge the responsibility to protect FBI information. I also acknowledge the responsibility to protect FBI information when using OGA IT/IS assets in FBI controlled facilities.

I acknowledge that it is my responsibility to ensure the proper marking, storage, protection, and disposition of all non-public information to which I am given access as a result of my work with the FBI.

I will not:

1. Knowingly violate any statute or order, such as compliance legislation, copyright laws, or laws governing disclosure of information, including but not limited to:

c. Remove sensitive/classified media (paper or electronic) from controlled areas/facilities (i.e. taking classified media home) without authorization.
d. Use FBI IT/IS or FBI information for personal benefit, profit, to benefit other persons, non-profit business dealings, any political (e.g., lobbying or campaigning) party candidate or issue or for any illegal activity.

17. On or about March 29 and 30, 2016, a presumed U.S. Person (USPER1) representing an online media outlet (News Outlet) made two separate requests for copies of specific documents from the FBI pursuant to the Freedom of Information Act (FOIA), 5 U.S.C. § 552. The requests contained specific information identifying the names of the particular documents that had not been released to the public. Subsequently, the FBI identified approximately 27 FBI and U.S. Government documents published online by the News Outlet from on or about April 2016 and February 2017. Of these approximately 27 documents, approximately 16 are marked classified. The FBI believes that the classified and/or controlled nature of the documents indicates the News Outlet obtained these

documents from someone with direct access to them. Furthermore, reviews of FBI internal records indicate ALBURY has electronically accessed over two-thirds of the approximately 27 documents via trusted access granted to him on FBI information systems.

18. One of the FOIA requests, dated March 29, 2016, requested copies of an identified document classified at the SECRET level (hereinafter DOCUMENT1). According to information obtained directly from the News Outlet's website, DOCUMENT1 was uploaded to an online document repository on January 26, 2017 by another individual working for the News Outlet. The electronic copy of DOCUMENT1 posted on the News Outlet's website identified a creation date of August 17, 2011 on the first page. Based on the investigation, the FBI believes that the News Outlet, prior to the March 2016 FOIA requests referenced above, had obtained a cache of FBI documents, which included classified documents, such as DOCUMENT1. The News Outlet then used its knowledge of such documents to create the FOIA requests.

19. Of note, the electronic version of DOCUMENT1 published by the News Outlet includes a gray highlight across one row of text on page four. This gray highlight is not present in the original document. DOCUMENT1 was available to authorized FBI users on such a system. If the user accessed DOCUMENT1 in this available web interface, left clicked on the mouse, took a screen shot, and pasted the image, the gray highlight would be preserved in the pasted document. As detailed further below, a review of FBI internal audit records indicates that not only did ALBURY electronically access DOCUMENT1 via an FBI information system classified at the SECRET level, but

ALBURY also conducted cut and paste activity on DOCUMENT1 that could have resulted in the capture of a gray highlight in a saved electronic copy of DOCUMENT1.

20. A review of FBI user activity related to DOCUMENT1 identified 16 individuals, including ALBURY, who had accessed the document on the relevant FBI classified network between August 2011 and March 29, 2016, the date of the first FOIA request. ALBURY accessed the document on February 19, 2016, approximately one month and ten days prior to the FOIA request for DOCUMENT1, at approximately 1:25 pm CST. From approximately 1:28 pm CST to approximately 1:37 pm CST, ALBURY cut and pasted 11 screen shots into an electronic document. At approximately 1:40 pm CST on February 19, 2016, ALBURY printed this cut-and-paste version of DOCUMENT1. ALBURY's activity was conducted on an FBI information system classified at the SECRET level.[1] To date, a review of FBI records has revealed no indication that any

[1] The classified FBI information system referenced here and throughout this document requires user agreements and displays the following banner prior to logging on to any session by any user:

You are accessing a U.S. Government information system, which includes this computer, this computer network, all computers connected to this network, and all devices/or storage media attached to this network or to a computer on this network. This Information system is provided for U.S. Government –authorized use only. Unauthorized or improper use of this system may result in disciplinary action, and civil and criminal penalties. By using this information system you understand and consent to the following: You have no reasonable expectation of privacy regarding any communication transmitted through or data stored on this information system. At any time the government may monitor, intercept, search and/or seize data transmitted through or data stored on this information system. Any communications transmitted through or data stored on this information system may be disclosed or used for any U.S. Government authorized purpose.

individual other than ALBURY both accessed this document and conducted cut and paste actions.

21. Further, earlier on February 19, 2016, from approximately 11:08 am CST to approximately 12:09 pm CST, ALBURY accessed six additional documents on an FBI information system classified at the SECRET level. Two of these documents, in addition to DOCUMENT1, are clearly referenced in the March 29, 2016 FOIA request and are marked as UNCLASSIFIED/FOR OFFICIAL USE ONLY. DOCUMENT1 and one of the other documents clearly referenced in the FOIA request have been published on the Internet by the News Outlet.

22. Based on the descriptions in the FOIA request, the FBI believes that the remaining four documents accessed by ALBURY on February 19, 2016, are also referenced in the March 29, 2016 request. All four of these documents have been published on the News Outlet website. Two of these four published documents are marked SECRET and the other two carry no classification markings. In total, three of the seven documents at issue from February 19, 2016, were marked as classified at the SECRET//NOFORN level, and six of the seven were published on the Internet by October 2016 by the News Outlet.

23. On May 10, 2016, FBI records indicate ALBURY accessed several more documents on an FBI information system classified at the SECRET level that were also published on the Internet by the News Outlet. Between approximately 12:34 pm CST and approximately 12:50 pm CST, ALBURY accessed two documents, both classified at the

SECRET level and posted to the Internet by the News Outlet in October 2016. At approximately 1:09 pm CST and approximately 1:10 pm CST, ALBURY cut and pasted two screen shots into an unsaved Microsoft Word document. Between approximately 1:10 pm CST and approximately 1:56 pm CST, ALBURY pasted eleven screen shots into an unsaved Microsoft Excel document.

24. Additionally, between approximately 2:21 pm CST and approximately 3:07 pm CST that same day, ALBURY accessed six documents on an FBI information system classified at the SECRET level. Three of these documents were subsequently published by the News Outlet. Between approximately 3:19 pm CST and approximately 3:23 pm CST, ALBURY pasted three screen shots into the same unsaved Microsoft Excel document referenced above. At approximately 5:29 pm CST, ALBURY printed the unsaved Microsoft Excel document.

25. Analysis of internal FBI audit records revealed that ALBURY also printed various pages from FBI systems on February 11, 2016 that match documents published on the Internet by the News Outlet. These include six pages of presentation slides encompassing five separate presentations, in a format where multiple slides are displayed on each page with a blue background. These pages of slides appear to be cut and pasted into a separate document. For two specific sets of presentation slides, the first slide is highlighted in orange. These two sets of slides printed by ALBURY appear identical to two UNCLASSIFIED documents published on the Internet by the News Outlet on October 5, 2016, which both have first slides highlighted in orange and have blue backgrounds.

26. A review of the documents posted on the News Outlet's Internet website on January 31, 2017 suggests that the source of the documents photographed some of them. This review reveals common screen defects in consistent locations on some of these posted documents. For instance, for three documents posted by the News Outlet on the Internet, two of which are classified SECRET and one of which is UNCLASSIFIED, a discoloration consistently appears in the same place in the top left margin on alternating pages. Given that the discolorations do not appear in the original documents, one possibility is that they are the result of either a temporary or permanent defect on either the electronic display or lens of the camera or capture device. The lack of the discoloration on even-numbered pages of the documents posted on the Internet indicates that the arrangement of the pages at the moment of capture (for instance two-page view) was such that it would not capture the defect on every page. One explanation for the condition of these three documents is that an individual used a camera to photograph the documents while viewing them in two-page view. A review of the software and configuration of the relevant FBI classified network from which the three documents were accessed indicates a readily available capability within the default document viewer to view documents in two-page view. Once a file is opened in two-page view, a user could photograph the pages displayed on the electronic display. A defect on either the electronic display or lens of the camera or capture device would then plausibly replicate the observed pattern of discolorations.

27. This explanation is corroborated via closed circuit video surveillance of ALBURY at the OFFICE on June 16, August 23, and August 24, 2017. On June 16, 2017,

ALBURY was observed holding a silver digital camera at approximately 7:44 am CST and inserting what appears to be a digital memory stick into said camera. At approximately 7:56 am CST, ALBURY appeared to start taking photographs of his computer screen of his FBI information system classified at the SECRET level. This activity continued until approximately 8:27 am CST. On August 23, 2017, ALBURY was observed holding a silver digital camera at approximately 7:10 am CST and inserting what appeared to be a digital memory stick. At approximately 7:18 am CST, ALBURY appeared to start taking photographs of his computer screen of his FBI information system classified at the SECRET level. This activity continued until approximately 7:58 am CST. On August 24, 2017, ALBURY was observed holding a silver digital camera at approximately 6:27 am CST and inserting what appeared to be a digital memory stick. At approximately 6:37 am CST, ALBURY appeared to start taking photographs of his computer screen of his FBI information system classified at the SECRET level. This activity continued until approximately 7:03 am CST. Analyses of internal FBI audit information for all three days indicates that during these sessions, ALBURY was viewing various classified and UNCLASSIFIED documents on his computer screen while he was taking the referenced photographs.

28. In total, the FBI's review to date of ALBURY's user activity has identified ALBURY has electronically accessed at least two thirds of the approximately 27 documents on an FBI information system classified at the SECRET level, prior to their reference in the FOIA requests and/or prior to the documents being posted on the Internet

by the News Outlet. To date, a review of FBI records has not revealed any other individual besides ALBURY who electronically accessed DOCUMENT1 and conducted cut and paste actions, let alone any other individual who has electronically accessed as many of the published documents prior to the FOIA requests made by USPER1.

29. Contained on the News Outlet's website are directions for various ways to contact the News Outlet anonymously. One of the methods includes taking a personal computer to a Wi-Fi network that is not associated with the user or their employer to access the News Outlet's SecureDrop server. Another method provided to communicate anonymously is to download the Signal application on an Android or iPhone device. ALBURY owns an iPhone as a personal device. Noted in the directions is the ability to install the desktop versions of such applications on a personal computer after the user downloads the mobile application and registers their telephone number. In addition to the methods involving computer devices to transfer material, the News Outlet also provides postal mailing addresses to which one may physically send the materials.

30. Prior to accessing the above-described documents in February and May of 2016, ALBURY exchanged a series of communications with a coworker on December 21, 2015. During this series of communications, ALBURY and the coworker discussed reporting an inappropriate e-mail sent by another coworker. During their discussion, ALBURY sent a message stating, "if [the Office of Professional Responsibility] does not respond, let me go on record and say i will contact the press." While the coworker's e-mail is unrelated to the unauthorized disclosure of classified documents to the News Outlet,

the exchange of these messages shows that ALBURY had considered disclosing internal FBI information to the media.

31. Based on my review of DMV records, FBI employee records, and county property records, it is believed that ALBURY currently lives at [redacted]

32. Based on my training and experience, as well as discussions with other law enforcement officers, individuals who unlawfully possess, disclose, and/or retain classified documents and/or information must typically transport on their person, in a vehicle, or electronically through email or other electronic means, including web-based applications accessible through smart telephones or other web-enabled devices, the information from a secure facility or computer to another location. This may be done by printing the information from a classified computer, downloading the information to an electronic storage device, copying the information by hand into another medium, using photographic equipment to take pictures of the information, disclosing the information via written or spoken word, etc. For printed documents, the individual may then scan or send the copies to another person. For electronic documents and photographed documents, files may be transferred to other electronic storage devices or transmitted to others via a computer or another similar electronic device capable of connecting to the Internet.

33. In my training and experience, one such place where documents and/or classified material may be taken is an individual's home. Due to the training most individuals with access to classified information receive, individuals with access to

classified information typically understand that the unlawful retention of classified information is a serious offense. Thus, those who seek to remove classified documents from secure facilities seek to store or retain them in a location where others will not discover their unlawful acts. This is frequently their personal residence, as it is a location to which the individual can control access. In other situations, this may include commercial storage lockers, vehicles, security deposit boxes, etc.

V

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

34. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, OFFICE, VEHICLE, and ALBURY. 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).

35. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, 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."

36. *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 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 inculpating 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 inculpate 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.

37. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises 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, 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.

38. *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.

39. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those

computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

CONCLUSION

40. I submit that this affidavit supports probable cause for a warrant to search the locations described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING

41. 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 into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. 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.

Further your affiant sayeth not.

Respectfully submitted,

Matthew T. Pietropola
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me

on August 28, 2017:

DAVID T. SCHULTZ
UNITED STATES MAGISTRATE JUDGE