UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF GEORGIA

|  |  |
| --- | --- |
| EMORY UNIVERSITY  Office of the General Counsel  101 Administration Building  201 Dowman Drive  Atlanta, Georgia 30322  Phone Number: (404) 727-6123  Fax Number: 404-712-5522 | Case No. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  **APPLICATION AND AFFIDAVIT**  **FOR SEARCH WARRANT** |

I, AGENT PARKWAY 007, being duly sworn, depose and say:

I am a Special Agent with the DHS and have reason to believe that on the property or premises known as (name, description and/or location)

See ATTACHMENT A

in the NORTHERN District of GEORGIA there is now concealed a certain person or property, namely (described the person or property)

See ATTACHMENT B

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure) evidence concerning violations of 18 United States Code § 2332b (Acts of Terrorism Transcending National Boundaries)

The facts to support a finding of Probable Cause are as follows:

See Affidavit attached and made a part thereof. X Yes \_\_\_ No



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Affiant

Sworn to before me, and subscribed in my presence

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date City and State

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ at \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name and Title of Judicial Officer Signature of Judicial Officer

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT**

I, Agent Parkway 007, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a warrant authorizing EMORY UNIVERSITY (“Emory”), as described in ATTACHMENT A, to provide law enforcement with any and all means of gaining access including login and password information, password reset, and/or any information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Emory, an email provider headquartered at 201 Dowman Drive, Atlanta, Georgia 30322. The information to be searched is described in the following paragraphs and in ATTACHMENT B. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Emory to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications. In addition, I am requesting all current subscriber and other account information pertaining to the identity of the registrant of the Emory account.

2. I am a Special Agent with the DHS, and have been since 20 July 2015. I have had extensive work in many career fields including Forensic Analysis, Computer Network Support Specialist, and a Computer System Analysis. We have solved numerous amounts of cases involving National Security.

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

**PROBABLE CAUSE**

4. Astrapi bullet train was scheduled to reach Abeline, Texas at 7:25 A.M. and never reached the checkpoint in Texas. The train was determined to be hacked by an ip address linked to Emory University. This attack was traced more specifically to the organization BLOWC, “Better Living Off Without Chemicals.” Analysis linked the IP address used to disable the security modules of the Astrapi originated from a network linked to the university where this organization. A previous search warrant by the Department of Homeland Security found communications between multiple students, discussing what is believed to be a code that indicates plans for a terror plot.

We have reason to believe that Sandra Bullock among other students are different users from the a forum popular among black-hat hackers and international cyberterrorists. This site is used heavily by the cyberterrorism group IndiShell. We believe that Sandra, a student at Emory, which is part of REM, is “Sistine Sister’ in the forum. Sandra’s insider ability with both Emory and REM spurns a relationship, which we believe results in a cyberterrorist attack. Our reasoning behind this is that we have conversation from a known cyberterrorist web forum, <http://www.eco-now.com/>. She explicitly stated “...we need to jack them up.” This establishes an intent to commit crime. A user replied “send a private message to my burner… [burnernogo@gmail.com](mailto:burnernogo@gmail.com).” This conversation proves that she is establishing contact with a suspected cyber terrorist, and shows intent to act. We believe that she provided IndiShell with insider access to Emory and REM to allow them to hack and commit a cyberterrorist attack. We also believe another user she makes contact with is an associate of hers. This associate is believed to be the user “Big Eat.” We believe that this “Big Eat” is Pete Bishop, who is also a student at Emory, because in the email conversations between here and the associate, Pete types in the text of all caps, where “Big Eat” types in the same text format. This gives us reason to believe all other associates are working with the noted gang IndiShell, and directly contribute to REM lowering security on the aforementioned train, allowing a cyberterrorist attack to occur.

**TECHNICAL BACKGROUND**

5. In my training and experience, I have learned how to effectively display and expose potential suspects to the case that could be a danger to National Security. I can effectively program a variety of different languages fluidly. The case can be furthered due to my skills at analyzing details to the problems at hand. The investigation of the missing train this morning can be traced back to messages sent between students at Emory. Emory provides a variety of online services, including electronic mail (“email”) access, to the general public. Subscribers obtain an account by registering with Emory. During the registration process, Emory asks subscribers to provide basic personal information. Therefore, the computers of Emory are likely to contain stored electron- Appendix I 257 ic communications (including retrieved and unretrieved email for Emory subscribers) and information concerning subscribers and their use of Emory services, such as account access information, email transaction information, and account application information.

6. In general, an email that is sent to a Emory subscriber is stored in the subscriber’s “mailbox” on Emory servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Emory servers indefinitely.

7. When the subscriber sends an email, it is initiated at the user’s computer, transferred via the Internet to Emory's servers, and then transmitted to its end destination. Emory often saves a copy of the email sent. Unless the sender of the email specifically deletes the email from the Emory server, the email can remain on the system indefinitely.

8. An Emory subscriber can also store files, including emails, address books, contact or buddy lists, pictures, and other files, on servers maintained and/or owned by Emory.

9. Subscribers to Emory might not store on their home computers copies of the emails stored in their Emory account. This is particularly true when they access their Emory account through the web, or if they do not wish to maintain particular emails or files in their residence.

10. In general, email providers like Emory ask each of their subscribers to provide certain personal identifying information when registering for an email account. This information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

11. Email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, 258 Searching and Seizing Computers the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Emory'S website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address (“IP address”) used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

12. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider’s support services, as well records of any actions taken by the provider or user as a result of the communications. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

13. I anticipate executing this warrant under the Stored Communications Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Emory to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government authorized persons will review that information to locate the items described in Section II of Attachment B. CONCLUSION

14. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the computer systems in the control of Emory there exists evidence of a crime [and contraband or fruits of a crime]. Accordingly, a search warrant is requested.

15. This Court has jurisdiction to issue the requested warrant because it is “a court with jurisdiction over the offense under investigation.” 18 U.S.C. § 2703(a).

16. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Appendix I 259 REQUEST FOR NONDISCLOSURE AND SEALING

17. The United States requests that pursuant to the preclusion of notice provisions of 18 U.S.C. § 2705(b), Emory be ordered not to notify any person (including the subscriber or customer to which the materials relate) of the existence of this warrant for such period as the Court deems appropriate. The United States submits that such an order is justified because notification of the existence of this Order would seriously jeopardize the ongoing investigation. Such a disclosure would give the subscriber an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee or continue his flight from prosecution.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

AGENT PARKWAY 007

Special Agent

Department of Homeland Security

Subscribed and sworn to before me on this 24th day of July, 2015.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

UNITED STATES MAGISTRATE JUDGE

NORTHERN DISTRICT OF GEORGIA

**ATTACHMENT A**

The location, property, and records to be searched are located at and described as: Emory University, Office of the General Counsel, 101 Administration Building, 201 Dowman Drive, Atlanta, GA 30322, telephone number: (404) 727-6123, fax number: 404-712-5522.

**ATTACHMENT B**

Particular Things to be Seized

I. Information to be disclosed by Emory To the extent that the information described in Attachment A is within the possession, custody, or control of Emory, Emory is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails stored in the account, including copies of emails sent from the account;

b. All records or other information regarding the identification of the account, to

include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, login IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;

d. All records pertaining to communications between Emory and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of the statutes listed on the warrant involving Sandra Bullock since 13 July 2015, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. All received email messages sent to the following address: sbullock@emory.edu

b. All email messages sent by the following address: sbullock@emory.edu

c. All email messages within the deleted files of the following address: sbullock@emory.edu

d. All archived email messages of the following address: sbullock@emory.edu

e. Communications between [sbullock@emory.edu](mailto:sbullock@emory.edu) and suspected burner emails.

f. Any communication with addresses belived to be assosiated with the site <http://www.eco-now.com/>