UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

FILED
JUL - 5 2013
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
THE YOUTUBE ACCOUNT BRADMANNING, MAINTAINED ON THE COMPUTER SYSTEMS OF GOOGLE, INC.

Case No. 1:13-SW-492

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 *(identify the person or describe the property to be searched and give its location)*:
See Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B

and 18 U.S.C. § 2703

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

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ 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*
18 U.S.C. § 793(d)	Unauthorized Disclosure of National Defense Information
18 U.S.C. § 1030	Exceeding Authorized Access to a Computer to Obtain and Disclose Protected Information

The application is based on these facts:
See Attached Affidavit

☑ 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.

Reviewed by AUSA/SAUSA:

AUSA Lindsay A. Kelly

Applicant's signature

Mark Mander, Special Agent, USACIDC

Printed name and title

Sworn to before me and signed in my presence.

Date: 07/05/2013

/s/Thomas Rawles Jones, Jr.

Judge's signature

City and state: Alexandria, Virginia

The Honorable T. Rawles Jones, Jr., U.S. Magistrate Judge

Printed name and title

ATTACHMENT A: ITEMS TO BE SEARCHED

The items to be searched are associated with the YouTube Account "bradmanning", that is stored at premises owned, maintained, controlled, or operated by Google, Inc., a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA, including:

- Copies of the complete videos with the following video IDs:
  - BH0jnyuJ1Tg
  - AalHTp1M8yg
  - AaIHTp1M8yg
  - iV-s2O4Gi2M
  - aZ9flPputYQ
  - aZ9fIPputYQ
  - 6mvTV_KtkLY
  - mssEpO3KRLk
  - qlj1K5F3bm8
  - qIj1K5F3bm8
- Copies of all other videos linked/saved/associated (such as "Favorite Videos") by the account user, but subsequently deleted (including videos uploaded to YouTube by other YouTube users)
- Copies of all other videos uploaded by the account user, but subsequently deleted
- All content presently or previously associated with the TARGET ACCOUNT's:
  - Inbox
  - Personal Messages
  - "Shared With You" page/folder
  - "Comments" page/folder
  - Contact Notifications
  - Video Responses

- Sent
- Address Book

(including sent, drafted, or deleted messages, notifications, or other types of correspondence still retrievable by Google)

ATTACHMENT B

ITEMS TO BE SEIZED

The items to be seized constitute fruits, evidence, contraband, and instrumentalities of violations of Title 18, United States Code, Section 793(d) (Unauthorized Disclosure of National Defense Information) and Title 18, United States Code, Section 1030 (Exceeding Authorized Access to a Computer to Obtain and Disclose Protected Information), including:

1. Records, documents, information or data evidencing ownership or use of the account listed in Attachment A.

2. Items containing potential passwords or passphrases.

3. U.S. Government records, documents, information, or data including national security and national defense information.

4. Records, documents, information, or data identifying persons or entities involved in such violations, including communications, financial transactions, and data exchange with or related to such persons, photographs and/or videos of such persons.

5. Records, documents, information, or data identifying the methods or means used to obtain U.S. government information or the communication, delivery, or transmission of such information.

6. Records, documents, information or data evidencing knowledge, intent, or motive.

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

JUL - 5 2013
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

IN THE MATTER OF THE SEARCH OF THE YOUTUBE ACCOUNT BRADMANNING, MAINTAINED ON THE COMPUTER SYSTEMS OF GOOGLE, INC.	Case Number: 1:13-sw-492

AFFIDAVIT IN SUPPORT OF A SEARCH AND SEIZURE WARRANT

I, MARK MANDER, being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. This affidavit is made in support of an application for a warrant pursuant to 18 U.S.C. §§ 2703(a) and 2703(b)(A) to compel Google, Incorporated (hereafter "Google" or "Provider"), a provider of electronic communication and remote computing services located at 1600 Amphitheater Parkway, Mountain View, California, to provide copies of videos and the contents of messages associated with the YouTube account "bradmanning" (hereafter the "TARGET ACCOUNT").

2. The TARGET ACCOUNT is an account on Google's video sharing website and communications platform, commonly known as "YouTube."[1] As discussed below, an investigation into the TARGET ACCOUNT indicates it is associated with the knowing and willful unlawful transmission of national defense information and the unlawful disclosure of classified and/or National Defense Information. Accordingly, there is probable cause to believe the contents of the wire and electronic communications pertaining to the TARGET ACCOUNT are evidence, fruits and instrumentalities of criminal violations of 18 U.S.C. § 793, Unlawfully

[1] YouTube is a well-known and widely used website owned and operated by Google, Incorporated, which allows users, who may be general members of the public, to upload, view, link to, search for, and comment on electronic video files its users provide to YouTube via the Internet.

Transmitting National Defense Information and 18 U.S.C. § 1030, Exceeding Authorized Access to a Computer to Obtain and Disclose Protected Information. This affidavit is made in support of an application to search for and seize evidence of a violation of 18 U.S.C. § 793 (d) (Transmitting National Defense Information) and 18 U.S.C. § 1030(a)(1) (Exceeding Authorized Access to a Computer to Obtain and Disclose Protected Information).

3. I am a Special Agent of the U.S. Army Criminal Investigation Command ("USACIDC") and have been so for approximately eleven years. I am currently assigned to the USACIDC, Washington Metro Resident Agency ("WMRA") of the Computer Crime Investigative Unit ("CCIU"), located at Quantico, Virginia, where I am responsible for the investigation of, among other things, violations pertaining to computer intrusions, denial of service attacks, and other types of malicious computer activity directed against U.S. Army and/or Department of Defense (DoD) computer networks anywhere in the world. My prior assignments were as a USACIDC Special Agent in South Korea and at Fort Lewis, Washington, where I was responsible for conducting felony investigations impacting the U.S. Army and/or DoD in those regions. In addition, between August 2008 and July 2009, I was assigned to the Baghdad CID Battalion as a Computer Crime Coordinator, responsible for conducting computer forensic examinations of seized computers, cellular phones, and other digital media collected and seized during USACIDC investigations within Iraq, Kuwait and Afghanistan.

4. My experience as a USACIDC Special Agent has also included the investigation of cases involving violent and non-violent crimes as well as the use of computers. I have received training and gained experience in interviewing and interrogation techniques, arrest procedure, search warrant applications, the execution of searches and seizures, and other criminal laws and procedures. Specifically, I have been trained in computer incident response,

digital evidence acquisition, forensic examinations of computers and digital media, and malicious software analysis, by the Department of Defense Cyber Investigations Training Academy ("DCITA"). I currently possess the "Department of Defense Certified Computer Crime Investigator" certification.

5. As a USACIDC Special Agent, I am authorized to investigate crimes involving all violations of the Uniform Code of Military Justice (10 U.S.C. § 47) and other applicable federal and state laws where there is a U.S. Army or Department of Defense ("DoD") interest.

BACKGROUND

6. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation from other individuals, including other law enforcement officers, as well as my review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances, and information gained through my training and experience.

7. This affidavit is intended only to demonstrate probable cause and does not set forth each and every fact that I or others have learned during the course of this investigation.

RELEVANT LAW

8. Title 18, United States Code, § 793(d) makes it unlawful to communicate national defense information to a person not entitled to receive such information. The statute provides in pertinent part that:

> Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, . . . 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 . . . the same

> to any person not entitled to receive it . . . shall be fined under this title or imprisoned not more than ten years, or both.

9. Title 18, United States Code, § 1030(a) makes it unlawful for a person to exceed authorized access to a government computer to obtain national defense information, and with reason to believe such information could injure the United States, to communicate it to a person not entitled to receive it. The statute provides in pertinent part that:

> Whoever – (1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations . . . with reason to believe that such information so obtained 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 . . . the same to any person not entitled to receive it . . . . shall be punished by a fine under this title or imprisonment for not more than ten years, or both . . . .

10. The Executive Branch controls national security information under the classification system established by Executive Order No. 13526 and its predecessor orders. Under Executive Order No. 13526, information may only be classified if an Original Classification Authority has made a determination that the unauthorized disclosure of the information would cause damage to the national security of the United States. Exec. Order No. 13526 § 1.1(a)(4) , 75 Fed. Reg. 707 (Dec. 29, 2009). Under the Executive Order, information may be classified "Confidential" if its unauthorized disclosure reasonably could be expected to cause damage to the national security; "Secret" if its unauthorized disclosure reasonably could be expected to cause serious damage to the national security; and "Top Secret" if its unauthorized

disclosure reasonably could be expected to cause exceptionally grave damage to the national security. *Id.* at §1.2.

PROBABLE CAUSE FOR SEARCH

A. MANNING'S ACCESS TO CLASSIFIED INFORMATION

11. Bradley E. MANNING ("MANNING") enlisted in the United States Army on or about October 2, 2007, and currently holds the rank of Private First Class. He received training in Intelligence Analysis, and on January 22, 2009, was granted a U.S. Government security clearance at the "Top Secret" level. On or about October 12, 2009, MANNING was deployed with his unit to Forward Operating Base ("FOB") Hammer, located approximately 40 miles east of Baghdad, Iraq.

12. Between October 2009 and May 2010, while assigned in Iraq and working in the role of an All-Source Intelligence Analyst, MANNING was granted access to national defense information through various U.S. Army and DoD computer network systems, including: the Non-Secure Internet Protocol Router ("NIPR") network, used for the processing of unclassified documents and unclassified communications; and the Secure Internet Protocol Router ("SIPR") network, used for the processing of classified documents and classified communications at the "Confidential" and "Secret" classification levels. MANNING also had access to a commercial, non-military, satellite-based ISP while in his living quarters, which he used with his personal laptop computer. This information has been verified by statements of co-workers in MANNING's unit, by examination of various computer accounts and network log file systems, the forensic examination of computers used by MANNING, and by documents obtained during the course of this investigation.

B. WIKILEAKS' DISCLOSURE OF NATIONAL DEFENSE INFORMATION

13. On April 5, 2010, Mr. Julian P. Assange ("Assange"), who has been identified as the founder, editor-in-chief, and director of the website Wikileaks.org (hereinafter "Wikileaks")[2], held a press conference at the National Press Club, located at 529 14th Street NW, Washington, D.C. During the event Assange disclosed to the public and displayed to attendees a video recorded in July 2007 by a U.S. Army Apache helicopter engaged in combat (hereinafter the "Apache Video"). The Apache Video depicts several combatants, as well as media personnel and non-combatants who were unidentified as such at the time but were in close proximity to the combatants, being wounded or killed. Subsequent to the publication of the Apache Video, the property of the U.S. Army, DoD officials determined this video to be authentic; it was initially believed that this video or metadata associated with the video contained classified information.[3] Over the next year, Wikileaks released a large number of classified documents.

C. MANNING ADMITS TO DISCLOSING CLASSIFIED INFORMATION

14. On May 20, 2010, MANNING, while still assigned in Iraq, contacted Mr. Adrian A. Lamo ("Lamo"), apparently after reading a published profile of Lamo. Lamo is well known in the computer security community as a computer hacker, and has been profiled extensively in the news media. Consequently, Lamo provided a sworn statement to USACIDC and U.S. State Department Diplomatic Security Service ("DSS") Special Agents, in which he detailed how MANNING had initially contacted him by sending several encrypted e-mails from the e-mail

---

[2] WikiLeaks is self-described as "a multi-jurisdictional public service designed to protect whistle blowers, journalists and activists who have sensitive materials to communicate to the public."

[3] After a classification review by an original classification authority it was determined this video was unclassified.

address bradley.e.manning@gmail.com[4] in late May 2010. Lamo told investigators he could not read most of the encrypted e-mails sent by MANNING, as MANNING appeared to have used a publicly available encryption key belonging to Lamo which Lamo no longer used. Lamo stated he replied to MANNING, advising him to communicate using the commercial chat software application AOL Instant Messenger ("AIM"), and provided his AIM account name so that MANNING could contact him.

15. Lamo further detailed that between May 20 and 26, 2010, MANNING and Lamo engaged in a series of AIM chats, additionally utilizing a publicly available encryption software application known as Off-the-Record ("OTR") to encrypt their communications. During these conversations, MANNING admitted to Lamo that MANNING had sent the Wikileaks website a U.S. Department of State diplomatic cable originating from the U.S. Embassy in Reykjavik, Iceland, which was classified "Confidential." MANNING further admitted to sending the Wikileaks website other classified and/or U.S. Government National Defense Information, to include: classified documents related to combat operations in Afghanistan and Iraq, many of which were classified at the "Confidential" and "Secret" level; classified documents related to detainees being held at Guantanamo Bay, Cuba, some of which were classified at the "Secret" level; the classified U.S. State Department diplomatic cable database,[5] which contained numerous documents classified at the "Confidential" and "Secret" level; a classified video and

---

[4] This email address has been verified as MANNING's address by several means, including the fact that MANNING provided this personal e-mail address when first registering for an official U.S. Army e-mail account.

[5] MANNING appears to have been referring to the Net Centric Diplomacy initiative database that is maintained on the SIPR network by the Department of State.

related documents of a 2009 air strike in Gharani, Afghanistan; and the aforementioned Apache Video.

16. Lamo provided investigators copies of e-mail messages that MANNING had sent from the e-mail address bradley.e.manning@gmail.com, as well as copies of the above-described unencrypted AIM chat logs between MANNING and himself. Lamo also surrendered to USACIDC and DSS Special Agents his personal computers and other digital media devices containing the original electronic MANNING chat logs. Lamo further consented in writing to the forensic examination of his computers and digital media containing this and other potential electronic evidence.

D. MANNING PLEADS GUILTY TO SOME CRIMINAL CHARGES AND ADMITS TO WRONGFUL DISCLOSURE OF CLASSIFIED INFORMATION

17. On February 28, 2013, MANNING read a lengthy prepared statement in the presence of a Military Judge as part of a preliminary courts-martial proceeding. In MANNING's statement he admitted to having disclosed (1) the Apache Video, which he believed to be classified as "Secret" material at the time of his unlawful disclosure; (2) classified documents associated with combat operations in Iraq and Afghanistan; (3) the U.S. State Department diplomatic cable database, though MANNING stated that he believed the disclosure of these cables would not damage the United States; and (4) other U.S. Government documents which were National Defense Information and in most cases also classified material. With respect to some materials he admitted disclosing, MANNING stated that in his personal assessment, the disclosed documents did not give away sensitive information. MANNING explained he unlawfully disclosed this material to the Wikileaks website and consequently to personnel unauthorized to receive it. MANNING also admitted to having lengthy internet chats with a

person whom he believed to be Assange, during the time he was deployed to Iraq and prior to his apprehension by USACIDC.

18. During the subsequent investigation into MANNING, it was determined MANNING had previously uploaded sensitive information to YouTube while attending Advanced Individual Training ("AIT") to become an Intelligence Analyst, while at Fort Huachuca, Arizona, between April 7, 2008, and August 16, 2008. Interviews with instructors who knew MANNING while he was in training revealed MANNING had posted several videos to YouTube, viewable to the public via the Internet, which contained sensitive but unclassified information about the Intelligence training facility at Fort Huachuca.

E. DISCOVERY OF THE TARGET ACCOUNT

19. On May 29, 2013, in preparation for military courts-martial proceeding against MANNING for various charges related to the unauthorized disclosure of classified and/or National Defense Information which MANNING did not plead guilty to, MANNING's Defense Attorney provided three pages of 'Reciprocal Discovery' to the U.S. Government. This Reciprocal Discovery included several messages MANNING had exchanged via the TARGET ACCOUNT with another YouTube user. A review of the USACIDC investigation determined investigators had previously attempted to identify all electronic accounts used by MANNING, but had not identified the TARGET ACCOUNT prior to the disclosure.

20. A review of the publicly accessible portions of the TARGET ACCOUNT by USACIDC Special Agents, at the Uniform Resource Locator ("URL") http://www.youtube.com/user/bradmanning, revealed the account was established on July 27, 2006. The TARGET ACCOUNT, which bears a photograph of MANNING, was further identified as having thirty-nine (39) videos associated as "Favorite Videos." One of these videos was a 17 minute and 47

second version of the Apache Video. Further examination showed this video was uploaded to YouTube by another YouTube account assigned the user name "sunshinepress" on April 3, 2010 – approximately two days prior to this video being disclosed to the general public at the previously mentioned National Press Club event on April 5, 2010.

21. A review of other content on the "sunshinepress" YouTube account revealed this account was associated with and/or controlled by Wikileaks. Additionally, research identified "Sunshine Press" was the unofficial organization which initially started the Wikileaks.org website in 2006. Historical media reports quoting known members of the Wikileaks organization indicate Sunshine Press Productions, Ehf (an Icelandic limited liability corporation), was registered as a legal entity in 2010, to conduct fundraising and/or information gathering activities on behalf of Wikileaks. Assange has publicly claimed to be director of Sunshine Press Productions, Ehf.

22. Further review of the TARGET ACCOUNT identified at least one video marked "Private" and therefore inaccessible publicly.

23. Based on the YouTube Terms of Service ("TOS") Agreement between YouTube and its users, dated June 9, 2010, wherein YouTube expressly states to its users: "You understand and agree, however, that YouTube may retain, but not display, distribute, or perform, server copies of your videos that have been removed or deleted," it is believed video files which may have been previously associated with the TARGET ACCOUNT and later disassociated from or deleted by MANNING may be retrievable by Google from electronic storage. For example, videos created by MANNING and uploaded to YouTube in 2008, in which MANNING discussed sensitive information related to AIT training at Fort Huachuca, Arizona, which may

have been removed or deleted by MANNING from the TARGET ACCOUNT, may still exist within the electronic storage of Google.

24. On June 13, 2013, the Honorable John F. Anderson issued a search warrant for subscriber information and content of the TARGET ACCOUNT, including (as relevant here):

a. All posted video files (both publicly accessible and private);

b. All videos and other content which may have been deleted by the account user but is still retrievable by Google; and

c. The content of Private Messages sent to or from this YouTube account, to include the time and date of messages sent, received, drafted, or deleted.

25. Google responded with a partial production on June 19, 2013, and a supplemental production on June 25, 2013. Google provided a list of video IDs, but no copies of videos, and further excluded contents of six of the seven folders comprising the TARGET ACCOUNT (producing only the contents of the "Personal Messages" folder). Based on the video IDs provided by Google, your Affiant was able to download most of the videos associated with the TARGET ACCOUNT independently. However, seven videos were inaccessible: YouTube displayed messages that the videos associated with those seven video IDs were "unavailable" or "private".

26. Google has taken the position that the original search warrant did not cover actual videos or contents of folders other than the "Personal Messages" folder, and is requesting a second search warrant. Given the ongoing court-martial of Bradley Manning, and the need to obtain this information quickly, your Affiant is submitting the present affidavit tailored to the two outstanding categories of information related to the TARGET ACCOUNT.

27. Based on Google's responses to the June 13, 2013, search warrant, and publicly-available information, it is still unknown whether: (1) MANNING exchanged messages via the

TARGET ACCOUNT with the "sunshinepress" YouTube account; (2) MANNING exchanged messages via the TARGET ACCOUNT with other individuals in relation to his unlawful disclosures; and (3) any "Private", "Unavailable", or deleted videos associated with the TARGET ACCOUNT contain classified and/or National Defense Information and/or evidence relevant to the government's investigation.

CONCLUSION

28. For the foregoing reasons, I request this Court to issue a warrant to authorize a search of the TARGET ACCOUNT more particularly described in Attachment A to obtain the fruits, evidence, contraband, and instrumentalities identified in Attachment B of violations of Title 18, United States Code, Section 793(d) (Unauthorized Disclosure of National Defense Information) and Title 18, United States Code, Section 1030 (Exceeding Authorized Access to a Computer to Obtain and Disclose Protected Information).

Mark Mander
Special Agent
U.S. Army Criminal Investigation Command

Subscribed and sworn to before me this
5th day of July, 2013.
Alexandria, Virginia

/s/Thomas Rawles Jones, Jr.

The Honorable T. Rawles Jones, Jr.
United States Magistrate Judge

Submitted by Assistant U.S. Attorney Lindsay Kelly