

FOR OFFICIAL USE ONLY

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

STIPULATION OF
EXPECTED TESTIMONY

Mr. Maxwell Allen

16 June 2013

It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if Mr. Maxwell Allen were present to testify during the merits and pre-sentencing phases of this court-martial, he would testify substantially as follows:

1. I am currently employed with the Central Intelligence Agency (CIA) and have worked there for six years. Before that, I was a contractor with Oracle for ten years. Oracle is the largest database company in the world and is the platform for the Open Source Center (OSC) database. I work on the contract for the OSC. I am the lead database engineer and database administrator for the OSC. I have been the lead database administrator and engineer for two years. As a database engineer, I build and develop databases to efficiently store and retrieve data and as a database administrator I maintain the databases. As the lead, I am in charge of the database engineers and administrators.
2. The OSC is a website controlled by the Central Intelligence Agency (CIA), which requires a user to have an OSC account to access information. The website is located on the unclassified system, SIPRNET, and JWICS and allows a user, once authenticated, to conduct searches of various files created by the CIA and other organizations. The OSC contains reports and translations from thousands of unclassified publications, television and radio programs, and Internet sources around the world.
3. The OSC cannot complete a request by a user without logging the request in the audit logs. In other words, if the OSC cannot log its actions, it will stop working and users will not be able to retrieve their requests and view pages on the website. We conduct a monthly check of the logs to ensure the system is functioning properly, and we always keep the database up to date by installing all updates. Typically, the purpose of checking the audit logs is to see if there are any errors in the automated process.
4. The OSC database creates three separate types of logs: application logs, server logs, and firewall logs. In this case, I pulled the application logs. The other logs would reflect the same basic information in a different format. The logs are created every time an event occurs. In this case, we were asked to pull any user information for "Bradley Manning," as well as audit logs associated with the user names on any "Bradley Manning" accounts.
5. As I stated, an OSC account is required to access the OSC. To apply for an OSC account, a user has to enter their personal information in the application. When applying for an account on SIPRNET, the account is automatically approved upon application and confirmation of the SIPRNET email address. Having an OSC account allows you to access the OSC website through

FOR OFFICIAL USE ONLY

PROSECUTION EXHIBIT 137 for identification
PAGE OFFERED: _____ PAGE ADMITTED: _____
PAGE _____ OF _____ PAGES

FOR OFFICIAL USE ONLY

SIPRNET. If a user wants to access sites not within OSC, the user has to log on to those sites separately even if the user clicks on a link from within the OSC website.

6. I searched the database for any combination of Bradley and Manning. After looking at the first and last names on the accounts, I determined that there were two accounts with the first name Bradley and the last name Manning. Both the accounts were on the SIPRNET. I opened the account information for those accounts and took screenshots of the account information by pressing control and enter to take a screenshot.

a. The first account had a user name of "Bmanning." The name entered by the individual creating the account was Bradley Edward Manning. The phone number was (240) 784-0431. The secret level email given was Bradley.manning@2bct10mtn. The security question was "What city/town did you grow up in?" The answer given by the account user was "Crescent." The account was opened on 6 November 2009 and the last login was 6 November 2010. **Prosecution Exhibit (PE) 138 for Identification** is the account screenshot with BATES number: 00374393.

b. The second account had a user name "bradass87." The name entered by the individual creating the account was Bradley Edward Manning. The phone number was (312) 848-8722. The secret level email given was bradley.manning@us.army.smil.mil. The security question was "What city/town did you grow up in?" The answer given by the account user was "Crescent." That account was opened on 20 February 2010 and the last login was 17 April 2010. **PE 139 for ID** is the second account screenshot with BATES number: 00374394.

7. To pull the logs associated with the accounts with the user names "bmanning" and "bradass87," I wrote a sql query and entered it into the database. In the query, I asked the database to pull all the audit events by the users "bmanning" and "bradass87." Sql is a structural query language for extracting and inserting in a database. It is a standard computer language to interact with databases. In other words, sql is a tool used to perform inquiries and pull data from a database. The sql query pulled the logs and put them into a readable format. In order to accomplish the sql query, I went to the black command prompt screen, typed in the query, hit enter, and the computer generated the logs. I then saved the logs as well as the sql query I used to pull those logs. A computer-generated process pulls the logs, and I did not format them as sql does it automatically. I then saved the logs.

8. I will explain the logs by column and using following line pulled from the "bradass87_distinct_export_with classifications.xls":

AUDIT_EVENT_ID	DATE_TIME	ACTOR	AUDIT_ACTION	TARGET	DATA_NAME	DATA_VALUE
36135654	20-FEB-10 04.45.52.000000000 AM	bradass87	Viewed Holding	11943026	TITLE	Daily Tells UK, Dutch To Stop 'Bullying', Accept Iceland's Compensation Offer (U)

a. Column 1 is the audit event identification, which is the system generated number assigned numerically to events. An event is data received, like looking at a document. Each different

FOR OFFICIAL USE ONLY

event has a different line on the audit data; however, each action has the same audit event identification. Therefore, there may be several lines to describe one action, which all have the same audit event identification. In the above example line, the audit event id is 36135654.

b. Column 2 is the Date/Time Group logs the date and time of the event. In the above example line, the date/time group is 20-Feb 10 at 04:45:52.000000000 AM.

c. Column 3 is the actor. It is the user account that is creating the event. In the above example line, the actor is "bradass87." That was the user account name for a SIPRNET OSC account with the name "Bradley Manning."

d. Column 4 is the audit action, which tells you what the user did on the OSC website. In the above example line, the audit action is "viewed holding." This means the document whose title appears in the data value column was opened by the "bradass87" user account.

e. Column 5 is the target. The target identifies what the user was accessing on the OSC website. In the logs that we pulled for this case, the targets were most often numbers that identified specific documents or other areas of the website the user clicked on, such as Topic Countries. In the above example line, the target is 11945572, which is a document.

f. Column 6 contains the data name, which further describes the target as well as the next column, the data value column. In the above example, the data name is title. That means that the target was the document and the data value in the following column is the title of the document.

g. Column 7 is the data value, which is what the data actually is. In the above example line, the data value is the title "Daily Tells UK, Dutch To Stop 'Bullying', Accept Iceland's Compensation Officer (U)."

h. To summarize, the above example means that the user "bradass87" clicked on the page with the document entitled "Daily Tells UK, Dutch To Stop 'Bullying', Accept Iceland's Compensation Officer (U)" on 20 February 2010. I know the page opened and the document displayed; otherwise, the action would not have logged.

9. In this case, I also conducted a sql search of the database for all the document titles that were viewed by the user account "bradass87." I saved them as "bradass87_sum_export_with classifications." I did this as it was an easier format to view what document titles were viewed by the user. Using the above example and "bradass87_sum_export_with classifications" you can match the target, which contains the holding identification with the document title. In the above example, the target (and holding identification) is 11945572, which again, matches with the title "Daily Tells UK, Dutch To Stop 'Bullying', Accept Iceland's Compensation Officer."

10. Based upon the review of the audit logs, it appears that "bmanning" began using his account on 26 November 2009 and looked at Homeland Security information. He did not conduct any activity on his account after that date. The subsequent two dates are automatic entries to track the lapsing and expiration of the accounts. **PE 14b for ID** are the OSC logs for the user account "bmanning."

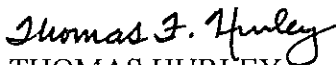
FOR OFFICIAL USE ONLY

11. Based upon the review of the audit logs, it appears that "bradass87" began using the OSC on 20 February 2010 and looked at a variety of documents associated with Wikileaks and Iceland. The "bradass87" account was last used on 17 April 2010. PE [u] for ID are the OSC logs for the user account "bradass87."

12. The information I provided is computer generated and only limited people have access to the information. I have no reason to believe that the information I provided was not accurate. On 29 June 2012, I attested to the authenticity of the OSC log files, containing the following logs, with the following date ranges: "bmanning_distinct_export_with_classification.xls" (date range 6 November 2009 to 9 November 2010); "bradass87_distinct_export_with_classification.xls" (date range 20 February 2010 to 17 April 2010); "bradass87_sum_export_with_classification.xls" (no date range). The logs that I attested to in this case were in the excel format. Although I originally pulled the logs in a different format, the content was identical to the logs that I pulled. In the same 29 June 2012 attestation, I attested to the authenticity of the OSC user information files entitled Opensource.gov-bmanning.pdf and Opensource.gov-bradass87.pdf. This attestation is BATES number 00505184.



ANGEL M. OVERGAARD
CPT, JA
Assistant Trial Counsel



THOMAS HURLEY
MAJ, JA
Defense Counsel



BRADLEY E. MANNING
PFC, USA
Accused