

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. Stephen Buchanan

9 June 2013

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

1. I work as a contractor for the National Security Agency (NSA). I provide support to Intelink. Intelink is a software suite operating on U.S. Government private networks which provides Internet-like services to enable collaboration between intelligence agencies within the U.S. Government. Primarily, it includes a web-based search engine of UNCLASSIFIED, SECRET, and TOP SECRET information systems. It hosts blogs and allows for messaging, sharing files, and searching for UNCLASSIFIED, SECRET, and TOP SECRET information across agencies, to include Intellipedia for online collaboration and Passport account management. In my current position, I provide security for Intelink and serve as the Information Assurance (IA) Manager. This means that I make sure the systems work as they were intended. I work to ensure the systems are properly maintained and guard against their misuse. I have worked in this role for five years.
2. Prior to holding my current position, from 1999-2008, I was an Information System Security Engineer for Intelink. In this position, I made sure the systems were built correctly to perform their intended connection, search, and storage functions. Before that, I worked in systems support within the Intelligence Community (IC). In total, I have worked in the IA industry supporting different agencies in the IC since 1985.
3. I have two primary IA and information systems certifications. First, I am a Certified Information Systems Security Professional (CISSP). This means I have heightened experience in and knowledge of information security. CISSP is a globally recognized standard of achievement that confirms an individual's knowledge in the field of information security. The training covers all parts of information security, including personal and building security aspects. CISSP indicates that an individual has attained specialized knowledge in the field of IA in accordance with standards articulated in Department of Defense Directive 8570. In addition to CISSP, I also have the Information Technology Infrastructure Library (ITIL) Foundation certification. ITIL is the most widely adopted framework for IT Service Management in the world. ITIL provides a framework on technology systems management, particularly on how to build information management systems and manage them with a specific process.
4. In my role as IA Manager for Intelink, I am familiar with the audit logs created by Intelink. The Intelink system obtains, manages, and stores its own audit data through the course of its day-to-day operations. This data can be used to respond to user inquiries, troubleshoot technical problems, and monitor and maintain Intelink usage and performance. These logs are created anytime anyone makes a connection with a computer system. The system detects these connections from servers – tracking the workstation making the request of the system, how the request routes through the system, and where the request ultimately gets the information. These connection logs are made in real time and stored in data

PROSECUTION EXHIBIT 69 for identification  
PAGE OFFERED:        PAGE ADMITTED:         
PAGE 1 OF 4 PAGES

files every hour. They are computer-generated and only a very limited number of people have access to them.

5. Intelink logs contain audit data captured from proxy servers that control access to Intelink services and show the activities of users and systems that connect to and use the Intelink services while on classified or unclassified networks. We know the Intelink audit logs are accurate for several reasons. First, they write to a secure server. Second, only limited personnel have access to them. Third, they are reviewed by our team at least on a weekly basis to ensure that the reporting process is occurring properly – meaning to ensure that the log data is being written properly. The log data is useful to us because it shows us how our services are being used, whether Intelink services are functioning properly, and whether adjustments should be made. We can also use the data to solve technical issues, determine security risks, and review data trends that help us develop our management strategies. We can tell if there are errors because information the logs normally collect would be missing. If a data file had been corrupted while being written it would not open. Missing or corrupt data files are regenerated from the system. So, in short, the data these system logs have captured is complete and accurate.

6. I am involved in this case because we received a request to pull Intelink audit logs given Intelink could have been used to gather information that was ultimately compromised. At that time, we did not track users by log-in identifiers; instead, we tracked usage by IP address. One of the log data requests was for the Secure Internet Protocol Routing Network (SIPRNET) IP addresses 22.225.41.22 and 22.225.41.40 from October 2009 to June 2010. Intelink audit logs are stored on a Linux-based system. To pull the requested log, I performed a Linux search on the server. This means that I issued a line command telling the server what information I wanted to read. When the system returns the data, the system writes the data to a file. In reviewing the files returned, I could find no relevant information in the data files for October 2009 or June 2010. However, there was activity recorded for the relevant IP addresses for the months November 2009 through and including May 2010. I double checked to make sure there was no activity from the relevant IP addresses during October 2009 and then ran the search again to verify results. The results of the second search matched the results of my original search. The results are saved automatically as a .txt file so that they are readable to the person running the query. When I received the response to my IP/date query, I opened the file to make sure it was readable and that all the data had been reported properly. I did not alter the file in any way. I burned the file to a CD and then turned it over to Special Agent Mark Mander with Army CID. These logs are on the CD marked **Prosecution Exhibit (PE) 61 for identification**. The filenames of the Intelink logs that I attested to showing activity for IP address 22.225.41.22 are the following: JF10\_22.log; MAM10\_22.txt; and ND09\_22.log. The filenames of the Intelink logs that I attested to showing activity for IP address 22.225.41.40 are the following: JF10\_40.log; MAM10\_40.txt; ND09\_40.log. The file “JF10\_22.log” contains audit logs capturing activity for the 22.225.41.22 IP address in January and February 2010. The file “MAM10\_22.txt” contains audit logs capturing activity for the 22.225.41.22 IP address in March, April, and May 2010. The file “ND09\_22.log” contains audit logs capturing activity for the 22.225.41.22 IP address in November and December 2009. I used the same filename structure to capture the contents of the audit logs associated with the 22.225.41.40 IP address.

7. The particular log data I captured reported several things. I will use the following discrete line of data to show, by way of example, what the Intelink logs mean:

```
22.225.41.40 - - [29/Nov/2009:04:50:10+0000] "GET
/intelink.wip.ismc.sgov.gov/WebResource.axd?d=az7kDRRCqClT13zGP2InQ2&t=633627756757031
250 HTTP/1.1" 200 6665
```

"http://www.intelink.sgov.gov/search/default.aspx?q=hqda"  
"Mozilla/5.0%(Windows;%20U;%20Windows%20NT%205.1;%20en-  
US;%20rv:1.9.1.2)%20Gecko/20090729%20Firefox/3.5.2" "-"

8. The significance of the above line that was pulled from Intelink is the following:

(a) The "22.225.41.40" is the IP address. This indicates that a computer with that IP address made the request for information. Essentially, it provides an electronic location for the user using Intelink.

(b) The "29/Nov/2009:04:50:10+0000" is the date/time group. The time zone is reflected as the offset from Greenwich Mean Time (GMT). In this case, "+0000" shows no offset.

(c) The next entry is the action the user took. In this case, for example, you see "GET". This command indicates the user is seeking particular information on SIPRNET through Intelink. This action reflects the user clicking on something in the website.

(d) The next entry is the page being requested by the action above. Here, it is  
"/intelink.wip.ismc.sgov.gov/WebResource.axd?d=az7kDRRcqClTV13zGP2lnQ2&t=63362775675703  
1250 HTTP/1.1". Intelink.wip.ismc.sgov.gov is the registered name for Intelink, which is on the SIPRNET, a secret government system.

(e) The code of numbers after the information tells you whether the user's request was successful and to what degree. For example, the code "200" after particular information indicates that an internet home page (HTTP) was successfully accessed.

(f) The "6665" is the size in bytes of the information returned by the query.

(g) The entry "http://www.intelink.sgov.gov/search/default.aspx?q=hqda" tells me that the user searched for the term "hqda" on intelink.sgov.gov. "www.intelink.sgov.gov" is the SIPRNET internet address for the secret government system on which Intelink sits. In this entry, "search" is the specific Intelink service used and "q=hqda" represents the search query entered into the search box on the Intelink webpage on the specific computer with the IP address listed above.

(h) The entry "Mozilla/5.0" tells me that the user of the SIPRNET computer with an IP address of "22.225.41.40" was using version 5 of the Mozilla internet browser. Mozilla is a company that produced internet browser software similar to Microsoft Internet Explorer or Apple Safari.

(i) The entry "%20" represents a space in the line.

(j) The entry "(Windows;%20U;%20Windows%20NT%205.1;%20en-US;20rv:1.9.1.6)" tells me the user of the SIPRNET computer with an IP address of "22.225.41.40" was using a Windows NT workstation computer.

(k) The entry "%20Gecko/20090729%20Firefox/3.5.2" "-"" tells me that the user of the SIPRNET computer with an IP address of "22.225.41.40" was using a version of the Firefox internet browser, version number "3.5.2". Firefox is the specific name of the internet web browser program produced by the Mozilla company.

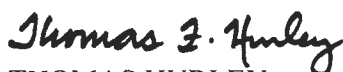
9. These Intelink logs only audit what happens on the Intelink systems. So, they can only tell you what a particular user IP address was doing when connecting with the Intelink system. It would reveal Intellipedia searches and other ways the user IP address used Intelink services by showing what files within Intelink that IP address accessed. At the time, users were not required to have Intelink Passport accounts to use most Intelink services, including the SIPRNET internet search and browsing. A SIPRNET Intelink Passport account is a username and password account established to allow access to some government websites. It is one of the many applications Intelink uses on its own internal systems to track what a user accesses. A user would need an account if he wanted to contribute to Intelink services or access certain websites or databases on SIPRNET, but not just to conduct searches. To create an account, a user would have to be on the SIPRNET, go to the account creation page, and insert personal information such as name, contact, and organizational information. The user is then notified via SIPRNET email with a code to use the first time he accesses the site. Other government organizations with websites and databases on SIPRNET, use SIPRNET Intelink Passport accounts to verify users before any user may access their information on SIPRNET.

10. Our Intelink organization maintains and stores the Intelink Passport account profiles of registered Intelink users. In response to a request by Army CID, I looked Bradley Manning up in our system. Someone with the name "Manning, Bradley E" did have an account. The user name of the individual was "bradley.e.manning". According to the user account, "bradley.e.manning" was in the military, his pay grade was E-4, and used an email address of "bradley.manning@us.army.smil.mil". The username is automatically generated based on the common name which is entered by the individual setting up the account. The user information includes each identifying factor (such as name, contact information, security questions and answers) that the user inputted into the system at the time of account creation. According to the Passport Account, the last time that the user logged in was 27 April 2010 at 1805:46 Zulu time. According to the Passport Account, the registration date was 11 October 2008. The Passport Account information is marked as **PE 62** for identification.

11. I signed an attestation on 22 June 2012 (BATES Number: 00505257) attesting to the authenticity of the what have been marked as PE 61 and PE 62 for identification and are the provided logs and the Intelink Passport account information for "bradley.e.manning", contained in the file "manning.ldif".



ANGEL M. OVERGAARD  
CPT, JA  
Assistant Trial Counsel



THOMAS HURLEY  
MAJ, JA  
Defense Counsel



BRADLEY E. MANNING  
PFC, USA  
Accused