

IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC
U.S. Army, (b) (6)
HHC, U.S. Army Garrison
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

)
)
) **RULING: GOVERNMENT**
) **MOTION TO ADMIT**
) **PROSECUTION EXHIBITS 31, 32,**
) **AND 109 FOR IDENTIFICATION**

) **DATED: 28 June 2013**
)

On 10 June 2013, after hearing testimony from Special Agent (SA) Mander, the Court ordered the parties to file briefs on the admissibility of Prosecution Exhibits (PE) 31, 32, and 109 for Identification (ID). On 15 June 2013, the parties filed briefs (Government at AE 567; Defense at AE 568). On 18 June 2013, the Court heard oral argument from counsel. On 27 June 2013, the Government recalled SA Mander and offered PE 31A and B and PE 32A and B for ID into evidence. The Court has considered the filings by the parties, evidence presented, the testimony of Special Agent (SA) Mander, and oral argument of counsel. The Court finds and rules as follows:

On 10 June 2013, the Government offered Prosecution Exhibits (PE) 31, 32, and 109 for ID into evidence through the testimony of SA Mander. On 27 June 2013, the Government offered PEs 31A and B and PEs 32A and B into evidence via additional testimony from SA Mander. The Government offers to authenticate PEs 31, 31A, 31B, 32, 32A, and 32B for ID in accordance with (IAW) MRE 901(b)(1) (Testimony of a Witness with knowledge – SA Mander) and MRE 901(b)(4) (Distinctive Characteristics and the Like: the appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances). The Government offers to authenticate PE 109 for ID as a self-authenticating business record IAW MRE 803(6) and MRE 902(11) and IAW MRE 901(b)(1) (Testimony of a Witness With Knowledge) through the testimony of SA Mander and the attestation by Mr. Christopher Butler, Office Manager of archive.org (AE 567, enclosure 1).

Findings of Fact:

PEs 31, 31A, 31B, 32, 32A, and 32B for ID.

1. PE 31 and 32 for ID are screen captures from Google Cache, a website that archives past versions of other websites. In this case, PE 31 and 32 for ID are Google Cache archives of WikiLeaks' [twitter.com](https://twitter.com/wikileaks) postings. SA Mander is unfamiliar with the process of how google cache archives web postings.
2. WikiLeaks has an account on the twitter website. Twitter accounts post messages in chronological order with the most recent on top. All published messages remain on the site indefinitely. On or about August 2012, SA Mander accessed the WikiLeaks account on twitter through a google search. The WikiLeaks account or "feed" had thousands of messages, making searches for particular tweets onerous directly through the WikiLeaks feed. SA Mander then looked for specific WikiLeaks tweets by using search terms on google. The search terms caused google to pull up the twitter website with the tweets in PE 31A and PE 32A for ID. PE 31A and PE 32A for ID are screen captures taken by SA Mander on or about August 2012 while he was reviewing the WikiLeaks tweets on the twitter

website. SA Mander typed the uniform research locator (URL) address of each tweet in a text box in the screen capture. The URL for PE 31A for ID is <http://www.twitter.com/#!/wikileaks/status/13570878440>. The URL for PE 32A for ID is <http://www.twitter.com/#!/wikileaks/status/7530875613>. SA Mander personally viewed the WikiLeaks twitter account and found that the tweets on the account have the same web address except for a serial number unique to each tweet. SA Mander visited the twitter page for WikiLeaks on or about 3 June 2013 and, again, on 27 June 2013. On 27 June 2013, SA Mander typed in the URL of PE 32A in a google search and retrieved the twitter website with the tweet in PE 32B. From the twitter website, SA Mander then typed in the URL for PE 31A and retrieved the tweet in PE 31B. SA Mander took screen shots of both tweets. PE 31B and PE 32B have the same URL as PE 31A and 32A except that PE 31B and PE 32B begin the URL with "https" rather than "http" and they do not have the "/#!/". Nevertheless, a search using the URL for PEs 31A and 32A for ID in google retrieves PEs 31B and 32B for ID. Also on 27 June 2013, SA Mander went directly to the WikiLeaks feed on twitter to try to find the tweets in PE 31 and 32 for ID. The feed would not let him have access to messages prior to March, 2013. SA Mander has never viewed the tweets in PE 31 and 32 for ID directly from the WikiLeaks twitter feed.

3. PEs 31, 31A, 31B, 32, 32A, and 32B for ID have the following distinctive characteristics attributable to WikiLeaks: the tweets feature the WikiLeaks logo; they feature WikiLeaks name as the account name "WikiLeaks" used on Twitter; the serial numbers the URL are the same for PEs 31, 31A, and 31B for ID; the serial numbers for the URL of PEs 32, 32A, and 32B are the same; and the content of the tweets in the PE 31 for ID series of exhibits and the PE 32 for ID series of exhibits relates to the information allegedly compromised by PFC Manning.

4. The date and time of the tweets in PEs 31, 31A, and 31B for ID are the same and are actually on the tweets themselves and not generated from Google.cache or any other internet archive process. PE 31, 31A, and 31B are screen images of the same tweet with the WikiLeaks label, logo, text, time/date, and URL serial number. The same is true for the date and time of the tweets in PEs 32, 32A, and 32B for ID.

PE 109 for ID

1. PE 109 for ID is a screen capture from archive.org, another website that archives past versions of websites from across the internet. More specifically, PE 109 for ID is a webpage from archive.org purporting to show a [WikiLeaks.com](http://wikileaks.com) webpage available on the internet on 5 November 2009 at 06:13:30.

2. SA Mander has not viewed the original [WikiLeaks.com](http://wikileaks.com) webpage that the archive.org webpage purports to have archived as PE 109 for ID. He also has no personal knowledge of the methods or standards employed by archive.org in creating and maintaining their web pages or with methods or standards used to capture web pages by third party donors to archive.org.

3. On 15 June 2013, the parties submitted briefs on the admissibility of PE 31, 32, and 109 for ID. As additional evidence to authenticate PE 109 for ID IAW MRE 902(11) and MRE 901(b)(2), the Government submitted an Attestation Certificate from Mr. Christopher Butler, Office Manager of archive.org dated 12 June 2013 (AE 567, Enclosure 1). The attestation reads:

I swear or affirm that each of the following is true regarding the attached records to the best of my knowledge and belief:

1. I am an employee familiar with the manner and process in which these records are created and maintained, by virtue of my duties and responsibilities;

2. to the best that the electronic systems involved can accurately record and reflect, such files were captured at or near the time of the date reflected in the URL assigned to each file by virtue of an automated transfer of electronic data.

3. such records were captured by Internet Archive or received from third party donors in the course of regularly conducted business activity by the Internet Archive;

4. The records are true and accurate copies of the original documents in Internet Archive's Wayback Machine service at web.archive.org.

The Court notes the attached record to this attestation is entitled "Draft: The Most Wanted Leaks of 2009-sort" with the same content and URL as PE 109 for ID.

4. The Defense also submitted an attestation from Mr. Butler dated 13 June 2013 (enclosure 10 of the Defense brief - AE 568). The attestation reads as follows:

1. I am the Office Manager at the Internet Archive, located in San Francisco, California. I make this declaration of my own personal knowledge.

2. The Internet Archive is a website that provides access to a digital library of Internet sites and other cultural artifacts in digital form. Like a paper library, we provide free access to researchers, historians, scholars, and the general public. The Internet Archive has partnered with and receives support from various institutions, including the Library of Congress.

3. The Internet Archive has created a service known as the Wayback Machine. The Wayback Machine makes it possible to surf more than 240 billion pages stored on the Internet Archive's web archive. Visitors to the Wayback machine can search archives by URL (i.e. a website address). If archived records for a URL are available, the visitor will be presented with a list of available dates. The visitor may select one of those dates and then begin surfing on an archived version of the Web. The links on the archived files, when saved by the Wayback Machine, point to other archived files (whether HTML pages or images). If a visitor clicks on a link on an archived page, the Wayback Machine will serve the archived file with the closest available date to the page upon which the link appeared and was clicked.

4. The archived data made viewable and browseable by the Wayback Machine is compiled using software programs known as crawlers, which surf the Web and automatically store copies of web files, preserving these files as they exist at the point of time of capture.

5. The Internet Archive assigns a URL on its site to the archived files in the format [http://web.archive.org/web/\[Year in yyyy\]\[day in dd\]\[Time code in hh:mm:ss\]/\[Archived URL\]](http://web.archive.org/web/[Year in yyyy][day in dd][Time code in hh:mm:ss]/[Archived URL]). Thus, the Internet Archive URL <http://web.archive.org/web/19970126045828/http://www.archive.org/would> be the URL for the record of the Internet Archive home page HTML file (<http://www.archive.org/>) archived on January 26, 1997 at 4:58 a.m. and 28 seconds (1997/01/26 at 04:58:28). A web browser may be set such that a printout from it will display the URL of a web page in the printout's footer. The date assigned by the Internet Archive applies to the HTML file but not to image files linked therein. Thus images that appear on a page may not have been archived on the same date as the HTML file. Likewise, if a website is designed with "frames," the date assigned by the Internet Archive applies to the frameset as a whole, and not the individual pages within each frame.

6. Regarding archived files stored in and made available via the Wayback Machine, I further declare that:

A. to the best that the electronic systems involved can accurately record and reflect, such files were captured at or near the time of the date reflected in the URL assigned to each file by virtue of an automated transfer of electronic data;

B. such records were captured by Internet Archive or received from third party donors in the course of regularly conducted activity by the Internet Archive; and

C. the Internet Archive captures, stores, and receives from third party donors web data as a regular practice.

7. The web archives for the year 2009 in the Wayback Machine at web.archive.org were largely obtained from third-party organizations, which donated the archived data, captured by automatic electronic systems, to the Internet Archive. I do not affirm that these web archives were set forth by, or from information transmitted by, people with knowledge of the information recorded therein.

8. This document is the Internet Archive 's standard affidavit, the affidavit Internet Archive normally provides to parties seeking to use Wayback Machine records as evidence in legal proceedings, with additional language provided in paragraphs 6-8.

9. Attached hereto as Exhibit A are true and accurate copies of printouts of the Internet Archive's records of the HTML files for the URLs and the dates specified in the footer of the printout.

10. I declare under penalty of perjury that the foregoing is true and correct.

The Court notes that Exhibit A contains a document entitled "Draft: The Most Wanted Leaks of 2009" that is similar to DE F but not identical as it contains additions, deletions, and changes. The URL is: http://web.archive.org/web/200911042112937/http://WikiLeaks.org/wiki/Draft:The_Most_Wanted_Leaks_of_2009. Thus, there are at least 3 versions of "Draft: The Most Wanted Leaks of 2009 available on the Internet today.

Hearsay/Relevance (the Court refers to PEs 31, 31A, and 31B for ID together as PE 31 for ID and refers to PEs 32, 32A, and 32B for ID as PE 32 for ID for purposes of Hearsay/Relevance findings of fact. The PE 31 and PE 32 series of exhibits are the same 2 tweets, thus hearsay/relevance findings are the same for all the exhibits in the series.

1. Defense asserts that PEs 31 and 32 for ID and PE 109 for ID are hearsay in that (1) the statement by the webpage or tweet itself is hearsay; (2) the statement of the individual who allegedly captured the site and relayed the information to achive.org or Google.cache is hearsay; and (3) the statement of archive.org or Google.cache is hearsay.

2. The Government offers PEs 31, 32, and 109 for ID not for the truth of the matters asserted within the exhibits. Rather, they offering these exhibits to show the effect that they may have had on PFC Manning. The Government asserts that, to the extent the contents of PEs 31, 32, and 109 for ID could have influenced PFC Manning, the exhibits are relevant. Defense asserts the Government has presented no evidence that PFC Manning saw or was aware of PEs 31, 32, or 109 for ID, therefore they are not relevant to any fact of consequence.

3. The Government theory of the case with respect to PE 109 for ID is that PFC Manning viewed the WikiLeaks Most Wanted List directly from the WikiLeaks webpage as depicted in PE 109 for ID on or

after 5 November 2009 not that PFC Manning viewed the list as depicted in PE 109 for ID from the archive.org website.

4. The Government has presented no forensic evidence that the tweets in PE 31 and 32 for ID or the “Most Wanted List of 2009” in PE 109 for ID were downloaded by PFC Manning. The Government has offered evidence that PFC Manning conducted searches for WikiLeaks and OpenSource.gov on Intelink; evidence of chats between PFC Manning and Press Association/Julian Assange that discussed OpenSource.gov; and evidence that when conducting searches on Intelink, when the searcher pulls up a website and proceeds to search within that website, Intelink no longer captures the search data.

The Law.

1. Evidence must be relevant to be admissible. MRE 402.
2. Evidence is relevant if it has the tendency to make a fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence. MRE 401.
3. Hearsay is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted. MRE 801(c).
4. Hearsay evidence is inadmissible unless an exception applies or the evidence is offered for a purpose other than to prove the truth of the matter asserted. MRE 802. This rule applies to testimony given by witnesses at trial and to exhibits to the extent that exhibits contain statements.
5. Statements offered to prove the effects those statements may have had on a listener, or reader, are not offered to prove the truth of the matter asserted and, therefore, may be considered for that limited non-hearsay purpose.
6. Exhibits require authentication as a condition precedent to their admission. The requirement of authentication is satisfied by evidence sufficient to support a finding that the exhibit in question is what its proponent claims. MRE 901(a); *U.S. v. Lubich*, 72 MJ 170 (C.A.A.F. 2013).
7. Authentication is an issue of conditional relevance. MRE 104(b) and MRE 1008 govern the inquiry under MRE 901. Thus, the Court may consider only evidence offered by the proponent that is admissible at trial to make a preliminary determination whether the exhibit(s) are sufficiently authenticated for the fact-finder to make a determination that they are authentic. *Lubich*, (“MRE 901 is the same as Federal Rule of Evidence (FRE) 901 and embraces the well-established view that authentication is a component of relevancy.” And citing *U.S. v. Blanchard*, 48 M.J. 306, 309 (C.A.A.F. 1998) “federal court of appeals decisions applying these principles would be most helpful.”). FRE 901 advisory committee’s note “The requirement of showing authenticity or identity falls in the category of relevancy dependent upon fulfillment of a condition of fact and is governed by the procedure set forth in Rule 104(b).” Thus, only admissible exhibits may be considered by the Court in making its preliminary determination.
8. Two methods of satisfying the authentication requirement, and the methods attempted by the Government in moving for admission of PEs 31, 31A, 31B, 32, 32A ID, and 32B are: (1) through a witness with knowledge that the exhibit is what it is claimed to be. MRE 901(b)(1) and (2) evidence of distinctive characteristics and the like. MRE 901(b)(4).

9. There are no military cases directly addressing the authentication requirements of online webpage archives. However, there are federal and state cases that have addressed authentication of online webpage archives.

a. Self Authenticated Business Record MRE 902(11)/MRE 803(6): The Government has provided no authority where a court addressing a challenge to authentication has ruled that online webpage archives from a non-government source are self-authenticating business records. The authority is to the contrary. *In re Homestore.com., Inc. v. Securities Litigation*, 340 F.Supp.2d 769 (C.D. Cal. 2004) (Printouts from a web site do not bear the indicia of reliability demanded for other self-authenticating documents under FRE 902) .

b. Testimony by a Witness With Knowledge: Several federal courts have addressed challenges to authentication of archived websites by a witness with knowledge under FRE 901(b)(1). Courts addressing the issue squarely have agreed that the admission of such webpages must be predicated either upon the testimony of an employee of the archiving company or upon the testimony of someone having personal knowledge of the contents of the archived webpages such that the witness can testify that the archived copy is accurate. The only criminal case relied upon by the Government as authority to authenticate archived webpages IAW FRE 901(a)(1) is *U.S. v. Bansal*, 663 F.3d 634 (3rd Cir. 2011). In *Bansal*, the Government called a witness to testify about how the Wayback Machine website works and how reliable its contents are. The witness also compared the screenshots with previously authenticated and admitted images from the website at issue and opined based on her personal knowledge that they were authentic. The opinion did not identify who the witness was. The other two cases relied upon by the Government for the proposition that attestations by a witness with knowledge may be sufficient to authenticate archived webpages IAW FRE 901 are civil cases where confrontation is not at issue. *St. Luke's Cataract and Laser Institute, P.A. v. Sanderson*, 2006 W.L. 1320242 (M.D. Fla. 2006) and *Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*, 2004 WL 2367740 (N.D. Ill. 2004). Other courts addressing the issue include: *U.S. v. See, e.g., Sam's Riverside, Inc. v. Intercon Solutions, Inc.*, 790 F.Supp.2d 965, 980-982 (S.D. Iowa 2011) (Holding that an archive.org employee can authenticate archive.org webpages); *U.S. v. Shrum*, 2011 WL 1753488 at 1-3 (E.D. Arkansas 2011) (District court initially admitted archive.org webpage sponsored by a law enforcement witness but reconsidered and excluded it. Issue was whether the curative instruction to the jury was sufficient); *Netscape Communications Corp. v. Valueclick Inc.*, 707 F.Supp.2d 640, 644 at footnote 6 (E.D. Va 2010) (District court admitted archive.org website because sponsoring witness had seen original and could testify that the archive.org page was an accurate copy); and *Audi AG and Volkswagen of America v. Shokan Coachworks, Inc.*, 592 F.Supp.2d 246, 278 (N.D. New York 2008) ("Defendants correctly point out that the Adams Declaration cannot authenticate the search results from www.archive.org because such evidence may only be authenticated by a knowledgeable employee of the website.").

c. The only case presented to the Court by the parties that directly addresses authentication IAW FRE 901(a)(1) where a third party has donated an archived webpage to archive.org is a civil case, *Novak v. Tucow's, Inc.*, 2007 U.S. Dist. LEXIS 21269 (E.D.N.Y. 2007), *aff'd* 330 Fed. Appx. 204 (2nd Cir. 2009) (the information at issue was only as reliable as the third-party donor made it.)

10. The Court considers issues of hearsay and whether evidence should be excluded under MRE 403 as preliminary questions IAW MRE 104(a).

Conclusions of Law Authentication:

1. The Court will consider only admissible evidence offered by the proponent that will go before the fact-finder in making a preliminary determination regarding authentication.

2. PEs 31, 31A, 31B, 32, 32A, and 32B for ID have been properly authenticated IAW MRE 901(b)(1) via the testimony of SA Mander. Although PE 31 and 32 for ID are retrieved from Google.cache, SA Mander testified that he retrieved copies of the same tweets directly from twitter.com as PEs 31A and B and PEs 32A and B. These exhibits are also properly authenticated IAW MRE 901(b)(4) distinctive characteristics as set forth in the Court's findings of fact regarding these exhibits. PEs 31, 31A, 31B, 32, 32A, and 32B for ID are properly authenticated.

3. PE 109 for ID is not sufficiently reliable to be a self-authenticating business record IAW MRE 902(11) and MRE 803(6). For authentication IAW MRE 901, federal case law on the authentication issue is persuasive. A witness sponsoring the admission of archived webpages must either have knowledge of the archiving procedures used by the archiving entity and/or third party donor entity such that the witness can testify that the archive actually shows true copies of the websites they purport to archive or must have knowledge of the original webpage such that the witness can verify that the archived copy is a true copy of the original. The Government has advised the Court that it does not intend to admit the attestation by Mr. Butler (enclosure 1 of the Government's brief). Accordingly, this court finds that the Government has not properly authenticated PE 109 for ID and it is not admitted.

4. The PE 31 series of exhibits provide evidence that WikiLeaks or an entity purporting to be WikiLeaks posted a tweet on 7 May 2010, requesting a list of as many .mil email addresses as possible. The PE 31 series of exhibits is offered by the Government for non-hearsay purposes. PE 31 series of exhibits is offered as circumstantial evidence to show PFC Manning's intent to respond to WikiLeaks queries and his knowledge of the scope of disclosures WikiLeaks intended to make. The Government has introduced forensic evidence from SA Al Williamson that the accused downloaded the U.S. forces-Iraq Microsoft Outlook/Share-point Exchange Server global address list (GAL) between 11-27 May 2010. This evidence is relevant to the specification of Charge I (Aiding the Enemy) and specification 16 of Charge II (stealing, purloining, or knowingly converting the GAL between on or about 11 -27 May 2010).

5. The 8 January 2010 tweet in PE 32 series of exhibits states "Have encrypted videos of US bomb strikes on civilians <http://bit.ly/wlafghan2> we need supercomputer time <http://ljsf.org/>." The portion of the tweet stating "Have encrypted videos of U.S. bomb strike on civilians." is a statement. The Government offers the tweet (1) as a hearsay exception under MRE 803(3) (then existing state of mind) to demonstrate WikiLeaks publicized plan to compromise military information as of 8 January 2010; (2) for the non-hearsay purpose to show PFC Manning's awareness of WikiLeaks' openly and publicly posted plan to disclose classified information; (3) for the non-hearsay purpose of the publication of the tweet looking for assistance to unencrypt the video as circumstantial evidence to connect the timing of the tweet to the appearance on Mr. Jason Katz' computer on 15 December 2009 of an Afghan video with the same hash values as the Afghan video from the CENTCOM server allegedly communicated to WikiLeaks by PFC Manning; and (4) as a hearsay exception under MRE 803(3) to corroborate PFC Manning's admissions that he sent WikiLeaks an encrypted video in the internet chats. For the reasons proffered by the Government above PE 32 is relevant as evidence of PFC Manning's knowledge of the scope of WikiLeaks' intended disclosure for the specification of Charge I (Aiding the Enemy), specification 1 of Charge II (Wantonly Causing to be Published) and to prove willful communication of the Gharani video for specification 11 of Charge II.

6. PE 109 for ID is a request for information and is offered for the fact that the request was made not for the truth of the matter asserted. The Government offers PE 109 for ID for a non-hearsay purpose as circumstantial evidence that PFC Manning was aware of PE 109 for ID and his intent to gather information and send it to WikiLeaks. Although the Government has not presented evidence that the accused actually accessed PE 109 for ID, the Government has presented evidence that PFC Manning searched Intelink for WikiLeaks and for some of the information on PE 109 for ID. The Government also

presented evidence that when a person does an Intelink search and navigates to another website to continue the search, Intelink no longer captures the meta-data. The Court finds timing of the PE 109 for ID posting in conjunction with other evidence presented by the Government is relevant circumstantial evidence offered for a non-hearsay purpose to further the inference that PFC Manning was aware of the information requested by WikiLeaks in PE 109 for ID. Should PE 109 for ID be properly authenticated, it is relevant for the specifications in Charges I and II.

7. The Court has considered whether the probative value of PE 31 and 32 for ID series of exhibits is substantially outweighed by the danger of unfair prejudice under the criteria in MRE 403 and finds it is not. The Court as fact-finder will consider the evidence for the proper admissible purposes.

RULING: The Government motion to admit PEs 31, 31A, 31B, 32, 32A, and 32B for ID is **GRANTED**. The Government motion to admit PE 109 for ID is **DENIED**.

So **ORDERED** this 28th day of June 2013.



DENISE R. LIND
COL, JA
Chief Judge, 1st Judicial Circuit