IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES, Appellee, v. Heather D. LUBICH Electronics Technician Second Class (E-5) U.S. Navy Appellant.	APPELLANT'S BRIEF ON THE MERITS Crim.App. Dkt. No. 201100378 USCA Dkt. No. 12-0555/NA

TO THE JUDGES OF THE UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES:

KEVIN S. QUENCER
LT, JAGC, USN
CAAF Bar Number 35699
Appellate Defense Counsel
1254 Charles Morris Street, SE
Washington, DC 20374
(202) 685-8502

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Statutory Provisions

Military Rules of Evidence

Treatises

Granted Issue

II.

WHETHER THE MILITARY JUDGE ERRED BY OVERRULING DEFENSE COUNSEL'S FOUNDATION AND AUTHENTICATION OBJECTIONS AND ADMITTING COMPUTERIZED DATA EVIDENCE GATHERED BY AN UNNAMED NMCI ANALYST WHO USED AN UNIDENTIFIED PROCESS WITH UNKNOWN RELIABILITY TO COLLECT DATA RELATED TO APPELLANT'S NETWORK USER ACTIVITY.

Statement of Statutory Jurisdiction

ET2 Heather Lubich's approved court-martial sentence included a punitive discharge. Accordingly, her case fell within the Article 66(b)(1), Uniform Code of Military Justice (UCMJ) jurisdiction of the Navy-Marine Corps Court of Criminal Appeals (NMCCA).[1] She invokes this Court's jurisdiction under Article 67, UCMJ.[2]

Statement of the Case

A special court-martial composed of members with enlisted representation convicted ET2 Lubich, contrary to her pleas, of one specification of attempted larceny, one specification of wrongfully and knowingly transferring, possessing, or using a means of identification of another person, and one specification of impersonating a commissioned officer with the intent to defraud, in violation of Articles 80 and 134, UCMJ.[3] The members

[1] 10 U.S.C. § 866 (2006).
[2] 10 U.S.C. § 867.
[3] 10 U.S.C. §§ 880, 934.

sentenced ET2 Lubich to 45 days of confinement, a bad-conduct discharge, forfeiture of $1,300 pay per month for two months, and reduction to E-3. The convening authority approved the sentence as adjudged and, with the exception of the bad-conduct discharge, ordered the approved sentence executed.

The NMCCA issued its opinion in this case on April 19, 2012.[4] ET2 Lubich filed a timely petition for review with this Court on June 15, 2012 and asked for additional time to file her supplement, which this Court granted until July 5, 2012. This Court granted review on the above issue on September 6, 2012.

Statement of Facts

An unidentified NMCI computer analyst with unknown qualifications conducted a forensic analysis of ET2 Lubich's NMCI network activity. The analyst did not testify at trial. The process used for his or her analysis, its reliability, and the analyst's experience with the process are unknown. But the work performed by the mystery analyst determined that specific computer activity on the NMCI network was attributable to ET2 Lubich. The analyst then created a compilation of this data, formatted it in an unknown manner, and burned it to six CD-ROMs. The unknown person then gave the discs to NCIS. NCIS then used the data on those disks to produce two computer forensic reports

[4] *United States v. Lubich*, No. 201100378, slip op. (N-M. Ct. Crim. App. Apr. 19, 2012).

detailing the computer and internet activities of ET2 Lubich, which were used to convict ET2 Lubich at trial.

The only information about the data collected on those disks that emerged at trial came from Special Agent (SA) Erik Schmidt. SA Schmidt referred to them at trial as ET2 Lubich's "NMCI user data provided to us from the Information Assurance Department of NMCI."[5] SA Schmidt had no direct knowledge about how NMCI had collected user data on ET2 Lubich, but did testify that he had received some information on the subject over the phone. SA Schmidt testified that based upon phone conversations with NMCI, he believed that NMCI used an "automated" process to collect this data[6] and attempted to explain that process. But he admitted that his knowledge was based on this phone call explanation[7], that he was not fully familiar with NMCI's process[8], and that had no role in collecting the data:[9]

> DC: Special Agent Schmidt, have you ever worked at NMCI?
> A: No.
> DC: Are you currently an NMCI employee?
> A: No, I'm not.
> DC: Are you familiar with the software they use at NMCI?
> A: Some, not all.[10]
>
> . . .
>
> DC: Mr. Schmidt, there were several computers involved, the

[5] JA at 19.
[6] JA at 28.
[7] JA at 29.
[8] JA at 25,29.
[9] JA at 32.
[10] JA at 25.

data of several computers involved in this case, is that correct?
A: That is correct.
DC: Someone at NMCI had to verify which computers ET2 Lubich had used, correct?
A: Personally verified?
DC: Yes.
A: I couldn't tell you. I can't testify to that.
DC: So you're not familiar with that process then?
A: Not in the entire process in that manner, no. Just what they explained to me over the phone.[11]

. . .

DC: Just to verify again, Mr. Schmidt, with this [] data, you did not extract this data directly from any NMCI computer, correct?
A: Yeah, that is correct. I did not personally go---
DC: This data was placed in your hand in the form of a CD from somebody at NMCI?
A: Correct.[12]

The data on the disks provided by NMCI contained a vast amount of data that purported to be ET2 Lubich's work computer use, including: (1) websites visited,[13] (2) when those websites were visited,[14] (3) the usernames and passwords used to enter those websites,[15] and (4) other information, such as social security numbers, which were also used to log onto websites.[16]

Mr. Schmidt used forensic analysis software to analyze this data compilation to create a 179-page forensic report,

[11] JA at 29 (emphasis added).
[12] JA at 32.
[13] JA at 19.
[14] JA at 37.
[15] JA at 38.
[16] JA at 40.

Prosecution Exhibit 19,[17] and a 13-page forensic report, Prosecution Exhibit 23.[18] The Government offered these reports into evidence, but the defense objected[19] based upon authenticity, lack of personal knowledge, and the confrontation clause.[20] The military judge also recognized that foundation was in question.[21]

Among other things, the defense counsel objected that "someone in NMCI, I don't know who, pulled the data up," that the court had "no assurance on how this data was collected," "whether [NMCI] followed accurate approved techniques," "whether there's any chance the data could have been corrupted," and that there was no one "from NMCI testifying [about] the collection processes that took the data from ET2 Lubich's computers."[22]

The military judge overruled the defense's objection and admitted Prosecution Exhibits 19 and 23 into evidence, stating:

> I believe that argument goes more to the weight of the evidence. . . that the exhibits have been sufficiently authenticated and that the Confrontation Clause is not implicated because we're dealing with an automated process, no conclusions in these documents themselves and, again, it's an automated process with

[17] JA at 20.
[18] JA at 32.
[19] JA at 20.
[20] JA at 25.
[21] JA at 21.
[22] JA at 23.

> very little discretion involved on the part of the person that was obtaining the data.[23]

Mr. Schmidt then testified to the following from his forensic report:

- ET2 Lubich accessed the Omni Financial website 15 times, the last time on May 18, 2009.[24] The fraudulent loan was applied for through this website.
- ET2 Lubich accessed the Military.com website 150 times, the last time on April 21, 2009.[25] A military.com email address was used to apply for the loan.[26]
- The username "[Username]" was used for the Military.com website.[27]
- The password "[Password]" was used for the Military.com website.[28] This was ET2 Lubich's personal password.[29]
- ET2 Lubich's social security number was used to log on to the Omni Financial website.[30]
- ET2 Lubich entered ENS L's social security number into the Omni Financial website on March 25, 2009, the date the loan was applied for online.[31]

Trial counsel repeatedly highlighted the importance of Prosecution Exhibits 19 and 23 in his closing argument.[32] In addition to stressing the above facts, the Government also used

---

[23] JA at 34.
[24] JA at 37.
[25] JA at 38.
[26] R. at 299.
[27] JA at 40.
[28] JA at 40.
[29] R. at 612.
[30] JA at 40-41.
[31] JA at 41.
[32] JA at 57, 58, 60, 62, 66.

these exhibits to prove motive. The Government pointed to ET2 Lubich's frequent visits to online shopping sites, for example, and argued that she planned to use the $10,000 to fund her online shopping sprees.[33]

Summary of the Argument

This Court should hold that the Military Judge erred when he overruled the defense's timely objection to the data collected by NMCI. This Court should also find that this error prejudiced ET2 Lubich because the trial counsel repeatedly pointed to the erroneously admitted evidence during his closing arguments and even urged the members to specifically use the erroneously admitted evidence as irrefutable proof of ET2 Lubich's guilt.

Argument

II.

THE MILITARY JUDGE ERRED BY OVERRULING DEFENSE COUNSEL'S FOUNDATION AND AUTHENTICATION OBJECTIONS AND ADMITTING COMPUTERIZED DATA EVIDENCE GATHERED BY AN UNNAMED NMCI ANALYST WHO USED AN UNIDENTIFIED PROCESS WITH UNKNOWN RELIABILITY TO COLLECT DATA RELATED TO APPELLANT'S NETWORK USER ACTIVITY.

[33] JA at 56-58.

Standard of Review

A military judge's decision to admit evidence is reviewed for an abuse of discretion.[34] "'Abuse of discretion' is a term of art applied to appellate review of the discretionary judgments of a trial court. An abuse of discretion occurs when the trial court's findings of fact are clearly erroneous or if the court's decision is influenced by an erroneous view of the law."[35]

Discussion

The Government admitted a large amount of user data purported to be from ET2 Lubich's NMCI account, but did so through the testimony of an NCIS agent, SA Schmidt, who did not gather the data, did not understand the process NMCI used to collect the data, and did not know what software NMCI used to do so. Furthermore, SA Schmidt did not and could not testify that the system NMCI used to gather and report this data was reliable, accurate, in good working order, and produced trustworthy results.

A. Authenticating computerized data evidence.

When the proponent of computerized data tries to enter data into evidence, the proponent bears the burden of establishing

[34] *United States v. Freeman,* 65 M.J. 451, 453 (C.A.A.F. 2008), (citing *United States v. Ayala,* 43 M.J. 296, 298 (C.A.A.F. 1995)).
[35] *United States v. Freeman,* 65 M.J. 451, 453 (C.A.A.F. 2008).

the accuracy and reliability of that data.[36] This can be done by introducing "evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result."[37]

Computerized data evidence raises unique issues concerning authenticity and accuracy because there are many potential pitfalls in the collection, storage, and production of computer data.[38] The "accuracy [of the data] may be impaired by incomplete data entry," for example, and there may be "mistakes in output instructions, programming errors, damage and contamination of storage media, power outages, and equipment malfunctions."[39] Later, when the data is being compiled and presented to law enforcement, "the integrity of [the] data may [] be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling."[40]

Some courts and commentators have recognized that "early versions of computer foundations were too cursory, even though the basic elements covered the ground. . . . [Those were that] a qualified witness must testify as to the mode of record

---

[36] *Lorraine v. Mack*, 241 F.R.D. 534, 557, n.34, 2007 U.S. Dist. LEXIS 33020 (D. Md. 2007)(quoting MANUAL FOR COMPLEX LITIGATION § 11.447 (4th ed. 2004)).
[37] MIL.R.EVID. 901(b)(9), MANUAL FOR COURTS-MARTIAL, UNITED STATES (2008 ed).
[38] *Lorraine*, 241 F.R.D. at 557, n.34.
[39] *Id*.
[40] *Id*.

preparation, that the computer is the standard acceptable type, and that business is conducted in reliance upon the accuracy of the computer in retaining and retrieving information."[41]

One modern court has refined its standards for authenticating computerized data evidence and adopted an eleven-step process to determine when a piece of computerized data is authentic and reliable.[42] These factors include whether:

(1) The business uses a computer;

(2) The computer is reliable;

(3) The business has developed a procedure for inserting data into the computer;

(4) The procedure has built-in safeguards to ensure accuracy and identify errors;

(5) The business keeps the computer in a good state of repair;

(6) The witness had the computer readout certain data;

(7) The witness used the proper procedures to obtain the readout;

(8) The computer was in working order at the time the witness obtained the readout;

(9) The witness recognizes the exhibit as the readout;

(10) The witness explains how he or she recognizes the readout; and

---

[41] *In Re Vee Vinhee*, 336 B.R. 437, 445-46 (B.A.P. 9th Cir. 2005) (citing BARRY RUSSELL, BANKRUPTCY EVIDENCE MANUAL P803.17 (2005)).
[42] *In Re Vee Vinhee*, 336 B.R. at 446 (citing EDWARD J. IMWINKELREID, EVIDENTIARY FOUNDATIONS § 4.03[2] (5th ed. 2002)).

(11) If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms.[43]

Other courts have adopted similar standards. At the heart of each standard, however, is the requirement that the proponent of computerized data evidence must show that the system that created the evidence is reliable and produces trustworthy and accurate results.[44]

Here the testimony of SA Schmidt did not establish the reliability, accuracy, or trustworthiness of the data NCIS received from NMCI. His rough understanding of the process was not based on personal experience with the process or experience with the collection that occurred in this case. He didn't testify about any procedural safeguards or other indications that the data collection by NCMI was reliable. Therefore he could not establish that the collection of data by NMCI was done by a system that produces accurate and reliable results.

In *People v. Taylor*, the Supreme Court of Illinois discussed factors it and other courts have considered when determining whether an analogous piece of evidence -- photos

---

[43] *Id*.

[44] *Lorraine*, 241 F.R.D. at 564-55 (quoting *State v. Hall*, 976 S.W.2d 121, 147 (Tenn. 1998)("the admissibility of the computer tracing system record should be measured by the reliability of the system, itself relative to its proper functioning and accuracy"); *State v. Dunn*, 7 S.W.3d 427, 432 (Mo. Ct. App. 2000)("the admissibility [of computer generated telephone records] should be determined on the reliability and accuracy of the process involved")).

taken by an automated surveillance camera -- is authentic.[45] These include: (1) the operating condition and capability of the equipment used, (2) the reliability of the equipment used, (3) the competency of the operator, (4) the lack of alterations, (5) the operating procedures used, and, *inter alia*, (6) the quality of the recorded product.[46]

This Court in *United States v. Harris*, like *Taylor*, discussed the authentication of surveillance footage and now can apply *Harris's* evidentiary standards to computerized data evidence.[47] In *Harris*, this Court held that the photos in question were authenticated because evidence at trial showed that (1) the automated camera system was reliable, (2) the system was in good working order when the photos were taken, and (3) the photos were properly safeguarded and handled from the time they were taken until the date of trial.[48]

Applying the standard set forth by this Court to surveillance footage in *Harris*, there was no testimony that the system that produced the data on the disks from NMCI was reliable, and no evidence regarding the handling of that data at

---

[45] 956 N.E.2d 431 (Ill. 2011).
[46] *Id.* (citing *United States v. Harris*, 55 M.J. 433, 439-40 (C.A.A.F. 2001); *Ex Parte Fuller*, 620 So.2d 675, 678 (Ala. 1993); *Wagner v. State*, 707 So.2d 827, 831 (Fla. Dist. Ct. App. 1998); *Edwards v. State*, 762 N.E.2d 128, 136 (Ind. Ct. App. 2002); *Washington v. State*, 961 A.2d 1110, 1116 (Md. 2008)).
[47] 55 M.J. 433.
[48] 55 M.J. at 439-40.

any point during NMCI's data collection procedures before it was handed to NCIS. Indeed the only witness that testified on the subject, SA Schmidt, had at best a limited understanding of what happens generally at NMCI, and was even less clear on how the data was collected in this case. He did not testify about the reliability or procedural safeguards in place to ensure the data was collect reliably. Nor did SA Schmidt testify about how the data was handled during NMCI's collection process before he received it at NCIS. This testimony is insufficient to establish the process used or the reliability of that process.

B. NMCCA's decision cites conflicting standards, and then incorrectly determined that SA Schmidt's testimony was sufficient to authenticate the underlying data produced by NMCI.

The court below cites several different authentication standards in its opinion, each of which differs from the other.

First, the court cited its earlier unpublished decision in *United States v. Fisher*[49] for the proposition that the proponent of a computer-generated report must do two separate and independent things to authenticate the report: (1) "authenticate the exhibit as the print-out it purports to be, as well as (2) authenticate the process by which it was prepared to show that the print-out produced accurately reflects the input data."[50]

Then the court stated that an exhibit may be authenticated

[49] No. 2010000287, 2011 CCA LEXIS 122, at *8 (N-M. Ct. Crim. App. Jun. 30, 2011).
[50] *Lubich*, slip op. at 5 (emphasis added).

if a witness can testify with knowledge that "a matter is what it is claimed to be" or if evidence can be produced "describing a process or system used to produce a result and showing that the process or system produces an accurate result."[51]

But earlier, the decision cites to *United States v. Duncan*,[52] a published 1990 Navy-Marine Corps Court of Military Review case that appears to be the last comprehensive published opinion from the Navy-Marine Corps court dealing with the authentication of computerized data evidence.[53] *Duncan* states that "the most direct manner of authenticating a process or system . . . would seem to be by the expert testimony of an engineer or systems analyst, but we believe that the reliability of a process or system may also be established circumstantially, as through the testimony of a user of the process or system *who can describe its error-free operation over a suitable period of time*."[54]

But even in articulating or citing to three arguably different standards, the lower court's opinion does not properly address the underlying problem with the evidence, that ET2 Lubich was convicted using data that was collected by an unknown NCMI employee with unknown qualifications using an unknown

---

[51] *Id.* at 5.
[52] 30 M.J. 1284, 1289 (N.M.C.M.R. 1990).
[53] *Lubich*, slip op. at 4.
[54] 30 M.J. at 1289 (emphasis added).

method of data collection with unknown reliability and accuracy. The court below stated that:

> Taking into account this record as a whole, the testimony of Mr. Schmidt was sufficient to authenticate PE 19 and PE 23. He described the process by which the raw data from the appellant's NMCI account was downloaded onto CD-ROMs, and the process by which he generated PE 19 and PE 23 from that raw data.[55]

This view is correct in that SA Schmidt could authenticate his own work, forensic reports culled from data provided by NMCI. But it is incorrect in that the testimony of SA Schmidt could not authenticate the underlying data he used, the NMCI collected data, which was the subject of the defense objection.

C. The Government did not properly authenticate ET2 Lubich's user data.

Regardless of the authentication standard used, the Government did not properly authenticate ET2 Lubich's user data. SA Schmidt did not know if the data was in fact ET2 Lubich's data, that the data was complete, or that the data was accurately collected. Nor did he have any knowledge of the reliability or procedural safeguards to ensure reliability present in the system. SA Schmidt did not testify -- nor could he -- that the system NMCI used to collect, maintain, and cull this data worked by consistently producing reliable results. All he could testify about was his rough understanding of what

[55] *Lubich*, slip op. at 5.

methods NCMI had used. This rough understanding came not through his own experience with the methods used, but rather through an incomplete description of those methods given to him over the phone. He did testify that he had received some information on the subject over the phone. SA Schmidt testified that based upon phone conversations with NMCI, he believed that NMCI used an "automated" process to collect this data[56] and attempted to explain that process. But he admitted that his knowledge was based on this phone call explanation[57], that he was not fully familiar with NMCI's process[58], and that had no role in collecting the data:[59]

> DC: Special Agent Schmidt, have you ever worked at NMCI?
> A: No.
> DC: Are you currently an NMCI employee?
> A: No, I'm not.
> DC: Are you familiar with the software they use at NMCI?
> A: Some, not all.[60]
>
> . . .
>
> DC: Mr. Schmidt, there were several computers involved, the data of several computers involved in this case, is that correct?
> A: That is correct.
> **DC: Someone at NMCI had to verify which computers ET2 Lubich had used, correct?**
> **A: Personally verified?**
> **DC: Yes.**
> **A: I couldn't tell you. I can't testify to that.**
> DC: So you're not familiar with that process then?

[56] JA at 28.
[57] JA at 29.
[58] JA at 25, 29.
[59] JA at 32.
[60] JA at 25.

> A: Not in the entire process in that manner, no. Just what they explained to me over the phone.[61]
>
> . . .
>
> DC: Just to verify again, Mr. Schmidt, with this [] data, you did not extract this data directly from any NMCI computer, correct?
> A: Yeah, that is correct. I did not personally go---
> DC: This data was placed in your hand in the form of a CD from somebody at NMCI?
> A: Correct.[62]

Therefore, while SA Schmidt could testify that his work produces accurate and reliable results, he could not testify that the data that underpinned his work was the product of a system that produced accurate and reliable results. And no one else testified on that subject.

As a result, all we know from the record is that a mystery NMCI analyst used an unknown process or system to obtain the data, the analyst burned the data to six CD-ROMs, and then gave the data to NCIS. Not only do we not know the name of this analyst or his qualifications, we do not know what steps he took to find this data, accurately determine its relevance, and save the information to CD-ROM.

Mr. Schmidt could not assure the court that the process NMCI used to collect, manage, and search for this data was reliable and accurate. As such, the Government did not properly authenticate Prosecution Exhibits 19 and 23.

---

[61] JA at 29 (emphasis added).
[62] JA at 32.

D. The admission of Prosecution Exhibits 19 and 23 was not harmless.

In *United States v. Durbin*, this Court stated that it evaluates prejudice from an erroneous evidentiary ruling by weighing (1) the strength of the Government's case, (2) the strength of the defense case, (3) the materiality of the evidence in question, and (4) the quality of the evidence in question.[63] The burden is on the Government to demonstrate that the error did not have a substantial influence on the findings.[64]

Here the Government cannot meet that burden. The Government's case was largely built around the testimony of SA Schmidt and his forensic analysis of the data (PE 19, 23) collected by NCMI, which was the evidence at issue. SA Schmidt testified that based on the data on the disks provided by NCMI he created forensic reports that became PE 19 and 23.[65] He testified that from his forensic reports created with the data from NMCI that ET2 Lubich had visited the loan website 15 times.[66] He also testified that from his reports he could determine that ET2 Lubich had utilized Ensign L's social security number on the loan website.[67] These are crucial allegations in a case where ET2 Lubich was charged with

[63] *United States v. Durbin*, 68 M.J. 271, 275 (C.A.A.F. 2010).
[64] *United States v. Diaz,* 69 M.J. 127, 137 (C.A.A.F. 2010).
[65] JA at 20, 30.
[66] JA at 37.
[67] Ja at 40, 41.

fraudulently seeking a loan from an online loan website with the name and identity of Ensign L.

Moreover, trial counsel repeatedly pointed to PE 19 and PE 23 in his closing, which shows just how important the trial counsel thought the evidence at issue was to the Government's case. During trial counsel's closing and rebuttal arguments, he stated:

> And what's really telling is somebody's internet history. And while it wasn't passed out to you throughout the trial, you're going to get it when you go back to deliberate, Prosecution Exhibit 19. It's 179 pages of internet history. It will tell you so much about the accused.[68]
>
> . . .
>
> What's critical here, members, is all the activity in the spring of 2009, and you'll see that in Prosecution Exhibit 19.[69]
>
> . . .
>
> You can see here this is the Military.com, the NTUSER.DAT, 143 Wiese . . . Americredit, 143 Wiese. . .she uses 143 Wiese on Kitchendining.com, on Debroot.net . . .[70]
>
> . . .
>
> And if this circumstantial evidence is not enough for you, members you have direct evidence. NTUSER.DAT files, these things do not lie. These things show that she is the one that stole Ensign L's identity and put his

[68] JA at 57.
[69] JA at 58.
[70] JA at 60.

> Social Security numbers into that database at Omni Financial.[71]

Moreover, in order to establish a financial motive to get a fraudulent loan, trial counsel argued that the data showed ET2 Lubich had spent enormous amounts of time online shopping for household items. Trial counsel stated that the data showed ET2 Lubich had been to the website for One Way Furniture 210 times, Ashley Furniture 125, Mattress Discounters 168 times, and Bedroom Furniture 222 times.[72] Trial counsel also argued that ET2 Lubich visited maid service websites 144 times, the Body Shop 226 times, and Bed, Bath, and Beyond 176 times.[73] This argument was based entirely on the erroneously admitted data collected by NMCI. Trial counsel also pointed to PE 19 and 23 to show that ET2 Lubich used one password throughout all the websites that she visits.[74] And ultimately the trial counsel argued that from the data collected by NMCI, it is clear that ET2 Lubich submitted the loan application to YesOmni.[75] The trial counsel repeatedly, throughout his closing argument, used the erroneously admitted evidence to convincingly establish motive, prove opportunity, draw direct connections to ET2 Lubich and the loan website, and even argue that the erroneously

---

[71] JA at 66 (emphasis added).
[72] JA at 57.
[73] JA at 58
[74] JA at 60.
[75] JA at 62.

admitted evidence directly shows that she stole Ensign L's identity. The Government cannot meet its burden to show that this evidence, featured so prominently in nearly every aspect of the Government's case, did not have a substantial influence on the findings.

Conclusion

The admission of the NMCI collected data was erroneous because there was insufficient evidence in the record to establish the reliability or accuracy of the data. Furthermore, the erroneous admission of the evidence was central to the Government's case, and therefore prejudiced ET2 Lubich.

WHEREFORE, Appellant respectfully requests that this Court set aside the conviction of ET2 Lubich.

/s/

KEVIN S. QUENCER
LT, JAGC, USN
CAAF Bar Number 35699
Appellate Defense Counsel
1254 Charles Morris Street, SE
Washington, DC 20374
(202) 685-8502

Certificate of Compliance

1. This brief complies with the type-volume limitation of Rule 24(c) because this brief contains approximately 4,600 words.

2. This brief complies with the typeface and type style requirements of Rule 37 because this brief has been prepared using a monospaced typeface on Microsoft Word with 12 point Courier New font.

CERTIFICATE OF FILING AND SERVICE

I certify that the foregoing was electronically delivered to the Court, Appellate Government Division, and to Code 40 on October 9, 2012.

/s/

KEVIN S. QUENCER
LT, JAGC, USN
CAAF Bar Number 35699
Appellate Defense Counsel
1254 Charles Morris Street, SE
Washington, DC 20374
(202) 685-8502