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 REPLY TO THE GOVERNMENT'S BRIEF 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

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.

1. SA Schmidt's testimony, which relayed the telephonic statement of an unknown NMCI employee giving a limited description of how NCMI searched for and collected data, was insufficient to authenticate the NMCI data as accurate and reliable.

The Government incorrectly argues that the testimony of SA Schmidt at trial was sufficient to authenticate the NMCI data that formed the basis of SA Schmidt's testimony.

When the proponent of computerized data attempts to enter data into evidence, the proponent bears the burden of establishing the accuracy and reliability of that data.[1] 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."[2]

In this case SA Schmidt had no personal knowledge of how the NMCI data he used was collected by NMCI. SA Schmidt testified that his knowledge regarding NMCI's system came from a

---

[1] *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)).

[2] MIL.R.EVID. 901(b)(9), MANUAL FOR COURTS-MARTIAL, UNITED STATES (2008 ed).

phone conversation he had with an unnamed employee at NMCI.[3] SA Schmidt testified, based on that phone call, that NMCI used an automated process to search and collect a user's data. But SA Schmidt also made clear that he was not familiar with what software NMCI used,[4] what level of human decision making and involvement existed,[5] and that his own knowledge was limited to what he received over the phone.[6]

Importantly, SA Schmidt's testimony did not cover many aspects of the NMCI system or process. SA Schmidt did not testify that the system used by NMCI was reliable, he did not testify that the system had been used for any given period of time by NMCI without problem, nor did he testify that the system used had produced accurate results in the past for NMCI. SA Schmidt did not testify about the NMCI technicians that conducted the data collection. Nor did SA Schmidt detail the qualifications, training, or experience the NMCI employees conducting the process possessed. SA Schmidt did not identify the type of software that was used, its reliability, or its accuracy.

[3] JA at 29.
[4] JA at 25.
[5] JA at 29.
[6] JA at 29.

SA Schmidt had never worked for NMCI, had never received any formal training in the methods used by NMCI, and he had never been involved in the actual collection of data by NMCI.[7]

This lack of personal knowledge is problematic for two reasons. First, the limited description given over the phone does not establish that the system used was accurate or reliable as required by M.R.E. 901(b)(9) and this Court's opinion in *United States v. Harris.*[8] Second, the only evidence admitted to prove the authenticity of the NMCI data was the statement of an unknown NMCI employee that SA Schmidt relayed to the military judge outside the presence of the members.

a. In order to authenticate a system or process, admissible evidence must be introduced that indicates the system or process used was reliable.

M.R.E. 901(b)(9) requires "Evidence...showing that the process or system produces an accurate result." In *United States v. Harris*, this Court held that automated video camera evidence could be authenticated if the automated video camera system was reliable.[9]

SA Schmidt did not and could not offer any evidence that could authenticate the accuracy and reliability of the NMCI data that he received. He did testify that through a phone call he

[7] JA at 25.
[8] MIL.R.EVID. 901(b)(9), MANUAL FOR COURTS-MARTIAL, UNITED STATES (2008 ed); *United States v. Harris*, 55 M.J. 433 (C.A.A.F. 2001).
[9] *Harris*, 55 M.J. at 439-40.

had been told that NMCI used an "automated process" to search for and collect data. In *In Re Vee Vinhee*, the court adopted an eleven-step process to determine when a piece of computerized data is authentic and reliable, and therefore admissible.[10] 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
(11) If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms.[11]

Other courts, while not always adopting a standard as detailed as *In Re Vee Vinhee*, 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.[12] Particularly when viewed

[10] *In Re Vee Vinhee*, 336 B.R. at 446 (citing EDWARD J. IMWINKELREID, EVIDENTIARY FOUNDATIONS § 4.03[2] (5th ed. 2002)).
[11] *Id*.
[12] *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

next to the eleven factors laid out *In Re Vee Vinhee*, the testimony of SA Schmidt is woefully deficient, and does not show that the NMCI data was the result of a reliable system that produces trustworthy and accurate results.

b. The only evidence at trial regarding the NMCI system and process for collecting data, a phone call from an unnamed NMCI employee, was hearsay evidence.

SA Schmidt testified that the only information he had regarding the system or process that NMCI used to collect user data came from a phone call with an unnamed person at NCMI.[13] He had no personal knowledge of the procedures used, so he relayed the statement regarding the procedures used from an unnamed NMCI employee. This was hearsay. It was the out of court statement of an unknown person at NMCI that was admitted for the truth of the matter asserted: How NMCI compiled the data in this case.

Hearsay is generally inadmissible because it is not reliable. Common sense dictates that a court, seeking to authenticate NMCI's system or process, should not rely on the unreliable out of court statements of an unknown person with unknown qualifications at NMCI.

---

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")).

[13] JA at 29.

While not binding authority, the Federal Rules of Evidence Manual states "In order for the trier of fact to make a rational decision as to authenticity, the foundation evidence must be admissible and it must actually be placed before the Jury if the Judge admits the evidence."[14] The Military Rules of Evidence Manual states "One thing is clear: the evidence that is used to authenticate or identify an item must itself be admissible."[15]

Here the only authenticity evidence offered at trial was the information relayed via telephone to SA Schmidt by an unnamed NMCI employee. This was done outside the presence of the members. As SA Schmidt himself was not familiar with the process NMCI used, he restated what he was told over the telephone by the unnamed NMCI employee. This was hearsay, and it was error to authenticate the NMCI data based on this hearsay.

2. *United States v. Garces*[16] is factually very different than this case and its holding must be viewed in light of those vast differences.

The Government argues that *United States v. Garces* establishes a rule that "the witness providing the foundation

[14] 5 STEPHEN A. SALTZBURG ET AL., FEDERAL RULES OF EVIDENCE MANUAL § 901-10 (9th ed. 2006).
[15] 2 STEPHEN A. SALTZBURG ET AL., MILITARY RULES OF EVIDENCE MANUAL § 9-4 (5th ed. 2006).
[16] *United States v. Garces*, 32 M.J. 345 (C.M.A. 1991).

only be generally familiar with the process".[17] But this holding in *Garces* must be viewed through the prism of the facts and contentions in that case, which are entirely different than the facts and contentions present in this case.

In *Garces*, the Government sought to authenticate various bank records and credit-card transaction documents.[18] The Government produced *multiple* bank officers *and* credit-card merchants who testified from *personal knowledge* about a *host* of the procedures required to produce the documents in question.[19] The defense in *Garces* conceded that these witnesses understood the procedures used to create the documents in question. But the defense also argued that the Government needed to bring the persons that were "intimately familiar" with the creation of the records.[20] The Court in *Garces* rejected an "intimately familiar" standard and held that "the witnesses showed sufficient understanding of the record systems to explain them to the military judge and to establish the reliability of the entries on the documents."[21]

This stands in remarkable contrast to the situation present here. No officers or employees of NMCI were called and no evidence regarding the reliability and accuracy of the NMCI data

---

[17] Government Br. at 7.
[18] *United States v. Garces*, 32 M.J. 345 (C.M.A. 1991).
[19] *Garces*, 32 M.J. at 347.
[20] *Id*.
[21] *Garces*, 32 M.J. at 348.

exists. Instead, all the Government offered was the testimony of one witness, SA Schmidt, who had no personal knowledge of NMCI procedures, their data collection system, or the accuracy and reliability of those procedures and system. All SA Schmidt could offer was the hearsay information he received in a phone call with an unnamed NMCI employee that the process was "automated". This is a far cry from the situation in *Garces* where the multiple employees of the business in question with personal knowledge of the procedures and systems in place within their own business "showed sufficient understanding of the record systems to explain them to the military judge and to establish the reliability of the entries on the documents".[22]

Because the facts in *Garces* are so different than this case, the Government's argument that *Garces* permits the flimsy testimony of SA Schmidt to authenticate NMCI's process is misplaced.

3. The issue of authentication is an important one in this case because the data collected by NMCI likely had a strong impression on the members, and if the process or system was inaccurate, susceptible to error or alteration, or otherwise unreliable, it should not have been admitted.

The data in this case was offered as the accurate and complete internet history of ET2 Lubich. Indeed, the importance of the NMCI data was hammered home by the trial counsel during

[22] *Garces,* 32 M.J. at 348.

his closing argument, when he repeatedly referred to it and argued that it proved ET2 Lubich's guilt.[23]

In *United States v. Morrison*, the 2nd Circuit stated that "recorded evidence is likely to have a strong impression upon a jury".[24] In *Morrison*, the evidence in question was a tape recording, not computer data, but the effect on the members is similar. Indeed, during closing arguments, the Government itself argued that the NMCI data did not lie and that the data proved ET2 Lubich was guilty.[25]

In light of this evidence and its obvious and intended effect on the members, it should have been properly authenticated prior to its admission as reliable and accurate. 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.[26] 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."[27] Later, when the data is being compiled and presented to law enforcement, "the integrity of [the] data may

---

[23] *See* JA at 57, 58, 60, 66.
[24] *United States v. Morrison,* 153 F.3d 34, 56 (2d Cir. 1998).
[25] JA at 66.
[26] *Lorraine*, 241 F.R.D. at 557, n.34.
[27] *Id*.

be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling."[28]

Because of the importance of this data at trial, the pitfalls that exist in computerized data, and the flimsy testimony that could not establish its accuracy and reliability, this Court should apply a test that at the minimum requires someone with personal knowledge to testify about the reliability and accuracy of the computer data before it can be admitted. If the Court applies such a test in this case, it was error to admit the NMCI data.

/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

[28] *Lorraine*, 241 F.R.D. at 557, n.34.

Certificate of Compliance

1. This brief complies with the type-volume limitation of Rule 24(c) because this reply brief contains approximately 2,300 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 November 19, 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