UNITED STATES, Appellee

v.

Heather D. LUBICH, Electronics Technician Second Class
U.S. Navy, Appellant

No. 12-0555

Crim. App. No. 201100378

United States Court of Appeals for the Armed Forces

Argued February 19, 2013

Decided May 3, 2013

ERDMANN, J., delivered the opinion of the court, in which BAKER, C.J., STUCKY and RYAN, JJ., and EFFRON, S.J., joined.

Counsel

For Appellant: Lieutenant Kevin S. Quencer, JAGC, USN (argued).

For Appellee: Major William C. Kirby, USMC, (argued); Colonel Kurt J. Brubaker, USMC, Colonel Stephen C. Newman, USMC, and Brian K. Keller, Esq. (on brief).

Military Judge: Carole J. Gaasch

Judge ERDMANN delivered the opinion of the court.

At a special court-martial with members, Electronics Technician Second Class (ET2) Heather D. Lubich was convicted, 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, Uniform Code of Military Justice (UCMJ), 10 U.S.C. §§ 880, 934 (2006). The convening authority approved the sentence of forty-five days confinement, forfeiture of $1,300 pay per month for two months, reduction to E-3, and a bad-conduct discharge. The United States Navy-Marine Corps Court of Criminal Appeals (CCA) affirmed the findings and sentence. United States v. Lubich, No. NMCCA 201100378, 2012 CCA LEXIS 767, at *9 (N-M. Ct. Crim. App. Apr. 19, 2012).

Military Rule of Evidence (M.R.E.) 901(a) provides that "[t]he requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." We granted review in this case to determine whether the military judge abused her discretion when she overruled a defense authentication objection and admitted

two Government exhibits which were based on computerized data.[1] We hold that the military judge did not abuse her discretion and affirm the decision of the CCA.

Background

The charges against Lubich were based on allegations that she impersonated her supervisor, a commissioned officer, by using his name, personal information and Leave and Earnings Statement (LES), to apply for a $10,000 loan from Omni Financial, Inc. via the Internet. In the course of the investigation, the Naval Criminal Investigative Service (NCIS) made a request to the Information Assurance Department of the Navy-Marine Corps Intranet (NMCI) for Lubich's Internet account data. NMCI downloaded the requested data on six CD-ROMs and sent the discs to NCIS.

At trial, Erik Schmidt, a cyber forensic examiner with NCIS, testified that he conducted a forensic examination of the six CD-ROMs provided by NMCI utilizing automated forensic tool

[1] We granted review of the following issue:

> Whether the military judge erred by overruling defense counsel's foundation and authentication objections and admitting computerized data evidence gathered by an unnamed Navy-Marine Corps Intranet (NMCI) analyst who used an unidentified process with unknown reliability to collect data related to Appellant's network user activity.

United States v. Lubich, 71 M.J. 394 (C.A.A.F. 2012) (order granting review).

programs.[2] Schmidt's examination produced two computerized reports: Prosecution Exhibit (PE) 19, a report which listed the web sites accessed by Lubich's account and the dates and number of times the web sites were accessed; and PE 23, a report that compiled the user names and passwords for the web sites accessed from Lubich's Internet account.[3]

Following a brief foundational examination, the Government moved for the admission of PE 19. The defense objected on the grounds that Schmidt lacked the "requisite personal knowledge to authenticate th[e] document" and the military judge convened an

[2] Schmidt utilized EnCase Forensic and AccessData Forensic Toolkit.

[3] PE 19 is titled "Internet Explorer Cookie Index," and is based on the Index.DAT file of Lubich's account. Schmidt testified that "[a] cookie is a text file that is saved on your user's profile from web pages; when you visit the web page, it tracks the user's access." Schmidt testified that cookies are automatically created and stored in a "database type" file called Index.DAT. PE 19 is a 179-page report which recounts information about hundreds of cookies, such as the "URL," "Filename," "Last Accessed" date, and "Hits." Notably, the "URL" field for each of the hundreds of cookies reads "Cookie:heather.lubich@" followed by the name of the relevant web site. Similarly, the "Filename" field for each of the hundreds of cookies reads "heather.lubich@," followed by an identifier for the site and the extension ".txt." PE 23, on its face, is a "NTUSER.DAT Registry Report" from the "HEATHER_LUBICH" account. Schmidt testified that NTUSER.DAT is a Windows Operating System file that holds data for a user account profile, and stores saved user names and passwords for web sites that the user visited. As printed, the Registry Report notes on every page that it is the NTUSER.DAT of the HEATHER_LUBICH account. The saved user names and passwords noted on the report include, on a number of occasions, Lubich's official Navy e-mail address, her password, and her Social Security number.

Article 39(a), UCMJ, 10 U.S.C. § 839(a) (2006), session to address the objection. During the Article 39(a) hearing, the defense expanded their objection to include a Confrontation Clause objection and told the military judge that he had the same objections to the admission of PE 23. The authentication objection was directed at the data contained on the CD-ROMs which had been provided by NMCI. The defense argued that "[The data] can't be authenticated without somebody from NMCI testifying to the collection processes that took the data from ET2 Lubich's computers to those six CDs that Mr. Schmidt was given a week or two ago."

In response to questions from the military judge as to the process NMCI utilized to gather the data from Lubich's Internet accounts, Schmidt testified as follows:

> It's an automated process. They enter the user account information in this process which in the background will run the search through the server logs and then find the computers and then remotely pull the folders themselves from the user accounts, the My Documents and folder settings -- or section, to the work station. He's actually located over on the East Coast out in Washington -- I'm sorry -- Norfolk. He will then burn the information to a CD-ROM and then ship it Fed Ex to our office.

The military judge asked if there was "any discretion on the part of the person drawing the data, or is it all automated?" Schmidt replied, "[t]he only interaction would be burning it [to] the CD-ROM itself I think." On cross-examination during the Article 39(a) hearing, Schmidt testified that he had never

worked at NMCI and was not familiar with all the software they utilized. When asked whether someone at NMCI had personally verified which computers Lubich used, Schmidt responded, "I couldn't tell you. I can't testify to that."

Following Schmidt's testimony and counsel's arguments regarding authentication and the Confrontation Clause, the military judge ruled:

> I believe that argument goes more to the weight of the evidence, and you certainly can explore that in cross-examination. The objection is overruled. I find that both Prosecution Exhibits 19 and 23 for identification 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 very little discretion involved on the part of the person that was obtaining the data.
>
> So Prosecution Exhibits 19 and 23 for identification are received into evidence.

Schmidt's subsequent testimony, based on the data in PEs 19 and 23, linked Lubich's account and her user name and password to the loan application which utilized her supervisor's name, Social Security number and LES.[4] On cross-examination, Schmidt testified that there was no way to know whether Lubich was sitting at her computer at the times when certain data was

[4] PE 19 revealed that someone using Lubich's account visited the web site, "secure.yesomni.com," the web site of the company to which she allegedly sent the loan application in the name of her supervisor, fifteen times. PE 19 showed that "secure.yesomni.com" was last accessed May 18, 2009. Similarly, PE 23 shows that someone using the HEATHER_LUBICH account input the Social Security numbers of Lubich and her supervisor into "secure.yesomni.com" on March 25, 2009.

entered or if she logged in with her password, then left the computer and someone else sat down in her place. He also testified that he had not personally accessed the computer hard drives to obtain the information on the CD-ROMs and that it was possible there was additional information on the hard drives.

During closing arguments, trial counsel argued that PEs 19 and 23 provided direct evidence that Lubich stole the victim's identity and used his Social Security number in an attempt to obtain a loan from Omni Financial. Lubich was convicted of attempted larceny, identity theft, and impersonating a commissioned officer with an intent to defraud. The CCA affirmed, holding that Schmidt's descriptions of the processes used to download the data to the CD-ROMs properly authenticated PEs 19 and 23. Lubich, 2012 CCA LEXIS 767, at *8-*9.

Discussion

At trial, "the Government bears the burden of establishing an adequate foundation for admission of evidence against an accused." United States v. Maxwell, 38 M.J. 148, 150 (C.M.A. 1993) (citation omitted). "The Government may meet its burden of proof with direct or circumstantial evidence." Id. at 150-51. On appeal, we review a military judge's decision to admit evidence for an abuse of discretion. United States v. Freeman, 65 M.J. 451, 453 (C.A.A.F. 2008) (citation omitted). "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." Id. "'Further, the abuse of discretion standard of review recognizes that a judge has a range of choices and will not be reversed so long as the decision remains within that range.'" Id. (citation omitted).

Lubich argues that the military judge erred because Schmidt did not establish the reliability, accuracy, or trustworthiness of the data NCIS received from NMCI. Lubich urges the court to reverse the CCA and suggests we adopt the type of detailed analyses for the authentication of computerized data set forth in In re Vee Vinhnee, 336 B.R. 437 (B.A.P. 9th Cir. 2005), and Lorraine v. Markel, 241 F.R.D. 534 (D. Md. 2007).[5] Lubich also relies on this Court's analysis for the authentication of video surveillance footage in United States v. Harris, 55 M.J. 433 (C.A.A.F. 2001), as an example of the type of authentication process the court should require for the admission of computerized data. Finally, Lubich argues that the admission of PEs 19 and 23 was not harmless because the error had a substantial influence on the findings.

The Government counters that the military judge did not err in the authentication of PEs 19 and 23 because she was satisfied, by a preponderance of the evidence, that the matter

[5] In re Vee Vinhnee adopted an eleven-step analysis for the foundation of computer records. 336 B.R. at 446. Lorraine cited this eleven-step test in its analysis of the foundational requirements for electronic records. 241 F.R.D. at 558.

in question was what it purported to be based on Schmidt's testimony. According to the Government, Lubich's NMCI account data was automatically stored and collected by an NMCI process with only minimal human interaction. Finally, the Government argues that the fact that Schmidt did not personally collect the data goes to its weight, not its admissibility.

"The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." M.R.E. 901(a). Evidence may be authenticated through the testimony of a witness with knowledge "that a matter is what it is claimed to be." M.R.E. 901(b)(1). M.R.E. 901(b)(9) permits evidence resulting from a "process or system" to be authenticated via "[e]vidence describing [the] process or system used to produce [the] result and showing that the process or system produces an accurate result."

It is important in this case to identify the basis for the defense objection. Authentication simply requires establishing that the evidence is what the proponent claims it to be.[6] M.R.E.

[6] Much of the case law addressing the authentication of computer data, including the authority relied on by Lubich, see supra p.8 and note 5, analyzes the requirements of M.R.E. 901 in the context of M.R.E. 803(6), the business records exception to the rule against hearsay. See, e.g., In re Vee Vinhnee, 336 B.R. at 444 ("The primary authenticity issue in the context of business records is . . . ."); Lorraine, 241 F.R.D. at 542 ("The requirement of authentication and identification also insures that evidence is trustworthy, which is especially important in

901(a). Here the Government claimed that the data contained on the six CD-ROMs was taken from Lubich's NMCI Internet accounts. During argument on the motion, the military judge invited the defense counsel to elaborate on the authentication objection. Defense counsel responded, "It's my understanding that the data that Mr. Schmidt analyzed came from Petty Officer Lubich's computers at NSAWC.[7] I mean, I don't think there's any dispute about that." This is significant as the defense recognized that the data was from Lubich's Internet accounts, but nevertheless argued that it was necessary to have direct testimony from NMCI personnel as to the process utilized by NMCI to collect the data.

In United States v. Blanchard, 48 M.J. 306, 309 (C.A.A.F. 1998), we noted that the M.R.E. 901 is the same as Fed. R. Evid.

---

analyzing hearsay issues. Indeed, these two evidentiary concepts often are considered together when determining the admissibility of exhibits or documents."). While authentication and hearsay are distinct issues, some cases conflate the two or use the same facts to address both issues. See In re Vee Vinhnee, 336 B.R. at 444 ("Ordinarily, because the business record foundation commonly covers the ground, the authenticity analysis is merged into the business record analysis without formal focus on the question." (citing 5 Weinstein § 900.06 [2] [a])). However, authentication under M.R.E. 901 and admissibility as a hearsay exception are distinct inquiries. Authenticity is a "condition precedent to admissibility" and requires only a prima facie showing that is "sufficient to support a finding that the matter in question is what its proponent claims." M.R.E. 901(a). As the business records hearsay exemption is not at issue in this case, our analysis focuses solely on authentication under M.R.E. 901, and we distinguish our analysis from those cases which blend authentication and hearsay analyses.

[7] "NSAWC" is the Naval Strike and Air Warfare Center.

901 and embraces the well-established view that authentication is a component of relevancy. We stated:

> [I]t requires a preliminary determination by the judge that sufficient evidence of authenticity exists to present the authenticity question to the members for their ultimate factual determination. See generally United States v. Sliker, 751 F.2d 477 (2d Cir. 1984); see Ricketts v. City of Hartford, 74 F.3d 1397, 1411 (2d Cir. 1996) (judge's discretion to exclude evidence on authenticity ground is limited to deciding whether sufficient proof exists for a reasonable juror to determine authenticity). It suffices to say that these same principles are applicable at courts-martial and, accordingly, federal court of appeals decisions applying these principles would be most helpful. See United States v. Richendollar, 22 M.J. 231 (C.M.A. 1986).

Id. at 309-10.

The process for authentication is more fully discussed in 5 Jack B. Weinstein & Margaret A. Berger, Weinstein's Federal Evidence § 901.02[3], at 901-13 to 901-14 (Joseph M. McLaughlin ed., 2d ed. 2003) (footnotes omitted):

> Generally speaking, the proponent of a proffered item of evidence needs only to make a prima facie showing that the item is what the proponent claims it to be. . . .
>
> Once the proponent has made the requisite showing, the trial court should admit the item, assuming it meets the other prerequisites to admissibility, such as relevance and compliance with the rule against hearsay, in spite of any issues the opponent has raised about flaws in the authentication. Such flaws go to the weight of the evidence instead of its admissibility. The trial court's admission of the exhibit means only that the fact finder may consider the item of evidence during its deliberations. The fact finder remains free to disregard the item if the trial evidence overcomes the preliminary showing of authenticity.

Weinstein explains "[i]n general, electronic documents or records that are merely stored in a computer raise no computer-specific authentication issues. If a computer processes data rather than merely storing it, authentication issues may arise." Weinstein & Berger § 900.06[3], at 900-68.

Schmidt's testimony satisfied the rules set forth in Blanchard and as discussed in Weinstein's Federal Evidence. During the Article 39(a) session, Schmidt explained that he had worked in this area for seven years. He described the collection process that retrieved the data from Lubich's account on two occasions. First, in response to trial counsel's question about how the data was collected, Schmidt explained:

> The Information Assurance Department reviews server logs for the network and verifies from the server logs themselves what computers the user account logged into. They, in turn -- it's all an automated process -- in turn will go to the computer itself and copy that user account's profile and provide it and burn it to CD-ROM.

Later Schmidt described the automated process in more detail to the military judge: NMCI personnel "enter the user account information in this process which in the background will run the search through the server logs and then find the computers and then remotely pull the folders themselves from the user accounts . . . to the work station." He also testified that he verified this process with NMCI.

The Government therefore made a prima facie showing of authenticity by presenting evidence sufficient to allow a reasonable juror to find that data on the six CD-ROMs was data from Lubich's Internet accounts. Schmidt's testimony established that NMCI transferred data stored on the computers to the CD-ROMs utilizing an automated process rather than analyzing or manipulating the data. See United States v. Tank, 200 F.3d 627, 630 (9th Cir. 2000) ("'Any question as to the accuracy of the printouts . . . would have affected only the weight of the printouts, not their admissibility.'" (alteration in original) (quoting United States v. Catabran, 836 F.2d 453, 458 (9th Cir. 1988))).

The Government also met several of the illustrative criteria of M.R.E. 901(b):

> M.R.E. 901(b)(1) -- "Testimony of witness with knowledge" was satisfied through Schmidt's familiarity with the NMCI procedures;
>
> M.R.E. 901(b)(4) -- "Distinctive characteristics and the like" was satisfied as the computer data contained numerous references to Lubich's personal computer information;
>
> M.R.E. 901(b)(9) -- "Process or system" was satisfied by Schmidt's discussion regarding the NMCI process.

Once this preliminary standard for reliability was established, the defense had the opportunity to attack the perceived weaknesses in the case through cross-examination of Schmidt. Indeed, Lubich's counsel questioned Schmidt about the possibility that someone else was sitting at a computer that

Lubich previously logged onto and entered the information without her knowledge. Defense counsel also questioned Schmidt about whether any other forensic data was reviewed, whether they sought forensic evidence from other individuals, and whether there may have been other Internet history data associated with the account that could have been deleted from the profile but remained on hard drives that were not examined by NCIS. Thus, Lubich had the opportunity to confront Schmidt about this evidence and attempt to diminish its impact on the members.

We decline to adopt Lubich's proposal that we develop a detailed authentication analysis for computer data.[8] There are numerous scenarios in which this issue will arise and we see no benefit in attempting to craft a "standard" test to analyze all computer data situations. We will continue to rely on the military judge's discretion to determine authenticity. See Blanchard, 48 M.J. at 310 (explaining that "[M.R.E.] 104 gives discretion to the trial judge as to the manner in which he makes preliminary determinations concerning admissibility of evidence" and "reject[ing] appellant's general argument that the military

[8] Lubich's reliance on Harris is also misplaced. Harris involved the authentication of a videotape under M.R.E. 901 utilizing the "silent witness" theory. 55 M.J. at 436. There the court established the authentication criteria for photos taken by an automated camera. Id. at 438-40. That situation differs from this case where Lubich concedes that the data was taken from her Internet account.

judge erred by failing to strictly follow selected federal decisions in making his authenticity determination.”).

We hold that the military judge did not abuse her discretion in admitting PEs 19 and 23. Once these exhibits were admitted, it was then up to the members to determine the true authenticity and probative value of the evidence based on Schmidt’s testimony.

Decision

The decision of the United States Navy-Marine Corps Court of Criminal Appeals is affirmed.