UNITED STATES AIR FORCE COURT OF CRIMINAL APPEALS

UNITED STATES

v.

Airman First Class NICKOLAS A. WATSON
United States Air Force

ACM 37416

13 December 2010

Sentence adjudged 23 January 2009 by GCM convened at Sheppard Air Force Base, Texas. Military Judge: William M. Burd.

Approved sentence: Bad-conduct discharge, forfeiture of all pay and allowances, and reduction to E-1.

Appellate Counsel for the Appellant: Lieutenant Colonel Gail E. Crawford, Major Shannon A. Bennett, Major Michael A. Burnat, Major Darrin K. Johns, Captain Phillip T. Korman, Captain Nicholas McCue, and William E. Cassara, Esquire (civilian counsel).

Appellate Counsel for the United States: Colonel Don M. Christensen, Lieutenant Colonel Jeremy S. Weber, Captain Joseph Kubler, and Gerald R. Bruce, Esquire.

Before

BRAND, GREGORY, and WEISS
Appellate Military Judges

PER CURIAM:

Contrary to his pleas, the appellant was found guilty by a panel of officer members of one specification of wrongfully and knowingly possessing visual depictions of minors engaging in sexually explicit conduct, in violation of Article 134, UCMJ, 10 U.S.C. § 934. The approved sentence consists of a bad-conduct discharge, forfeiture of all pay and allowances, and reduction to E-1.[1]

[1] Pursuant to Article 57(a)(2), UCMJ, 10 U.S.C § 857(a)(2), the convening authority deferred the reduction in rank and adjudged forfeitures from 6 February 2009 until the date of Action. Additionally, because the appellant was not

The issue on appeal is whether the evidence is legally and factually sufficient to support the finding of guilty for wrongful and knowing possession of visual images depicting minor children engaged in sexually explicit conduct. Finding no error, we affirm.

Background

On 17 September 2007, the appellant arrived at Sheppard Air Force Base, Texas. From September to December 2007, the appellant resided with Airman First Class (A1C) BP. Sometime in late September to early October 2007, A1C BP obtained a laptop computer which the appellant borrowed on a regular basis. A1C BP testified that on one or two occasions after the appellant had used his computer, he noticed that the Internet history of his computer had been deleted. A1C BP never allowed anyone other than the appellant to borrow his computer and he never viewed child pornography on his computer. He was subsequently interviewed by the Air Force Office of Special Investigations (AFOSI) and turned over his computer.

From 10-12 November 2007, another airman, A1C BD, testified that he loaned his laptop computer to the appellant. When he entered the appellant's room to retrieve his computer, he saw the appellant exit out of an Internet browser. When he returned to his room, A1C BD attempted to access the Internet but was unable to do so. He checked the Internet history browser and saw some questionable websites, such as "Little Nymphets" and "Magic Beauties." A1C BD looked at these websites and observed very young girls clothed in underwear and posed in sexual positions. He then proceeded to delete the browser history. A1C BD eventually informed his chain of command and subsequently provided his computer to the AFOSI. He admitted to watching adult pornography on his computer but not child pornography.

On 20 November 2007, the appellant was interviewed by then Special Agent (SA) RH from the AFOSI. SA RH informed the appellant that he was being accused of possessing child pornography and advised the appellant of his Article 31, UCMJ, 10 U.S.C. § 831, rights. During the interview and in a subsequent written statement, the appellant indicated that his first interaction with child pornography occurred in February 2007 (prior to his enlistment in the Air Force) when he received an e-mail that contained

---

sentenced to confinement, the amount of forfeitures is limited to two-thirds pay per month. Rule for Courts-Martial (R.C.M.) 1107(d)(2), Discussion. *See also United States v. Craze*, 56 M.J. 777 (A.F. Ct. Crim. App. 2002); *United States v. York*, 53 M.J. 553 (A.F. Ct. Crim. App. 2000); *United States v. Warner*, 25 M.J. 64 (C.M.A. 1987). When an appellant alleges an error in the application of a sentence involving forfeitures, he must demonstrate that the error was prejudicial. Article 59(a), UCMJ, 10 U.S.C. § 859(a); *United States v. Lonnette*, 62 M.J. 296, 297 (C.A.A.F. 2006). The appellant did not allege this as an error. Although the sentence was incorrectly approved as adjudged, the convening authority deferred the forfeitures until action. Upon action, the appellant was placed on involuntary appellate leave. There is no showing that the appellant suffered any prejudice as a result of the erroneously approved sentence.

child pornography. At that point, the appellant made it a mission to get rid of child pornography on the Internet so he would search for websites that contained child pornography and on two occasions reported those websites to a non-profit organization known as Cyberangels. He provided his e-mail address on those two occasions only, because all subsequent reports were just a follow-up of his previous reports. The appellant admitted to using A1C BD's and A1C BP's computers on numerous occasions to search the Internet for child pornography in pursuit of his quest to rid the Internet of child pornography, most recently during the weekend of 10-12 November 2007 when he borrowed A1C BD's computer. He also admitted to "click[ing] link after link of child pornography." He described in detail some of the videos and pictures that he viewed and claimed that he received absolutely no pleasure from visiting the websites but continued to search because it became what he described as a "curiosity obsession." The appellant further stated that after viewing the child pornography, he would erase the Internet history to ensure no one could tell what websites he visited. The appellant provided AFOSI with a list of websites that he visited while searching for child pornography.

The government called Mr. AD, a program manager for Cyberangels. He testified that Cyberangels is a clearing house of information regarding cybercrime and Internet safety in general. According to records maintained by Cyberangels, they received e-mails from the appellant on 25 June 2007 and again on 10 July 2007. A case was opened upon receipt of the e-mails but was subsequently closed after Cyberangels provided a response to the appellant. There were no e-mails from the appellant between the charged timeframe of 17 September 2007 and 12 November 2007. In one of their responses, Cyberangels advised the appellant to ensure that he deleted the Internet cache if he had not already done so.

The government also called Mr. JC, an expert in the field of computer forensics, from the Defense Computer Forensics Laboratory (DCFL). Mr. JC testified that he analyzed the hard drives from the two computers seized from A1C BD and A1C BP. He explained that a computer system locates files similar to how a card catalog tracks the books in a library. The "logical" level on a hard drive is anything that a typical user sees, usually the C-drive, when operating a computer. "Unallocated space" refers to the part of the hard drive that contains files which are no longer being tracked by the operating system. These are files that have been deleted but the data is still present. Eventually these files can be overwritten if the operating system chooses to use that location for other files. Compared to a library system, although a card may be removed from the catalog, the book still may be physically on the shelf. In conducting his examination, Mr. JC used a forensic software tool called EnCase to look for those files in the unallocated space.

Mr. JC testified that when a person uses Internet Explorer to access the Internet, Internet Explorer has a system that saves the web addresses and files that are downloaded from the Internet in a "cache" somewhere on the logical level of the operating system.

The cache can either be deleted by the user or automatically by the computer, depending on the computer's settings.

Upon examining the two computers in this case, Mr. JC found 31 known images of child pornography, 23 of which were unique, that have been identified by the National Center for Missing and Exploited Children. Both computers contained images in the unallocated space and some of the images were found in the Vista back-up system of A1C BP's computer. Mr. JC further testified that he conducted a key word search to locate the child pornography using the list of websites provided by the appellant. He opined that the evidence showed that someone was actively searching for and found child pornography.

The members were instructed by the military judge that "[p]ossess means to exercise control of something." The military judge also advised the members, in response to their request for him to elaborate on the definition of "exercise control," that it was a factual issue for them to determine.

Discussion
Legal and Factual Sufficiency

The appellant asserts that his conviction for wrongful and knowing possession of images depicting minor children engaged in sexually explicit conduct is legally and factually insufficient because the evidence failed to show beyond a reasonable doubt that he exercised control over the images.

In accordance with Article 66(c), UCMJ, 10 U.S.C. § 866(c), we review issues of legal and factual sufficiency de novo. *United States v. Washington*, 57 M.J. 394, 399 (C.A.A.F. 2002). "The test for legal sufficiency of the evidence is whether, considering the evidence in the light most favorable to the prosecution, any reasonable fact-finder could have found all the essential elements beyond a reasonable doubt." *United States v. Day*, 66 M.J. 172, 173 (C.A.A.F. 2008) (citing *United States v. Turner*, 25 M.J. 324, 324 (C.M.A. 1987)).

The test for factual sufficiency is "whether, after weighing the evidence in the record of trial and making allowances for not having personally observed the witnesses, [we] are [ourselves] convinced of the [appellant's] guilt beyond a reasonable doubt." *Turner*, 25 M.J. at 325. Review of the evidence is limited to the entire record, which includes only the evidence admitted at trial and exposed to the crucible of cross-examination. Article 66(c), UCMJ; *United States v. Bethea*, 46 C.M.R. 223, 224-25 (C.M.A. 1973).

The gravamen of the appellant's position is that the government failed to prove beyond a reasonable doubt that he knowingly possessed the images of child pornography

that he admitted to viewing on A1C BD's and A1C BP's computers. In support of this position, the appellant highlights the testimony of the government's expert, Mr. JC, who testified that the images he found were at locations on the computers where a user could not physically save the images and he found no evidence that anyone had selected an image of child pornography to save it. Mr. JC could not tell if the images were intentionally viewed or saved by the appellant. He also could not determine if someone clicked on a specific link to intentionally download the pictures or just accessed the webpage, nor could he establish how long the individual stayed on a particular website. Therefore, there is no forensic evidence showing that the appellant deliberately downloaded an image to save it.

The appellant relies on our superior court's holding in *United States v. Navrestad*, 66 M.J. 262 (C.A.A.F. 2008), where the Court set aside a conviction for possession and distribution of child pornography when that appellant had used a computer at an Internet café to view child pornography. Citing the definition in the *Manual*, that "[p]osses[sion] means to exercise control of something," the Court held that the appellant's actions in that case went no further than just viewing the images. *Id.* at 267 (quoting *Manual for Courts-Martial, United States (MCM)*, Part IV, ¶ 37.c.(2) (2005 ed.)). Although the websites that he viewed on the Internet café computers were automatically saved in a temporary Internet folder, Navrestad did not have access to that folder and there was no evidence indicating that he was aware that the sites were being saved on the hard drive. Since Navrestad could not access the computer's hard drive where the images were automatically saved, nor could he download the images to a portable storage device, the Court held that he did not exercise sufficient dominion and control over the images to constitute possession. *Id.*

Unlike in *Navrestad*, in the present case the appellant had access to the Internet cache on the personal computers he borrowed and he knew that the images were being saved as he admitted to SA RH that he routinely accessed the Internet cache to erase the Internet history or clear the cache so A1C BD and A1C BP could not tell what websites he visited when the computers were returned. Additionally, the government's expert testified that although the images were found in the unallocated space of the computer, the files were being used by the operating system at some point. He stated the files had been in someone's control but he could not be certain if it was the system or the user.[2]

[2] We note that this expert testimony corroborates the appellant's admission that the appellant accessed the files in the Internet cache and, therefore, exercised some control over the files. *See* Mil. R. Evid. 304(g); *United States v. Ober*, 66 M.J. 393 (C.A.A.F. 2008) (explaining that though the computer forensics expert could not determine the individual user responsible for presence of child pornography on computer, his testimony sufficiently corroborated appellant's admissions to accessing child pornography); *United States v. Maio*, 34 M.J. 215, 218 (C.M.A. 1992) (holding that corroborating evidence need not itself establish proof of guilt beyond reasonable doubt).

The appellant also relies on the Ninth Circuit court's decision in *United States v. Kuchinski*, 469 F.3d 853 (9th Cir. 2006). In *Kuchinski*, the Ninth Circuit asserted that, "[w]here a defendant lacks knowledge about the cache files, and concomitantly lacks access to and control over those files, it is not proper to charge him with possession and control of the child pornography images located in those files, without some other indication of dominion and control over the images." *Id.* at 863. However, the facts of the present case are more analogous to the Tenth Circuit court's decision in *United States v. Tucker*, 305 F.3d 1193, 1204-05 (10th Cir. 2002), where the appellant was found to knowingly possess images cached on his Web browser when he knew the images would be sent to his browser's cache file and stored on the hard drive. As in *Tucker*, the appellant in this case was computer savvy enough to know about the cache files as he routinely accessed them to erase the Internet history and to clear the cache.

We find that similar to someone pulling a book off of a library shelf to view it, even for a short period of time, the appellant possessed the images of child pornography when they were downloaded to the temporary Internet cache on the borrowed computers. At this point he could have accessed the Internet cache and saved the files to either another folder on the computers or to a portable storage device. Although there is no evidence the appellant further saved the images to a portable storage device, he was a sophisticated computer user who knew the images existed in the temporary Internet cache and did access those files to delete them. Accordingly, we conclude that at some point the appellant exercised sufficient dominion and control over the images to constitute possession.

Considering our review of the entire record of trial, a reasonable fact finder could have found that the appellant wrongfully and knowingly possessed images depicting minor children engaged in sexually explicit conduct. Furthermore, after weighing the evidence in the record of trial and making allowances for not having personally observed the witnesses' in-court testimony, we are ourselves convinced of the appellant's guilt beyond a reasonable doubt. Therefore, we find the evidence is legally and factually sufficient to sustain the conviction.

Conclusion

The approved findings and sentence are correct in law and fact and no error prejudicial to the substantial rights of the appellant occurred. Article 66(c), UCMJ; *United States v. Reed*, 54 M.J. 37, 41 (C.A.A.F. 2000).

Accordingly, the approved findings and sentence are

AFFIRMED.

OFFICIAL

STEVEN LUCAS
Clerk of the Court