UNITED STATES NAVY-MARINE CORPS
COURT OF CRIMINAL APPEALS
WASHINGTON, D.C.

Before
R.E. VINCENT, E.C. PRICE, J.E. STOLASZ
Appellate Military Judges

UNITED STATES OF AMERICA

v.

RICHARD B. TOSCHIADDI
CAPTAIN (O-3), U.S. MARINE CORPS

NMCCA 200800044
GENERAL COURT-MARTIAL

Sentence Adjudged: 01 March 2007.
Military Judge: LtCol Tracy Daly, USMC.
Convening Authority: Commanding General, Marine Corps Installations West, Camp Pendleton, CA.
Staff Judge Advocate's Recommendation: Col C.J. Woods, USMC.
For Appellant: Matthew S. Freedus, Esq.; Eugene R. Fidell, Esq.; Brent C. Harvey, Esq.; Maj Anthony Burgos, USMC.
For Appellee: LT Duke Kim, JAGC, USN.

16 July 2009

OPINION OF THE COURT

AS AN UNPUBLISHED DECISION, THIS OPINION DOES NOT SERVE AS PRECEDENT.

STOLASZ, Judge:

A military judge sitting as a general court-martial convicted the appellant, contrary to his pleas, of two specifications of conduct unbecoming an officer, comprising one specification for possession of child pornography and one specification for visiting a child pornography website; two specifications of electronically transferring images and video files of child pornography; one specification of attempted receipt of child pornography; one specification of reproducing

child pornography; and three specifications of advertising, promoting and soliciting child pornography, in violation of Articles 133 and 134, Uniform Code of Military Justice, 10 U.S.C. §§ 933 and 934, and 18 U.S.C. § 2252A.[1] The appellant was sentenced to confinement for 30 months, forfeiture of all pay and allowances for a period of 30 months, and a dismissal. On 21 December 2007, the convening authority (CA) approved the dismissal, confinement for a period of 892 days, and the adjudged forfeitures, but as an act of clemency suspended "that part of the sentence extending to forfeiture of $2208.00 per month in allowances . . . for six months from 1 January 2008" to be later remitted. The CA issued a supplemental action on 19 March 2008 approving the dismissal, confinement for a period of 892 days, and the adjudged forfeitures, but as an act of clemency suspended "that part of the sentence extending to adjudged forfeitures in the amount of $2208.00 per month . . . for a period of six months from the date of this action" to be later remitted, and waiving automatic forfeitures for 6 months from the date of his supplemental action.[2]

After careful consideration of the record of trial, the appellant's brief and four assignments of error, the Government's answer, and the appellant's reply, we conclude that the findings and sentence are correct in law and fact, and no error materially prejudicial to the substantial rights of the appellant was committed. Arts. 59(a) and 66(c), UCMJ.

The appellant asserts that: (1) the military judge committed plain error by admitting testimony from the appellant's executive officer regarding plea discussions; (2) the evidence was factually and legally insufficient for all of the charges and specifications of which he was found guilty; (3) the military judge committed plain error and violated the appellant's Sixth Amendment rights by preventing courtroom spectators from viewing the images of child pornography; and (4) the appellant was denied equal protection under the law because the military judge was not serving a fixed term.

---

[1] Specifications 1 and 2 (electronic transfer of images and video files of child pornography), 3 (receipt of child pornography), 4 (reproducing child pornography) and 5 and 6 (advertising, promoting and soliciting child pornography) of Charge II, Specification 1 of Additional Charge I (visiting internet relay chatroom 100%PreteenGirlsSexPics), and the specification of Additional Charge II (advertising child pornography over the computer) were charged under Article 134, UCMJ, clauses 1 and 2.

[2] Although the convening authority changed the terminal date of the period of suspension in his supplemental action, the appellant has not claimed any prejudice and, since both periods of suspension have passed, no corrective action is required.

I. Testimony Regarding Plea Discussions

Lieutenant Colonel (LtCol) C was the Executive Officer of the appellant's unit, Marine Corps Technical Systems and Support Activities (MCTSSA), and was regarded by the appellant as a mentor. Record at 579. LtCol C testified during the Government's case in chief that, prior to the court-martial, the appellant mentioned that his father-in-law advised him that pleading guilty as part of a plea bargain might be the right thing to do for the sake of his wife and daughter, because he would receive a known sentence rather than a contested trial with an unknown sentence. *Id.* LtCol C testified that he reacted with surprise because the appellant had always professed his innocence and willingness to defend against the charges. *Id.*

The defense did not object to LtCol C's testimony at trial. However, the appellant claims on appeal that LtCol C's testimony related to a plea discussion, the disclosure of which is prohibited by MILITARY RULE OF EVIDENCE 410, MANUAL FOR COURTS MARTIAL, UNITED STATES (2005 ed.). MIL. R. EVID 410(a)(4) prohibits the introduction into evidence of "any statement made in the course of plea discussions with the convening authority, staff judge advocate, trial counsel or other counsel for the Government which do not result in a plea of guilty . . . ." Since there was no objection at trial, we apply the plain error standard of review. Plain error occurs when: (1) an error was committed; (2) the error was plain, clear, or obvious; and (3) the error resulted in material prejudice to the appellant's substantial rights. *United States v. Nieto,* 66 M.J. 146, 149 (C.A.A.F. 2008)(citing *United States v. Moran,* 65 M.J. 178, 181 (C.A.A.F. 2007)).

There is no evidence to suggest the appellant was engaged in plea discussions or negotiations with LtCol C at the time he repeated the advice from his father-in-law. The record reflects the appellant spontaneously mentioned the advice he received from his father-in-law to LtCol C, a friend and mentor. As in *United States v. Watkins,* 34 M.J. 344, 348 (C.M.A. 992), LtCol C was acting neither as nor on behalf of the CA or the staff judge advocate, nor was he authorized to engage in plea negotiations with the appellant. The statement was voluntarily made and its admission was not an abuse of discretion.

The appellant's citation to *United States v. Tompkins,* 30 M.J. 1090, 1094 (N.M.C.M.R. 1989) in support of his argument is misplaced. In *Tompkins,* the appellant was denied an

administrative discharge in lieu of court-martial by the convening authority. In a subsequent attempt to procure a positive endorsement on his discharge request, the appellant enlisted the help of his friend, a corporal, who worked as a clerk in the office where the administrative discharge requests were processed. *Id.* We found that statements made by the appellant to the clerk/corporal during a conversation in which he requested assistance with negotiation of his administrative discharge request were within the ambit of MIL. R. EVID. 410(a)(4), and set aside the finding. The statement made by the appellant to LtCol C was not made or offered for the purpose of pretrial negotiation, and thus should not invoke the protection MIL. R. EVID. 410(a)(4) is intended to provide.

Furthermore, we are confident that the military judge, who is presumed to know and follow the law, considered the testimony within the proper context with which it was received. *United States v. Erickson,* 65 M.J. 221, 225 (C.A.A.F. 2007).

II. Legal and Factual Sufficiency

The appellant claims that the evidence is legally and factually insufficient to support findings of guilty on the charges and specifications.

A. Background

In 2004 and 2005, The German National Police, Bundeskriminalant, and the Federal Bureau of Investigation (FBI) were conducting separate and independent investigations targeting individuals trading child pornography over the Internet. Detective Chrestoph Adler of the BKA and Special Agents (SA) Kenneth Jensen and Christopher Trifiletti of the FBI each engaged in separate online, undercover operations in 2004 and 2005. Their investigations were initiated by accessing Internet Relay Chat (IRC) using fictitious names and accounts. IRC is a worldwide network of interconnecting computers serving as a conduit to various networks. Once in the network, access is available to channels or links where live activities, such as chats and trading, can take place. In order to access IRC, a commercial software program is required. The investigations conducted by BKA and the FBI involved accessing IRC, and thereafter the undercover operation focused on the channel "100%PreTeenGirlsSexPics."

The priority of each undercover operation was to initiate contact with another individual interested in trading child

pornography. Once contact was initiated, any chats or trades were recorded utilizing a commercial software program automatically programmed to create log files reflecting any chats or trades that occurred. If a trade of child pornography was conducted during the undercover operation, the next phase of the investigation involved securing the internet protocol (IP) address of the computer participating in the trade, and then tracing the IP address to a specific location through the internet service provider. After a specific location was identified as the IP address, search warrants were secured and served, followed by seizure of computers, hard drives and other digital media for forensic examination.

On 24 April 2004, Detective Adler, engaging in an online undercover investigation in Wiesbaden, Germany, traded two images of child pornography while connected to the IRC network within the channel "100%PreteenGirlsSexPics." Detective Adler initiated the trade after noticing a file server named "bigrl" issuing advertisements soliciting a trade of child pornography images and videos. Detective Adler proceeded to upload an image to the "bigrl" file server to obtain credit from "bigrl." After obtaining credit, he downloaded two images of child pornography from the "bigrl" file server. Detective Adler then secured the IP address for the "bigrl" file server which was from an Internet Service Provider located in California. This evidence was forwarded to United States Immigration and Customs Enforcement (ICE) officials, and they traced the IP address to the residence of the appellant. On 14 January 2005, ICE conducted a search of the appellant's residence seizing two computers and one hard drive. PE 1, 3, and 4.

On 15 May 2004, SA Trifiletti, engaging in an online undercover investigation in Maryland, was connected to the IRC network using the fictitious name "scubastev." He was using a file server to periodically run advertisements soliciting child pornography within the "100%PreteenGirlsSexPics" channel. Agent Trifiletti's file server used a commercial software program called MIRC to access "100%PreTeenGirlsSexPics."[3] The file server was configured to automatically run the advertisement at one and five minute intervals. The advertisement indicated that SA Trifiletti had a highly categorized collection of child pornography pictures available for trade. A file server named "bigrl" responded to the advertisement by texting the following

[3] MIRC is a commercial software program which allows access to the IRC in the same fashion as Internet Explorer allows access to the Internet, and facilitates the trading and transfer of files.

message “want to mutual leech (FTP or fserve).”[4] The text message or chat was recorded in a log showing the communication between "bigrl" and "scubastev." PE 15. SA Trifiletti testified that because his computer was running the advertisement in automated fashion, and was unmanned when "bigrl" accessed his file server, he did not respond to "bigrl’s" request for a mutual leech. Since SA Trifiletti did not engage in a trade of child pornography images, the investigation was not pursued, and the chat logs generated during the investigation were stored in a database for future reference.

On 10 January 2005, SA Jensen was engaged in an online undercover investigation while located in Buffalo, New York. He accessed the IRC network and navigated within the channel "100%PreteenGirlsSexPics." While in the channel, he connected to a file server named "bigrl," which was issuing advertisements soliciting child pornography. SA Jensen proceeded to upload a corrupted file, purporting to contain child pornography, to the "bigrl" file server.[5] He then used the credit he obtained from the upload to download numerous images and two video files of child pornography from the "bigrl" file server. SA Jensen then traced the IP address of the "bigrl" file server to the residence of the appellant. He did not pursue the investigation further by attempting to secure a search warrant because he learned a search of the appellant’s residence had taken place on 14 January 2005 as a result of the evidence developed in the two prior investigations.

The search of the appellant’s residence led to the seizure of three hard drives (desktop/tower drive (PE 1), encrypted hard drive (PE 4), and hard drive found in the garage (PE 3)). Robert Barnes, a retired SA for ICE, conducted a forensic examination of the seized hard drives. Mr. Barnes testified that he used the software program Encase to make a mirror image of the hard drive on the appellant’s computer. He also used the

[4] Mutual leech allows for mutual direct unlimited access to the files or videos offered for trade by another individual without having to earn credits. It is, essentially, a swap of what each individual has to offer.

[5] FBI policy prohibits the trade of child pornography, thus agents working online in an undercover capacity upload corrupted files, which cannot be opened, in order to obtain credit to download files from their trading partners. The BKA policy is apparently less stringent as, in this case, Detective Adler uploaded a picture of a nude girl which was not considered to be child pornography, to obtain credit from the appellant’s file server. Record at 271.

software program Snag It, which allowed him to capture images on the computer screen of PE 1 similar to a photograph. Mr. Barnes' comprehensive forensic examination discovered thumbnail files or images depicting child pornography residing in allocated space on the hard drive of the tower computer (PE 1) seized from the appellant's residence.[6] PE 49. He described a thumbnail as a small picture view of picture files or movie files contained on a directory or in a folder on the directory of the hard drive. He further testified the thumbnail images were located in a file named Panzer on a folder in the C directory of the hard drive of PE 1. Record at 734-35; PE 49 at 1-3.

Mr. Barnes testified that he utilized a hash calculation program (PE 34) which allowed him to find cyclic redundancy check (CRC) values for files or images found on the appellant's computer.[7] Essentially, Mr. Barnes located a text file, CRC1, within a subfolder named Panzer on the hard drive of PE 1. He discovered that the file CRC1 primarily served as a database in text format for all files within the "bigrl" file server that the Panzer subfolder had access to for sharing. This included any files or images uploaded on the hard drive. Record at 686. ICE SA John Mizusawa provided Mr. Barnes with the images that had been downloaded from the "bigrl" file server by Detective Adler and SA Jensen. Mr. Barnes then calculated the CRC values for the images and matched the CRC value to file names on the hard drive of PE 1. PE 34-39. Mr. Barnes testified that the uniqueness of a CRC value matching an image or file on the hard drive was 4.29 billion to 1 before a duplicate image with the same CRC value would appear. Record at 686.

B. Law

Article 66(c), UCMJ, requires this court to conduct a *de novo* review of the legal and factual sufficiency of each approved finding of guilty. *United States v. Washington*, 57 M.J. 394, 399 (C.A.A.F. 2002)(citing *United States v. Cole*, 31 M.J. 270, 272 (C.M.A. 1990)). 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," this court is convinced of the appellant's guilt

[6] Allocated space of the hard drive contains files, folders, user files, user folders and includes anything the operating system recognized and can go to. Record at 735.

[7] A CRC calculates a value for a file then matches that value to an image or file on the hard drive. Record at 685.

beyond a reasonable doubt. *United States v. Turner*, 25 M.J. 324, 325 (C.M.A. 1987). The test for legal sufficiency is whether, "considering the evidence in the light most favorable to the prosecution, a reasonable factfinder could have found all the essential elements beyond a reasonable doubt." *Id.* at 324 (citing *Jackson v. Virginia*, 443 U.S. 307, 319 (1979)).

C. Analysis:

Charge I, Specification 2

The appellant was found guilty of conduct unbecoming an officer for possessing 15 images of child pornography on divers occasions between 24 April 2004 and 14 January 2005. The appellant disputes the factual and legal sufficiency of the evidence claiming there was no direct evidence he knew that images of child pornography were located on the hard drives seized from his residence nor was there direct evidence that he accessed or exercised control over the images. He also claims the images were located on unallocated space within two of the seized computer hard drives (PE 1 and PE 3), and required forensic software, which he did not possess, to access.[8] Finally, he claims that multiple individuals had access to the computer.

We disagree and find the evidence presented is both factually and legally sufficient to show that the appellant exercised dominion and control of PE 1 as well as the contents of the hard drive.[9]

The child pornography images were discovered after Mr. Barnes, a computer forensic expert, performed a forensic analysis on the computer, and hard drives seized from the appellant's residence and garage.[10] One of the hard drives was located in his home office inside his desktop computer (PE 1), and the other hard drive was located in his garage (PE 3). A third hard drive was not analyzed because it contained an

[8] Unallocated space of the hard drive contains deleted files which are not organized and not accessible without the necessary software or forensic program. Record at 417.

[9] The appellant correctly cites to *United States v. Navrestad,* 66 M.J. 262, 267-68 (C.A.A.F. 2008) for the proposition that the Court of Appeals for the Armed Forces has adopted the definition of possession in Article 112a, UCMJ, in child pornography cases because the Child Pornography Prevention Act of 1996 (CPPA), 18 U.S.C. §§ 2251-2260 (2000), does not define possession.

[10] Mr. Barnes worked for ICE prior to his retirement.

encrypted container which Mr. Barnes was unable to access. (PE 4).

The evidence also showed the appellant was the administrator of and controlled the only password for the computer. PE 59 at 1-2. There were also personal documents found on the hard drive of the computer (PE 1), such as the appellant's resume, financial documents, and receipts for various purchases of computer related accessories and equipment, al of which contradict the appellant's argument that he lacked knowledge or dominion and control of the contents of the hard drive. PE 24, PE 66 at 1-17. It is apparent that each and every time the appellant turned on the desktop computer (PE 1), he controlled and had access to the images of child pornography which were categorized on folders and subfolders within the hard drive.

There is also no evidence to support the appellant's claim that other individuals with access to the computer were responsible for the images found on the hard drive. The appellant's neighbor and close friend, James Solomon, testified that he used the appellant's computer as did the appellant's wife and brother. He also testified that while using the appellant's computer, he downloaded adult pornography, but never downloaded child pornography. He further testified that the appellant built and maintained the tower or desktop computer (PE 1), on whose hard drive the images of child pornography were located. He also testified the appellant used a file server.

The evidence presented was also factually and legally sufficient to conclude that the appellant's possession of thumbnail images of child pornography is conduct which disgraces and dishonors the appellant, and seriously compromises his standing as an officer in the United States Marine Corps.

Considering the evidence adduced at trial in the light most favorable to the Government, we find that a rational trier of fact could have found the elements of the offense beyond a reasonable doubt. *Jackson*, 443 U.S. at 318-19; *Turner*, 25 M.J. at 325; *United States v. Reed*, 51 M.J. 559, 561-62 (N.M.Crim.Ct.App. 1999), *aff'd*, 54 M.J. 37 (C.A.A.F. 2000); *see also* Art. 66(c), UCMJ. In addition, after weighing all the evidence in the record of trial and recognizing that we did not see or hear the witnesses, this court is convinced of the appellant's guilt beyond a reasonable doubt. *Turner*, 25 M.J. at 325; *see also* Art. 66(c), UCMJ.

Charge II, Specifications 1 and 2

The appellant was convicted of electronically transferring two images of child pornography to Detective Adler of the BKA (Specification 1 of Charge II) on 24 April 2004, and electronically transferring 34 images and 2 video files of child pornography to SA Jensen of the FBI (Specification 2 of Charge II) on 10 January 2005.

The appellant argues that the evidence is insufficient to prove he knew the images were located on any of the seized hard drives, and that he cannot be found to have transferred the images and video files without the requisite knowledge. He further argues that the evidence shows the images were automatically transferred utilizing a software program called, Panzer, which allows files to be transferred automatically without the computer being manually operated.

The evidence shows that two images containing child pornography were electronically transferred to Detective Adler, and 34 images and two video files containing child pornography were electronically transferred to SA Jensen from a file server named "bigrl" on 24 April 2004 and 10 January 2005 respectively. The evidence establishes that "bigrl" entered the channel "100%PreTeenGirlsSexPics" utilizing two software programs, MIRC and Panzer, which work in combination. MIRC provides access to channels on the IRC, and in combination with Panzer allow a user to solicit or advertise in order to facilitate trades. However, Panzer requires manual installation and configuration prior to use. It can be programmed to run automatically, which presumably allows for the trade and accumulation of images at a rapid rate.

The appellant asserts that because Panzer is automated, the transfer of images and files to Detective Adler and SA Jensen likely occurred without someone manually operating the computer. However, this argument fails to consider that Panzer requires configuration and installation prior to automated operation. The rules and advertisements appearing on Panzer also require configuration. Notably, there was testimony from the appellant’s neighbor, James Solomon, that the appellant built, maintained, and loaded software on the desktop computer. Record at 585; PE 1. Further, the software programs utilized to transfer the images and video files, MIRC and Panzer were installed on the appellant’s computer. Finally, forensic analysis of the computer utilizing the Snag it program captured

screens showing the MIRC program with the username "bigrl." PE 41.

The evidence further indicates that on three different instances, 24 April 2004, 15 May 2004 and 10 January 2005, after entering an internet chatroom channel, "100%PreteenGirlsSexPics," dedicated to child pornography, a connection was made to a file server whose internet protocol address was ultimately traced to the residence of the appellant. Thereafter, log files automatically generated by the computers of the respective investigative agents, during the transactions in April and May 2004, as well as January 2005, captured the transfer of the child pornography from the file server traced to the appellant's residence. PE 9, 10, 11, 18, 19, 20. Finally, log files generated from the hard drive of the appellant's computer also captured the transfer of the child pornography from the appellant's file server to Detective Adler and SA Jensen. PE 43.

Mr. Barnes testified that detective Adler was using a fictitious name "Creator" when he downloaded two files from the hard drive of PE 1 on 24 Apr 2004. He testified that his forensic analysis located a text file matching that user name on the hard drive of PE 1 within the "ini" file in the Panzer subdirectory. He also located a log file of the transaction capturing the transfer of the images to Detective Adler. Record at 706, 707; PE 33. He further testified he followed the same process by using the fictitious name utilized by the FBI, "PackerDad@67-23-182," and found a related text file matching the log files from the FBI capturing the transfer of child pornography from the hard drive of PE 1 on 10 January 2005.

Considering the evidence adduced at trial in the light most favorable to the Government, we find that a rational trier of fact could have found the elements of the offense beyond a reasonable doubt. *Jackson*, 443 U.S. at 318-19; *Turner*, 25 M.J. at 325; *Reed*, 51 M.J. at 561-62; *see also* Art. 66(c), UCMJ. In addition, after weighing all the evidence in the record of trial and recognizing that we did not see or hear the witnesses, this court is convinced of the appellant's guilt beyond a reasonable doubt. *Turner*, 25 M.J. at 325; *see also* Art. 66(c), UCMJ.

Charge II, Specification 3

The appellant was found guilty of attempting to receive child pornography on divers occasions between 24 April 2004 and 14 January 2005. The evidence showed that on two occasions, the

appellant's file server using the name "bigrl" required an upload of files for credit prior to allowing Detective Adler and SA Jensen to download images. SA Jensen uploaded a corrupted file which could not be opened to the appellant's file server, while Detective Adler uploaded a file of a nude girl. On one other occasion, the file server "bigrl" attempted a mutual leech with the file server utilized by SA Trifiletti, but was unsuccessful because SA Trifiletti's computer was not being manually operated and could not engage in the trade.

We find the evidence both factually and legally sufficient to show that the appellant receive purported images of child pornography from Detective Adler and SA Jensen, and further attempted to receive images from SA Trifiletti.

Charge II, Specification 4,5 and 6; Additional Charge I, Specification 2; and Additional Charge II.

As for the remaining charges and specifications, reproducing child pornography for distribution between 24 April 2004 and 10 January 2005 (Charge II, Specification 4); advertising and soliciting child pornography on 24 April 2004 and 10 January 2005 (Charge II, Specifications 5 and 6); and visiting the channel "100%PreteenGirlsSexPics" (Additional Charge I, Specification 2 and Additional Charge II); we have considered the evidence adduced at trial in the light most favorable to the Government, and we find that a rational trier of fact could have found the elements of the offense beyond a reasonable doubt. *Jackson*, 443 U.S. at 318-19; *Turner*, 25 M.J. at 325; *Reed*, 51 M.J. at 561-62; *see also* Art. 66(c), UCMJ. In addition, after weighing all the evidence in the record of trial and recognizing that we did not see or hear the witnesses, this court is convinced of the appellant's guilt beyond a reasonable doubt. *Turner*, 25 M.J. at 325; *see also* Art. 66(c), UCMJ.

III. Preventing Spectators in the Courtroom from Viewing Images of Child Pornography

The appellant claims the military judge effectively closed the courtroom in violation of his Sixth Amendment right to an open and public trial, and committed plain error when he devised a system whereby the images of child pornography were restricted to computer monitors visible only to the testifying witness, the trial defense and Government counsels', the military judge, and the appellant. We disagree.

RULE FOR COURTS-MARTIAL 806(a), MANUAL FOR COURTS-MARTIAL, UNITED STATES (2005 ed.) provides that courts-martial shall be open to the public. R.C.M. 806(b)(1) allows the military judge to limit and even exclude spectators to maintain the dignity and decorum of the proceedings, provided the limitation or exclusion is narrowly tailored. R.C.M. 806(b)(2) provides for closure in certain circumstances.

Here, the military judge did not limit or exclude spectator access, nor close the courtroom. The prosecution exhibits containing images of child pornography, some of which were on CD ROMs, were broadcast on a plasma screen whose visibility was restricted to the witness authenticating the images, Government and trial defense counsels, the appellant, and the military judge. Prosecution and defense exhibits that did not contain images of child pornography were openly displayed and visible to the gallery.

The military judge noted his authority to limit the manner and scope of publishing exhibits. He concluded that this process was not a closure of the courtroom, but "a restriction on the viewing of contraband material relevant to the case but not relevant to the viewing of the general gallery to this court-martial." Record at 279. Since the trial defense counsels did not object to this process, we review under the plain error standard. *Nieto,* 66 M.J. at 149.

After review, we conclude the military judge did not commit plain error by restricting the spectators' view of the images of child pornography, and that his actions were not tantamount to a closure of the courtroom. The military judge acted within his discretion to maintain the dignity and decorum of the court-martial proceedings. He did not bar or limit spectator access, nor infringe upon the appellant's right to, and the public's interest in a public trial. *See* R.C.M. 806(b)(2), Discussion. Allowing the spectators to view the images of child pornography would not have fostered either the appellant's right to or the public's interest in a public trial.

IV. Violation of the Equal Protection Due Process Clause

We find the appellant's remaining assignment of error without merit. *See United States v. Gaines,* 61 M.J. 689 (N.M.Ct.Crim.App. 2005), *aff'd*, 64 M.J. 176 (C.A.A.A. 2006), *cert. denied*, 549 U.S. 1167 (2007); *see also Weiss v. United States,* 510 U.S. 163, 176-81 (1994).

Conclusion

The findings and approved sentence are affirmed.

Senior Judge VINCENT and Judge PRICE concur.

For the Court

R.H. TROIDL
Clerk of Court