IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

U N I T E D S T A T E S,	)	REPLY BRIEF ON BEHALF OF
	)	APPELLANT
	)	
v.	)	
	)	Crim. App. Dkt. No. 20090446
Specialist (E-4)	)	
MATTHEW J. McCLAIN,	)	
United States Army,	)	USCA Dkt. No. 12-0099/AR
Appellant	)	

MATTHEW T. GRADY
Captain, Judge Advocate
Appellate Defense Counsel
Defense Appellate Division
U.S. Army Legal Services Agency
9275 Gunston Road
Fort Belvoir, Virginia 22060
(703) 693-0737
U.S.C.A.A.F. Bar No. 35092

RICHARD E. GORINI
Major, Judge Advocate
Branch Chief, Defense Appellate Division
U.S.C.A.A.F. Bar No. 35189

IMOGENE M. JAMISON
Lieutenant Colonel, Judge Advocate
Deputy Chief, Defense Appellate Division
U.S.C.A.A.F. Bar No. 32153

PATRICIA A. HAM
Colonel, Judge Advocate
Chief, Defense Appellate Division
U.S.C.A.A.F. Bar No. 31186

INDEX OF REPLY BRIEF ON BEHALF OF APPELLANT

TABLE OF CASES, STATUTES, AND OTHER AUTHORITIES

IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

United States, Appellee	) REPLY BRIEF ON BEHALF OF) APPELLANT
v.	)
	) Crim. App. Dkt. No. 20090446
Specialist (E-4) **MATTHEW J. MCCLAIN,** United States Army, Appellant.	))) USCA Dkt. No. 12-0099/AR)

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

ISSUE PRESENTED

WHETHER THE EVIDENCE IS LEGALLY SUFFICIENT TO SUPPORT APPELLANT'S CONVICTION OF POSSESSING CHILD PORNOGRAPHY.

Summary of Argument

The government primarily argues that legally sufficient evidence exists as to Specification 1 of the Charge in this case "because appellant confessed to downloading the four charged videos of child pornography[] [and] the government introduced copies of those videos." (Government Appellate Brief ["GAB"] 6.) Neither of these arguments is accurate, which only highlights the fact that legally sufficient evidence does not exist as to Specification 1 of the Charge. Moreover, the government failed to prove that appellant exercised the requisite dominion and control over the charged videos to sustain a conviction for possessing child pornography.

Argument

1. Appellant Never Confessed To Downloading The Four Charged Videos At Issue

According to the government, "[a]ppellant admits in his sworn statement that he was assigned to Hawaii when he downloaded the '4 videos.'" (GAB 11.) The government further argues that "appellant's own words and admissions give rise to the inference that he knew what child pornography was and knowingly downloaded it to his computer." (GAB 14.) The government relies heavily on paragraph 20 in Prosecution Exhibit 6 for Identification (JA. at 369-70) and SA Marc Smith to support these propositions. For example, the government makes the following claim:

> Section 20 of the NCIS report contains the four specific videos charged and a description of the videos. In response to the military judge's questions and without objection, SA Smith confirmed that he showed those same four video titles to appellant from the report and appellant admitted to downloading them.

(GAB 14.)

At the outset, it is important to point out the obvious: neither the titles of the file names nor a description of the videos the government charged appellant with possessing are contained in the four corners of appellant's statement to SA Smith. (JA. at 357-59.) More importantly, SA Smith never testified as to the content or description of the four videos

contained in paragraph 20 of the "NCIS report." (JA. at 276-79.) Therefore, the description of the content of the videos contained in paragraph 20 of the "NCIS report" cannot be considered by this Court as substantive evidence. The description of the content of the videos contained in the "NCIS report" was never introduced into evidence, detailed by SA Smith as part of appellant's statement to him, or admitted by appellant.

At best, SA Smith's testimony only establishes that appellant admitted to downloading files with the same file names as those listed on the charge sheet. (JA. at 276-79.) However, this part of SA Smith's testimony directly conflicts with appellant's statement since appellant swore he did not recall the file names of the videos he downloaded. (JA. at 358.) This contradiction is curious since SA Smith also clarified that appellant typed the narrative portion of his statement while SA Smith typed the question and answer portion. (JA. at 279.) Presumably, SA Smith would have typed that appellant recognized the file names that he downloaded instead of typing "I don't recall there [sic] names now." (JA. at 358.)

In any event, neither appellant's statement nor SA Smith's testimony establishes the *content* of the charged videos. Appellant did not state that the videos he downloaded contained the same content as the videos that SA Devinny obtained from the

gnutella network. In addition, SA Smith did not have appellant describe the content of the four videos he allegedly downloaded while in Hawaii. Such a description could then have been compared to the videos SA Devinny downloaded from the gnutella network to determine if they were, in fact, the same.

In sum, appellant never admitted that the files he allegedly downloaded while in Hawaii were the same video files that SA Devinny obtained from others on the gnutella network. Stated differently, neither appellant's statement nor SA Smith's testimony sheds any light on the exact *content* of the videos the government charged appellant with possessing. In fact, both SA Smith and appellant specifically testified that SA Smith never showed appellant the four videos the government charged appellant with possessing. (JA. at 275, 335.) Such confirmation would be helpful in knowing if the videos appellant allegedly downloaded were the same videos that SA Devinny obtained from others on the Internet. Thus, the government's argument is misplaced because there is no support for the proposition that appellant admitted to downloading the same videos that SA Devinny obtained from the Internet.

2. The Government Charged Appellant With Possessing Four Specific Videos; However, It Has Yet To Show What The Exact Content Of These Videos Were As They Existed On Appellant's Computer On March 11, 2008

Assuming that SA Devinny's testimony was properly admitted under Military Rule of Evidence ["M.R.E."] 701 and that the military judge did not and could not consider the statistical significance of any testimony concerning SHA1 values, the remaining evidence does not show that the government introduced copies of the charged videos. Without considering the mathematical significance behind SHA1 values,[1] the government can only link the charged videos to appellant by filename.

Essentially, the government is asking this Court to find the evidence legally sufficient because a layperson opined that he obtained the *exact* same video that appellant had on his computer because he went on the Internet and found a file with the same title. The flaw in the government's reasoning is that the mere fact that two files may share the same file name does not necessarily mean that they share the exact same *content*. To this day, the government has not presented any evidence as to the exact content of the charged videos as they appeared and existed on appellant's computer. Moreover, the charged

[1] The military judge recognized the significance of SHA1 values was meaningless in this case because there was no expert testimony presented as to the statistical significance of them. (JA. at 212.)

filenames themselves are not indicative of content. *See United States v. Leedy*, 65 M.J. 208, 215 (C.A.A.F. 2007).

An example should help illustrate the inadequacy of the government's case. Suppose that the government charged appellant with receiving and possessing a stolen movie, i.e., *Chicago*,[2] that belonged to his First Sergeant in violation of Article 134, UCMJ. Further assume that the First Sergeant's version of *Chicago* contained never seen before footage and a unique "32 alphanumeric" serial number that the First Sergeant provided to law enforcement. At trial, assume that the only evidence produced was the following:

- Appellant listed a copy of *Chicago* for sale one day on Craig's List;[3]
- Appellant sold his copy of *Chicago* and law enforcement never retrieved it; and
- A NCIS agent testified that he obtained a copy of *Chicago* from the Internet from some unknown third party and this copy of *Chicago* was introduced into evidence.

In this example, it is obvious that the First Sergeant's version or copy of *Chicago* is not necessarily the same as the

---

[2] The military judge used the movie *Chicago* as an example in some of his exchanges with appellant's trial defense counsel. (JA. at 212.)

[3] Craig's List refers to a "centralized network of online communities featuring free online classified advertisements, with sections devoted to jobs, housing, personals, for sale, services, community, gigs, résumés, and discussion forums." http://en.wikipedia.org/wiki/Craigslist (last visited February 24, 2012).

one appellant had in his possession at one time. Yet the government would have this Court believe that the First Sergeant's stolen copy of *Chicago* was the same copy that appellant possessed at one time because they share the same title, size, and file type. Such a showing would be inadequate, just as the evidence in appellant's case in inadequate.

The only way the government could definitely prove that appellant possessed the First Sergeant's copy of *Chicago* in this example would be via the unique "32 alphanumeric" serial number. For instance, if appellant's Craig's List advertisement in this example contained the same unique "32 alphanumeric" serial number that the First Sergeant provided to law enforcement, then a case could be made that appellant received and possessed the First Sergeant's copy of *Chicago*. Similarly, the only way the government can prove that the *content* of the videos files SA Devinny obtained from the Internet are the same video files that appellant had on his computer on March 11, 2008, would be by considering the mathematical significance of hash values. However, the government presented no evidence on the merits as to the statistical significance of hash values and the military judge clarified that he would not consider the statistical significance of them. (JA. at 212.) "When a judge indicates that he will not consider inadmissible evidence, including

expert opinion testimony, we presume he will do as he says." *United States v. Davis*, 44 M.J. 13, 17 (C.A.A.F. 1996).

3. Even When Viewed In The Light Most Favorable To The Government, The Evidence Does Not Show That Appellant Exercised Sufficient Dominion and Control Over The Four Charged Videos

"In the electronic context, a person can . . . possess child pornography without downloading it, if he or she seeks it out and exercises dominion and control over it." *United States v. Romm*, 455 F.3d 990, 998 (9th Cir. 2006). In this case, the government failed to prove that appellant exercised the requisite dominion and control over the four charged videos in question. At best, the evidence shows that appellant possibly and fleetingly *viewed* the charged videos on some uncertain date. Fleetingly viewing videos is insufficient to prove that appellant knowingly possessed child pornography. *See id.* at 998 (holding that "Romm exercised dominion and control over the images in his cache by enlarging them on his screen, and saving them there for five minutes before deleting them"). Instead, the government must show that appellant actually exercised control over the videos, such as saving the videos into a separate folder or viewing them again on a separate occasion. *See id.* at 1001 (acknowledging that forensic and other evidence demonstrated that Romm actually exercised the requisite control over the charged images of child pornography).

United States v. Kuchinski, 469 F.3d 853 (9th Cir. 2006), is illustrative in demonstrating that appellant did not exercise dominion and control over the charged videos. There, the evidence showed that images would automatically download and save information to one's Temporary Internet Files and that this action would occur without any action or knowledge of the computer user. *Id.* at 862. There was also no evidence "that Kuchinski was sophisticated, that he tried to get access to the cache files, or that he even knew of the existence of the cache files." *Id.* Ultimately, the court concluded that it was improper to consider the cache file images in calculating Kuchinski's offense level for sentencing purposes. *Id.* at 863. The court gave the following reasoning:

> Where 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. To do so turns abysmal ignorance into knowledge and a less than valetudinarian grasp into dominion and control.

Id. at 863.

Finally, *United States v. Flyer*, 633 F.3d 911 (9th Cir. 2011), also demonstrates that appellant lacked the requisite dominion and control over the videos in this case. In *Flyer*, there was no evidence that Flyer knew of the presence of

contraband files in the unallocated space of his computer's hard drive. *Id.* at 919. There was also no forensic evidence demonstrating that Flyer could see or access the files in his unallocated space. *Id.* In addition, there was no forensic evidence indicating that Flyer had accessed, enlarged, or manipulated any of the charged images. *Id.* Finally, Flyer did not admit that he had viewed the charged images on or near the time he was charged with doing so. *Id.*

The government in *Flyer* argued that the evidence established possession because the files had been deleted at some point in time, which is how they were placed in the unallocated space of Flyer's hard drive to begin with. *Id.* at 920. Thus, the government's theory was that Flyer exercised dominion and control over the images by destroying the copies of the images located on his computer. *Id.* The court rejected this argument and found that "[n]o evidence indicated that on or about April 13, 2004, Flyer could recover or view any of the charged images in unallocated space or that he even knew of their presence there." *Id.* Thus, the court reversed Flyer's conviction as to the images he was charged with possessing in his unallocated space. *Id.*

The facts in this case are similar to *Kuchinski* and *Flyer*. Appellant was not a "sophisticated" computer user, as he had no formal training in computers and possessed only rudimentary

knowledge of them. (JA. at 301.) Back in March 2008, appellant did not completely understand how Limewire worked and just clicked "next" when downloading Limewire for the first time. (JA. at 303-04.) Appellant testified that he did not know what a share folder was and that he never went into the share folder on his computer. (JA. at 307-08.) Instead, appellant remained in the main Limewire application itself when he searched for movies. (JA. at 308.) In fact, appellant testified that he did not know where a Limewire share folder could be found on his computer. (JA. at 310.)

Similar to *Kuchinski*, there is no evidence that appellant was a sophisticated computer user or knew of the existence of a Limewire share folder. Similar to *Flyer*, there is no evidence that appellant accessed or viewed any of the charged videos, and appellant did not admit to viewing the charged videos on or about March 11, 2008. The only distinction between this case and *Kuchinski* and *Flyer* is that appellant seemingly would have access to the videos contained in his Limewire share folder. However, the government never proved that these videos were accessible. Stated differently, the government never proved that the videos were playable or operable. In fact, the opposite presumption is true in this case because SA Devinny attempted to download and play the four charged videos directly from appellant, but was unsuccessful for some unknown reason.

(JA. at 249.) Moreover, SA Devinny could not ascertain if the videos contained a virus or were corrupted in some fashion. (JA. at 248-49.) Given the similarities of this case with *Kuchinski* and *Flyer*, this Court should find the evidence legally insufficient as to Specification 1 of the Charge.

Conclusion

WHEREFORE, appellant requests that this Honorable Court dismiss the Charge with prejudice.

MATTHEW T. GRADY
Captain, Judge Advocate
Appellate Defense Counsel
Defense Appellate Division
U.S. Army Legal Services Agency
9275 Gunston Road, #3206
Fort Belvoir, Virginia 22060
(703)693-0656
USCAAF No. 35092

RICHARD E. GORINI
Major, Judge Advocate
Branch Chief
Defense Appellate Division
USCAAF No. 35189

IMOGENE M. JAMISON
Lieutenant Colonel,
Judge Advocate
Deputy,
Defense Appellate Division
USCAAF No. 32153

PATRICIA A. HAM
Colonel, Judge Advocate
Chief,
Defense Appellate Division
USCAAF No. 31186

CERTIFICATE OF COMPLIANCE WITH RULE 24(d)

1. This brief complies with the type-volume limitation of Rule 24(c) because this brief contains 2,580 words.

2. This brief complies with the typeface and type style requirements of Rule 37 because this brief has been prepared in a monospaced typeface (12-point, Courier New font) using Microsoft Word, Version 2007 with no more than ten and a half inch characters per inch.

MATTHEW T. GRADY
Captain, Judge Advocate
Appellate Defense Counsel
Defense Appellate Division
U.S. Army Legal Services Agency
9275 Gunston Road
Fort Belvoir, Virginia 22060
(703)693-0656
USCAAF Bar No. 35092

CERTIFICATE OF FILING AND SERVICE

I certify that a copy of the foregoing in the case of *United States v. McClain*, Crim.App.Dkt.No. 20090446, USCA Dkt. No. 12-0099/AR, was electronically filed with both the Court and Government Appellate Division on February 29, 2012.

MICHELLE L. WASHINGTON
Paralegal Specialist
Defense Appellate Division
(703) 693-0737