IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES *Appellee* v. Airman First Class (E-3) **JEREMIAH L. KING**, United States Air Force *Appellant*	**BRIEF ON BEHALF OF APPELLANT** Crim.App. Dkt. No. ACM 39055 USCA Dkt No. 18-0288/AF August 30, 2018

TO THE HONORABLE, THE JUDGES OF THE UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES

DUSTIN J. WEISMAN, Capt, USAF
Appellate Defense Counsel
U.S.C.A.A.F. Bar No. 35942
Air Force Appellate Defense Division
1500 W Perimeter Road, Suite 1100
JB Andrews, MD 20762
Office: (240) 612-4770
dustin.j.weisman.mil@mail.mil

Counsel for Appellant

INDEX

TABLE OF AUTHORITIES

Page(s)

Statutes

Court of Appeals for the Armed Forces

Service Courts of Criminal Appeals

Federal Circuit Courts of Appeals

Federal District Courts

Other Authorities

Issue Presented

THE MILITARY JUDGE FOUND APPELLANT GUILTY OF VIEWING CHILD PORNOGRAPHY. BUT ALL OF THE ALLEGED CHILD PORNOGRAPHY APPELLANT ALLEGEDLY VIEWED WAS FOUND IN UNALLOCATED SPACE OR A GOOGLE CACHE. IS THE EVIDENCE LEGALLY SUFFICIENT?

Statement of Statutory Jurisdiction

The lower court had jurisdiction pursuant to Article 66(b)(1), Uniform Code of Military Justice (UCMJ), 10 U.S.C. §866(b)(1) (2012). The jurisdiction of this Court is invoked under Article 67(a)(3), UCMJ, 10 U.S.C. §867(a)(3) (2012).

Statement of the Case

On March 2, 2016, A1C King was tried at a general court-martial by a military judge sitting alone at Eielson Air Force Base, Alaska. Contrary to his pleas, A1C King was found guilty of one charge and one specification of attempting to view child pornography (Charge I, Specification 1) in violation of Article 80, UCMJ, 10 U.S.C. § 880 (2012); one charge and one specification of violating a lawful general regulation in violation of Article 92, UCMJ, 10 U.S.C. § 892 (2012); and one charge and one specification of viewing child pornography (Charge III, Specification 2) in violation of Article 134, UCMJ, 10 U.S.C. § 934

(2012).[1] Joint Appendix (JA) at 452. A1C King was sentenced to be reduced to the grade of E-1, to be confined for nine months, and to be dishonorably discharged from the service. R. at 854-55. On April 20, 2016, the convening authority approved the findings and sentence as adjudged. JA at 4-9.

The CCA approved the findings and sentence on July 26, 2017. JA at 1-2. On August 25, 2017, A1C King timely filed a motion for reconsideration. JA at 3. The CCA denied the request on April 24, 2018. JA at 3.

Appellant petitioned this Court for review on June 20, 2018, and this Court granted review on August 7, 2018.

Statement of Facts

Air Force Office of Special Investigations (AFOSI) agents seized 34 of A1C King's electronic devices and sent the devices to the Defense

[1] A1C King was acquitted of: one specification of attempting to view child pornography in violation of Article 80, UCMJ, 10 U.S.C. § 880 (2012); one specification of possession of child pornography in violation of Article 134, UCMJ, 10 U.S.C. § 934 (2012); and, one specification of communicating indecent language in violation of Article 134, UCMJ, 10 U.S.C. § 934 (2012). JA at 452.

Additionally, prior to A1C King entering pleas, the government withdrew and dismissed: one specification of possession of child pornography in violation of Article 134, UCMJ, 10 U.S.C. § 934 (2012); and, one specification of viewing child pornography in violation of Article 134, UCMJ, 10 U.S.C. § 934 (2012). JA at 10-14.

Computer Forensics Lab (DCFL) for analysis. JA at 490-91. There, Mr. BB, the government's forensic computer examiner, combed through "thousands of photos" of anime pornography[2] and real pornography that was discovered on the devices. JA at 139, 186, 471-72. But he only found three files of child pornography.[3] *See* JA at 6.

Two of these files (01136627.jpg and 01136666.jpg) were found in a Google cache and the other (01173367.jpg) was found in unallocated space. JA at 259, 339, 479-81, 483. All three files were found on the same computer, a desktop computer seized from A1C King's home. JA at 197, 472, 479-81, 483.

---

[2] "Anime" is a "cartoon image[]." R. at 134.

[3] Although the government claimed that more than three files contained child pornography, the military judge only found the following files met the legal definition: "01136627.jpg," "01136666.jpg," and "01173367.jpg." JA at 6, 452.

The military judge determined that these three files were child pornography based upon his consideration of the statutory definitions and the *United States v. Dost*, 636 F.Supp. 828 (S.D. Cal. 1986), factors. "No NCMEC [National Center for Missing and Exploited Children] hash matches were found." Pros Ex. 10 at 2. Stated another way, there were "[n]o photographs or videos of known child pornography" found in this case. JA at 471.

Unallocated Space

Computers operate on two levels, the logical space and the physical (unallocated) space. JA at 209. Logical space is what computer users are most familiar with because it is the interactive level where information is displayed and users can manipulate files, visit webpages, and change settings. *Id*. It is "space that you have access to." *Id*.

Conversely, physical (unallocated) space is "all the space that's available on the hard drive itself." *Id*. It is an "an area on the system that the file system has availability to write to." JA at 342. "[I]t can contain files that previously existed, deleted files, things like that." JA at 210. The only way to get to unallocated space is through a forensic tool. JA at 343. Absent using forensic tools, a user does not have access to the physical (unallocated) space. JA at 210, 342, 345.

If a file is discovered in unallocated space there is no way to determine how long it has resided there, what the file name was, where the file was located on the computer, or where the file came from. JA at 344-45. Nor is there a "way to tell when it may have been initially looked at or pulled up on the web browser or search or anything like

that." JA at 346. In fact, it is impossible to determine if the file was ever even viewed by a person. *Id.* A file's existence in unallocated space "[j]ust [shows] that it existed on the system at one time." *Id.*

Internet Caches Generally and the Google Cache

An internet cache is "used by the web browsers to ultimately reduce the time that it would take a user to get to a specific webpage" if the user returned later. JA at 212. For instance:

> if you were to visit espn.com for example, your web browser would cache some of the images on ESPN or potentially, the whole webpage of ESPN to your local system; that way, if you ever navigated to espn.com, again, it would not need to request the complete webpage from the internet; it would have files locally to retrieve and provide a faster loading time.

Id. "It can . . . it captures anything . . . it'll save pictures or potentially whole webpages." *Id.*

This caching of webpages is something that happens automatically on a computer. JA at 213. A user has no control over it and has no way of knowing it is occurring. JA at 336. Depending on which browser is used, the cached files could be kept indefinitely. JA at 212-13.

A Google cache is a particular type of cache associated with the internet browser Google Chrome. JA at 330. Google Chrome, like

Internet Explorer, is a browser that allows a user to get access to the internet. JA at 324. As with other internet browsers, "[w]hen you visit a particular web page, Google Chrome has the ability to cache or save portions of the webpage, images from the webpage, or potentially the whole webpage to your system within the cache; and that ultimately reduces the amount of time it takes to load the webpage if you were to visit that page again." JA at 330, 479.

The Google cache that Google Chrome creates is an automatic function that the user does not see or have control over. JA at 324, 336. Whenever a user visits a website using Google Chrome, Google Chrome copies the images from the site over into the Google cache on its own, outside the purview of the user. JA at 336, 472. "[E]ach site [the user] go[es] to is actually performing this automatic cache." JA at 402, 479.

Although the Google cache is located in the logical (user accessible) space of a computer, it is generally not accessible to the average user for two reasons. First, the file path to find the Google cache is obscure. In the instant case, the Google cache file containing the images at issue (01136627.jpg and 01136666.jpg) has a complicated file path:

"C:\Windows.old\Users\jeremiah\AppData\Local\Google\Chrome\User Data\Default\Cache." JA at 479. Second, even if the user were able to locate the Google cache file, the file itself is inaccessible without forensic tools. JA at 360, 371. Even with the assistance of forensic tools, it is impossible to say which website the image came from, whether the image displayed on the user's screen, or whether the user clicked or otherwise manipulated the image. JA at 406.

Unlike other browsers, such as Internet Explorer, the cache that Google Chrome uses is a single file as opposed to multiple files within a single folder. JA at 371. Without forensic tools, a user cannot turn the Google cache file into a viewable image. JA at 369, 371. In other words, the Google cache images in this case (01136627.jpg and 01136666.jpg) were not directly viewable and had to be extracted from the Google cache using forensic tools to create a viewable image. *Id*.

In addition to not rendering viewable images, the Google cache does not link back to the websites where the images were cached. JA at 371. Stated another way, even if a user was able to open the Google cache, there are not hyperlinks that direct the user to the webpages where the images came from. *Id*.

Finally, like most other caches, the Google Cache is capable of being emptied (or cleared) by the user or by an automatic function. JA at 340-42. However, in the instant case, Mr. BB determined that A1C King did not manually clear the Google cache. JA at 341. When the Google cache automatically clears itself, the cache file is removed from the logical (user accessible) space on the computer and then resides in the computer's unallocated (non-accessible) space. JA at 342, 346.

What is Visible to the User

It is impossible to determine if an image found in a Google cache was ever displayed on the user's screen. JA at 383. This is because there are two ways images are cached, and neither way limits the caching to just those images displayed on the user's screen. JA at 253-54.

First, Google Chrome may cache the entire webpage. JA at 253-54. This is how most standard webpages are cached. *Id.* Since Google Chrome caches the entire webpage, the only way a user will see everything that is cached is if the user scrolls through all of the

webpage; however, there's no way to determine if the user looked at the entire webpage. JA at 335, 367, 401.

Second, instead of caching the entire webpage, Google Chrome may cache a certain part of the webpage and cache more of the webpage as the user continues to scroll down. JA at 253-54, 335. "For example, if you were doing a Google search, a Google image search, the images are displayed and they generally aren't loaded . . . further ones aren't loaded until you actually scroll down and then you can see the image as well." JA at 253-54. In this scenario, if there were 10 images on the screen, Google Chrome may cache another 20 or 30 images onto the computer that are outside of the user's view so that when the user scrolls down the images will be ready.[4] JA at 335. As a result, Google Chrome may cache an image that's further down than what the viewer saw and so the user may not even know the image existed and was cached. JA at 337-38. Even with forensic tools, Mr. BB testified he was "uncertain as to the certainty of what a user would or would not see." JA at 383.

[4] The government's forensic computer examiner, Mr. BB, used these numbers illustratively. JA at 335. Mr. BB testified that he had no idea or understanding of how many images Google Chrome will pre-load into the cache. JA at 401. It could be 10, 50, or more. *Id*.

Files 01136627.jpg and 01136666.jpg

The file 01136627.jpg is a picture that depicts a dark-haired female, of unknown age, with a penis near her mouth. JA at 498. Mr. BB found the file in the Google cache. JA at 251, 339, 479. The most Mr. BB was able to testify about the file was that "a website containing this image file was visited by the user "Jeremiah" between . . . 15 October 2012 and 18 April 2013." JA at 251. However, Mr. BB was "not sure exactly what website this specific image came from." JA at 256. "It could have been part of a whole webpage that was loaded [cached] or it may have loaded [cached] as the user scrolled down depending on what specific webpage that this image came from." *Id*. "[O]ther than he [the user] accessed a website at one time that resulted in this image automatically being cached to his system[,] [t]here [are] no artifacts that would show whether the user later accessed that file." JA at 338.

The file 01136666.jpg was also found in the Google cache. JA at 339, 479. It is a picture that depicts a nude female, approximately 8 to 9 years-old, covering her genitalia. JA at 496. Like the other file found in the Google cache (01136627.jpg), Mr. BB testified the image "would

have existed like on the webpage like we talked about, but I have no way of knowing, like we spoke about earlier, how long [it] may have been on the screen or if [it was] on the screen." JA at 363.

As it relates to both Google cache images, Mr. BB was "not certain of what specific webpage that these images would have come from." JA at 379. Nor was he able to point to any evidence that indicated A1C King ever saw either of these images. JA at 364. In fact, Mr. BB acknowledged that "it could have been that he didn't see it because the cache may have created it." *Id*. Neither file (01136627.jpg or 01136666.jpg) was found in the user-accessible space on any of the 34 devices AFOSI seized. JA at 398. Both are "remnants of previously existing files." *Id*.

File 01173367.jpg

File 01173367.jpg was found in unallocated space. JA at 259, 483. "Consequently, no additional information such as [the] original file name[], time and date stamps, or the origin of the file[] can be determined." JA at 483; *see also* JA at 260. In fact, Mr. BB testified that the only thing he was able to determine about the file is that "it may have existed in some logical [user-accessible] form on the machine,

either cache or otherwise, on the machine." JA at 366. *See also* JA at 261, 346, 365. Although it is possible that the file ended up in unallocated space after it was removed (deleted) from a cache during an automatic clearing process, ultimately Mr. BB had no way of telling if or how the file was removed from the user-accessible portion of the computer. JA at 366.

As with the two Google cache images, 01173367.jpg was not found on the logical (user-accessible) space of any of the 34 devices AFOSI seized. JA at 398. Finally, because the file (01173367.jpg) was found in unallocated space, it was impossible for A1C King to access, or convert the file into a visible image, without using forensic tools. JA at 369.

Evidence of Tampering

All three files of child pornography were inaccessible to A1C King unless he had the knowledge and tools to access them and convert them to a viewable image. JA at 369, 371, 398. But Mr. BB "did not see any indication" that A1C King had the forensic tools necessary to access the files. JA at 372. Nor did Mr. BB have any reason to believe A1C King knew the images existed, understood how the Google cache worked,

understood how unallocated space worked, or knew that images were being saved to his computer. JA at 340, 372-73.

Even if A1C King had the requisite knowledge and possessed the forensic tools necessary, "[n]o artifacts were found suggesting that a user [A1C King] attempted to hide prohibited material in a[n] encrypted container or file." JA at 472. Furthermore, "[t]here's no indication of" A1C King attempting to remove or otherwise access any of the three files. JA at 339-40; *see also* JA at 368. All three files were basically undisturbed. JA at 340.

Connection Between Search Terms and Files

The military judge convicted A1C King of attempting to view child pornography based on evidence that a user of a computer found in A1C King's home had entered search terms associated with child pornography into two internet search engines.[5] JA at 4, 452. The internet search engines that were used were Google and Bing. JA at 485. Mr. BB found that these searches were all conducted between September and November 2013. *Id*.

[5] The military judge found that A1C King searched for "skimpy preteen," "sexy little girls," "loli porn," "nude dani camy," "father/daughter porno," "little girl," "goth loli," and "lolion pictures," and that these searches amounted to an attempt to view child pornography. JA at 4, 452.

Despite the search terms being found on the computer, "[i]nternet analysis was conducted on [all 34 devices seized] and no determination was made on whether [A1C King] visited known child pornography websites." JA at 471. No photographs or videos of known child pornography were found. *Id.* And "[n]o webmail or email artifacts were found that indicate any attempts to produce, distribute child pornography, or arrange a sexual encounter with a minor." *Id.*

Mr. BB testified it is possible for a user to search for lawful pornography, but the search results contain illicit child pornography. JA at 399-400. These images of unintended child pornography (and the search that resulted in them) could then be automatically cached to the user's computer and the user would not know about it. *Id.* Another possibility is that a user who likes anime (like A1C King) could be looking for cartoons but then real images of child pornography could be returned inadvertently. *Id.*

As it relates to the three files the military judge determined were child pornography in this case, none were connected to search terms Mr. BB found in his forensic analysis. JA at 400. In fact, the two Google cache files were created sometime between October 2012 and

April 2013, which is over five months before the search terms were entered.[6] JA at 479, 485.

Summary of Argument

The military judge convicted A1C King of viewing child pornography (Charge III, Specification 2) based on the presence of three files found in user-inaccessible areas of a computer. This was error because no reasonable fact-finder could have found beyond a reasonable doubt that any of these three images were displayed on the computer screen and/or that A1C King knowingly viewed them. To the contrary, the government's own computer expert acknowledged there was no way to tell if the images were ever displayed, and there is no forensic evidence that A1C King ever even saw the images.

Argument

THE EVIDENCE SUPPORTING A1C KING'S CONVICTIONS FOR VIEWING AND ATTEMPTING TO VIEW CHILD PORNOGRAPHY IS LEGALLY INSUFFICIENT BECAUSE ALL OF THE ALLEGED CHILD PORNOGRAPHY WAS FOUND IN UNALLOCATED SPACE OR A GOOGLE CACHE.

[6] Mr. BB could not determine when the file found in unallocated space (01173367.jpg) was created because it is impossible to determine forensically the creation, modification, or deletion dates for files in unallocated space. JA at 344-45.

Standard of Review

Legal sufficiency of the evidence is reviewed *de novo*. *United States v. Kearns*, 73 M.J. 177, 180 (C.A.A.F. 2014). "[T]he question of legal sufficiency requires us to consider the evidence in the light most favorable to the Government, and to determine whether the evidence provides a sufficient basis upon which rational factfinders could find all the essential elements beyond a reasonable doubt." *United States v. Holt*, 52 M.J. 173, 186 (C.A.A.F. 1999).

Law

Elements of Article 134, UCMJ, Viewing Child Pornography

The elements of viewing child pornography, Article 134, UCMJ, 10 U.S.C. § 934, are: (1) the accused knowingly and wrongfully viewed child pornography; and (2) that under the circumstances, the conduct of the accused was of a nature to bring discredit upon the armed forces. Manual for Courts-Martial, United States (2012 ed.), pt. IV, ¶ 68b.b.(1). Two factors for consideration of wrongfulness are whether the images were (1) unintentionally or (2) inadvertently acquired. *MCM*, pt. IV, ¶ 68b.c.(9). This includes "the method by which the visual depiction was acquired, the length of time the visual depiction was maintained, and

whether the visual depiction was promptly, and in good faith, destroyed or reported to law enforcement." *MCM*, pt. IV, ¶ 68b.c.(9).

Court of Appeals for the Armed Forces Precedent

This Court has yet to directly address whether contraband files found in a computer's cache or unallocated space, standing alone, are legally sufficient to establish an accused's knowledge for the offense of viewing child pornography. The closest this Court has come to answering that question was in *United States v. Navrestad*, 66 M.J. 262, 267 (C.A.A.F. 2008). In that case, the Court set aside the accused's conviction for possessing child pornography, finding the evidence that the accused viewed and then sent a link containing child pornography to another person was legally insufficient to establish dominion and control. *Id*. at 268. In coming to this holding, the Court found that "knowing" possession of child pornography requires the viewing of the images to be both "knowing and conscious." *Id*. at 267. Applying these definitions, the Court held that the accused did not knowingly possess images of child pornography where: (1) he could not access the areas of the computer's hard drive where the subject images had been automatically saved; (2) he could not download the images to a portable

storage device; and (3) there was no evidence he had e-mailed, printed, or purchased copies of the subject images. *Id*. at 267.

Service Courts of Criminal Appeals Precedent

Although the Service Courts of Criminal Appeals (CCAs) have not addressed the knowledge requirement of viewing child pornography when the evidence is found solely in a cache or unallocated space, they have addressed it in the context of possession of child pornography.

For instance, in *United States v. Kamara*, the CCA set aside and dismissed a specification for possession of child pornography, finding no knowing possession. No. 201400156, 2015 CCA LEXIS 214 (N-M. Ct. Crim. App. May 21, 2015) (unpub. op.). The images were located in unallocated space and there was no evidence appellant had a forensic device to access the unallocated space or knew how to use such a forensic device. *Id*. at *10-11. Even if the appellant did have forensic tools, there was no evidence he knew the files were in unallocated space. *Id*. The fact that 70% of the images on appellant's devices were child pornography, and the fact that the government's expert could link search terms to child pornography that was charged in a different

specification[7], did not cure the lack of evidence demonstrating the appellant's knowledge of the files found in unallocated space. *Id*. at *3, 9-11.

Similarly, in *United States v. Nichlos*, the CCA set aside and dismissed a finding of guilty for possession of child pornography finding the evidence legally insufficient to establish that the appellant knowingly possessed child pornography within the charged timeframe. No. 201300321, 2014 CCA LEXIS 691, at *7-8 (N-M. Ct. Crim. App. September 18, 2014) (unpub. op.), *petition for grant of review denied*, 74 M.J. 358 (C.A.A.F. 2015). Although the evidence suggested the appellant likely possessed (in allocated space), and viewed, the child pornography because he used the Google search engine to search for and access a website responsive to the search term "9yo Jenny pics," the fact that the child pornography was only found in unallocated space proved dispositive. *Id*. at *29-34. The government did not put on any proof that the appellant (1) knew the file was in unallocated space or (2) had the knowledge or tools to access unallocated space. *Id*. at *33-34.

[7] This child pornography was found in allocated space. *Kamara*, 2015 CCA LEXIS 214 at *3, 9.

Finally, in *United States v. Schempp*, the Army CCA found the evidence legally insufficient to support a conviction for possession of child pornography when the pornographic files were all located in unallocated space. 20140313, 2016 CCA LEXIS 147 (A. Ct. Crim. App. February 26, 2016) (unpub. op.), *petition for grant of review denied*, 75 M.J. 341 (C.A.A.F. 2016). The Army court reasoned that since the accused "was unable to access any of the images in unallocated space, he lacked the ability to exercise 'dominion or control' over the[] files." *Id.* at *8. Even though the images in unallocated space could be accessed with forensic software, there was no evidence the accused possessed any such tools, or the knowledge to use them. *Id.* at *6-7. Thus, the government could not establish that he had constructive possession of the images in unallocated space. *Id.*

The CCAs have found the evidence sufficient to establish knowing possession, even when the evidence is located in unallocated space or a cache, when the government presents additional evidence demonstrating knowledge. *See*, *e.g.*, *United States v. Yohe*, ACM 37950, 2015 CCA LEXIS 380 at *3-*4 (A.F. Ct. Crim. App. July 22, 2013) (unpub. op.) *petition for grant of review denied*, 75 M.J. 286 (C.A.A.F.

2016) (finding sufficient evidence to support a conviction of knowingly and wrongfully viewing based on evidence that the appellant found the videos through LimeWire after using search terms designed to find it, and then specifically selected the two videos for downloading, and watched them while they downloaded); *see also*, *United States v. Weiss*, ACM 38611, 2015 CCA LEXIS 538 at *13 (A.F. Ct. Crim. App. December 1, 2015) (unpub. op.), *petition for grant of review denied*, 75 M.J. 335 (C.A.A.F. 2016) ("While it is true that these files were found in areas of the computer that an average user could not access without specialized computer software, none of which was found on Appellant's computer, there was direct evidence from Appellant's statements that he knew images were still on his computer and he 'needed to magnetically erase them' and do a 'hard drive scrub.'"); *United States v. Sanchez*, 59 M.J. 566, 570 (A.F. Ct. Crim. App. 2003), *aff'd*, 61 M.J. 330 (C.A.A.F. 2005) (prosecution was able to establish knowing possession because there was testimony that appellant was computer savvy and there was an "electronic evidentiary trail" that showed appellant received, and later forwarded, an email with the child pornography images attached).

United States Courts of Appeals Precedent

As with military jurisprudence, there is a dearth of federal caselaw on whether contraband files found in a computer's cache or unallocated space are legally sufficient to establish an accused's knowledge for the offense of viewing child pornography. This is due in part to the fact that, up until 2008, federal law criminalized "knowing possession" but not mere viewing. *United States v. Moreland*, 665 F.3d 137, 141 (5th Cir. 2011); *see* 18 U.S.C. § 2252A (2008). Even under the most recent version of the federal statute, mere viewing is not proscribed, although accessing child pornography with the intent to view is. *See* 18 U.S.C. § 2252A (2018). Most of the federal caselaw centers on whether an accused can be convicted of knowing possession of child pornography when the child pornography possessed was located in a cache or unallocated space.

For instance, the Fifth, Ninth, and Tenth Circuits have all set aside convictions (or ordered re-sentencing) for possession of child pornography where (1) the subject images were discovered in inaccessible areas of an accused's computer, and (2) there was no evidence the accused accessed the images or knew they existed. *See*

Moreland, 665 F. 3d at 150 ("the government was required to introduce evidence . . . to support a reasonable inference both that [the accused] knew that the images were in the computers and that [the accused] had the knowledge and ability to access the images and to exercise dominion or control over them."); *United States v. Flyer*, 633 F.3d 911 (9th Cir. 2011) (setting aside conviction for possessing child pornography where the images were found in the unallocated space of the accused's computer and government did not present any evidence that the accused knew of the presence of the files on his hard drive); *United States v. Kuchinski*, 469 F.3d 853 (9th Cir. 2006) (ordering re-sentencing for an accused convicted of possessing images of child pornography found in his hard drive's "cache" because the accused lacked knowledge of the cache files and did not access the cache files); *United States v. Dobbs*, 629 F.3d 1199, 1204 (10th Cir. 2011) (setting aside a conviction where the government "presented no evidence" that the accused "had accessed the files stored in his computer's cache" even though evidence established he had searched for and viewed child pornography using his computer).

These Circuit Court cases have settled on several principles when it comes to using evidence retrieved from unallocated space, or a cache, to prove a child pornography charge. For child pornography found in unallocated space:

> even when the defendant has exclusive possession of his computer, evidence of storage of child pornography images in the hard drive of a defendant's computer, without more, is insufficient to sustain a conviction or sentence for knowing possession or receipt of child pornography; . . . in exclusive possession cases in which convictions have been upheld, the government has presented additional evidence of the defendant's knowledge, access and control of the child pornographic images.

Moreland, 665 F. 3d at 152.

As it relates to cache files, "a user must have knowledge of and access to the files to exercise dominion and control over them." *Flyer*, 633 F.3d at 919. *see also Kuchinski*, 469 F.3d at 863 (court could not consider images recovered from the cache when no evidence indicated that the defendant had tried to access the cache files or knew of their existence); *Dobbs*, 629 F.3d at 1207; *but see United States v. Romm*, 455 F.3d 990, 1001 (9th Cir. 2006) (the defendant had access to, and control over, the images displayed on his screen and saved to his cache, as he could copy the images, print them or email them to others, and did, in

fact, enlarge several of the images and attempt to delete them). According to the Ninth Circuit, to permit criminal liability based solely on the presence of a contraband file in a computer cache would be unjust:

> 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.

Kuchinski, 469 F.3d at 863.

Elements of Article 80, UCMJ, Attempt

The elements of attempt, Article 80, UCMJ, 10 U.S.C. § 880 (2012), are: (1) that the accused did a certain overt act; (2) the act was done with the specific intent to commit a certain offense under the code; (3) the act amounted to more than mere preparation; and (4) the act apparently tended to effect the commission of the intended offense. *MCM*, pt. IV, ¶ 4.b. "Preparation consists of devising or arranging the means or measures necessary for the commission of the offense." *MCM*, pt. IV, ¶ 4.c.(2). "The overt act required goes beyond preparatory steps

and is a direct movement toward the commission of the offense." *MCM*, pt. IV, ¶ 4.c.(2).

"It is a defense to an attempt offense that the person voluntarily and completely abandoned the intended crime, solely because of the person's own sense that it was wrong, prior to the completion of the crime." *MCM*, pt. IV, ¶ 4.c.(4).

Argument

A1C King's Conviction for Viewing Child Pornography is Legally Insufficient

This Court should reaffirm the rationale pronounced by several of the Federal Courts of Appeals and the CCAs regarding possession of child pornography and apply that rationale to the offense of viewing child pornography. Such a holding would dictate that, in cases such as the instant case, the mere existence of child pornographic files on a computer would be insufficient to establish knowing viewing and that the government must present evidence establishing both that (1) the accused actually saw the images and (2) his viewing was knowing and wrongful. Applying that holding to the facts of A1C King's case, the conviction is legally insufficient because the government did not offer such additional evidence.

No reasonable fact-finder could have found that A1C King knowingly viewed any of the three images of alleged child pornography because the government failed to put on any evidence that (1) the images were ever displayed on the computer screen, or (2) A1C King actually saw the images on the computer screen.[8] Furthermore, there was insufficient additional evidence to reasonably infer either (1) or (2).

(1) The mere existence of the files in a cache or in unallocated space does not establish that the images were viewable because the files could be saved onto the computer without ever being displayed on the screen.

Although the two cache files (01136627.jpg and 01136666.jpg) likely came from a webpage, the government's expert had no idea which webpage(s).[9] JA at 256. Not knowing the webpage(s) from which the images came is significant because the government is unable to show if the images were part of a whole webpage that was cached in its entirety

[8] There is an additional, and fatal, gap in proof as it relates to the image from unallocated space (01173367.jpg); namely, that the government cannot prove the image was viewed during the charged timeframe. Because this image was found in unallocated space, there is no "way to tell when it may have been initially looked at or pulled up on the web browser or search or anything like that." JA at 346.

[9] Even less is known about the file found in unallocated space (01173367.jpg). Although it is possible this file once existed as a cache file and was automatically deleted (JA at 366), the government's expert could not testify about anything regarding the file except that it may have existed in logical space at some point in time (*Id*.).

the moment it was visited, or if it was a webpage that cached progressively more as the user navigated the webpage. JA at 256.

If one or both of the cached files are associated with a webpage in the first category (*i.e.* one that caches the entire webpage), then the odds that the image never even appeared on the computer screen are very high. For instance, if a user visits a 10-page[10] website that is completely cached, but the user only views the first page, then 90% of the material cached from that website was never even displayed to the user. Because most websites cache this way (JA at 253-54), the odds are that the cached images in this case came from a website that caches this way.

Even if the website the two cache files are associated with was in the second category (*i.e.* the website cached more as the user scrolled down), there is still a high likelihood that the images were never displayed. This is because webpages in this category still cache images that have not yet been displayed to the user. *Id.* How much of the

[10] By referring to "page" counsel is referencing the amount of material that is displayed in one screen-sized segment.

webpage is cached before the user scrolls down is something the government's own expert did not know. JA at 335.

Ultimately, the distinction between the two ways websites cache is one without a difference. Under both methods, materials are cached that are never displayed to the user. As a result, the government's expert conceded he was "uncertain as to the certainty of what a user would or would not see." JA at 383. He also admitted he was not able to point to any evidence that indicated any of the three images were displayed on the screen. JA at 364. Thus, there is insufficient evidence for a fact-finder to reasonably conclude that the three images of child pornography were even capable of being viewed.

(2) Even if the government could prove the images appeared on the computer screen, the government failed to offer any proof that A1C King was the user at the time the images were displayed, or that, even if he was the user at the time, he actually saw the images and his viewing was knowing and wrongful.

Assuming, *arguendo*, that the three images were displayed on the computer screen, the government offered insufficient proof to establish that A1C King was the user at the time the images were displayed. Additionally, even if A1C King was the user at the time, the

government offered no evidence that he actually saw the images and that his viewing was knowing and wrongful.

According to the government's expert, the two cache files (01136627.jpg and 01136666.jpg) were created when a user visited a website sometime between 15 October 2012 and 18 April 2013. JA at 251. Although the user profile used was "Jeremiah" (*Id.*), that does not prove that A1C King was the person behind the keyboard. Considering the large timeframe (6 months) the website could have been accessed, and the fact that the computer was located in a home with several people, A1C is just one of several people who could have been on the computer. JA at 197, 459 (14:08:30, 16:20:40), 472, 479-81, 483. As it relates to the file in unallocated space, absolutely nothing is known about when or how it was created, or the user profile used. JA at 366. Thus, the government failed to put on sufficient evidence to show that A1C King was the user when (or if) the images were displayed.

Adding another layer to the mountain of speculation needed to advance the government's theory to this point, even if A1C King were the user, and even if the images were displayed on the computer screen, the government offered no evidence that A1C King actually saw any of

the three pictures. In fact, the government's own expert stated he found no evidence that A1C King saw any of the three images. JA at 364. "[I]t could have been that [A1C King] didn't see it because the cache created it." *Id*.

In order to conclude that A1C King did see any of the three images, the fact-finder would have to "turn[] abysmal ignorance into knowledge" solely by virtue of the files' existence. *Kuchinski*, 469 F.3d at 863. Such an assumption or inference would be patently unreasonable without "additional evidence of the defendant's knowledge . . . of the child pornographic images." *Moreland*, 665 F.3d at 152.

Even still, the fact that A1C King laid eyes on the image is not enough to sustain a conviction for viewing child pornography. His viewing must be knowing and wrongful. *See MCM*, pt. IV, ¶ 68b.b(1) and 68b.c.(9); *Navrestad*, 66 M.J. at 267. In this case, the government offered no evidence that A1C King knowingly viewed the three images. The government, and fact-finder, just assumed knowledge based upon the three files' existence. But just because a user sees an image on a website does not mean the user knows what it is that he or she is looking at. Even if A1C King saw the images in question, he may not

have looked at them long or hard enough to know they were even child pornography.

Wrongfulness too proves to be a significant challenge for the government because, in order to determine wrongfulness, the fact-finder must consider whether the images were unintentionally or inadvertently acquired and "the length of time the visual depiction was maintained." (*MCM*, pt. IV, ¶ 68b.c.(9)). But in this case, there is no evidence of how any of the three images were acquired or low long they were viewed (assuming they were viewed at all). *See* JA at 256, 346, 366.

Thus, there is insufficient evidence for a fact-finder to reasonably conclude that A1C King was the computer user, that he actually saw any of the three files, and that he knowingly and wrongfully viewed the images.

(3) The government offered no additional evidence which reasonably supported an inference that A1C King knowingly viewed any of the three files.

It is well established in several Federal Circuits and CCAs that the mere presence of child pornography on a computer is insufficient to impose criminal liability. *See*, *e.g.*, *Flyer*, 633 F.3d 911; *Dobbs*, 629 F.3d

1199; *Kamara*, 2015 CCA LEXIS 214; *Schempp*, 2016 CCA LEXIS 147. But in this case, that is exactly what the government did. Unlike the Courts of Appeals and CCA cases where knowledge and wrongfulness could be inferred based upon other independent evidence (*see*, *e.g.*, *Romm*, 455 F.3d 990; *Yohe*, 2015 CCA LEXIS 380), in this case there was no such corroborating evidence.

First, unlike *Romm* and *Weiss*, where the accused attempted to delete the child pornography to hide it from law enforcement, there was no evidence whatsoever that A1C Kind attempted to delete the three files. JA at 339-40, 368, 472. In fact, the government's expert testified that A1C King may not have known the files even existed (JA at 364, 366) and he "did not see any indication" (JA at 372) that A1C King had the knowledge or tools to even access the files.

Second, unlike *Yohe* or *Sanchez*, where the government could prove that the accused watched the child pornography or intentionally forwarded it on to another person, here there was no evidence that A1C King saw or manipulated any of the three files. On the contrary, the government's expert found "[t]here's no indication of" A1C King attempting to remove or otherwise access any of the three files. JA at

339-40; *see also* JA at 368. All three files were basically undisturbed. JA at 340. Furthermore, "[n]o webmail or email artifacts were found that indicate any attempts to produce, distribute child pornography, or arrange a sexual encounter with a minor." JA at 471.

Third, unlike *Yohe*, here there was no connection between the search terms the expert found and the three images. *See* JA at 400. In *Yohe*, the CCA upheld the accused's conviction for possessing child pornography because the government was able to establish a direct connection between recovered search terms and the child pornography found in unallocated space.[11] 2015 CCA LEXIS 380 at *3-*4. Not only was such a link lacking in this case, but it could not possibly exist. This is because the search terms recovered were entered between September and November 2013 (JA at 485), which is after the two cache files were created (between October 2012 and April 2013) (JA at 479, 485).

Finally, the government did not offer evidence which established that A1C King even had a general predisposition to view child pornography. In fact, the evidence indicated the opposite. Despite

[11] Also critical to the CCA's decision was the fact that the accused selected the videos for download and watched them while they downloaded. 2015 CCA LEXIS 380 at *3-*4

reviewing 34 devices, the government was not able to show that A1C King visited a single known child pornography website (JA at 471), possessed any known child pornography (*id.*), or attempted to produce or distribute any child pornography (*id.*). Even the government's expert was unable to tie the search terms to any images on the 34 devices. *See* JA at 485.

Had A1C King been looking for child pornography, the government's expert would have found something to back up that theory. Instead, the government's case centered solely on three files about which A1C King neither knew nor could access. Far from being reasonable, it was wholly unreasonable for the fact-finder to simply infer knowing viewing and wrongfulness. What the evidence established, at most, is that A1C King (or some other user) visited a webpage had an image of child pornography on it and that image was automatically cached. *See* JA at 399-400.

The government's theory was wholly unreasonable because it would require the fact-finder to believe A1C King sought out and viewed the child pornography, yet somehow left no trace. This theory is

made all the more unreasonable given A1C King's utter lack of computer knowledge and forensic tools.

Thus, this Court should find that there was insufficient corroborating evidence for a reasonable fact-finder to rely upon to find that A1C King knowingly and wrongfully viewed the three images he stands convicted of viewing.

A1C King's Conviction for Attempting to View Child Pornography is Legally Insufficient

A1C King's convictions for viewing (Charge III, Specification 2) and attempting to view (Charge I, Specification 1) child pornography are interconnected because the government used the search terms from the attempt offense to bolster their case for the images charged in the viewing offense and *vice versa*. Because A1C King's conviction for viewing child is legally insufficient, so too is his conviction for attempting to view child pornography. Based on the evidence adduced at trial, no reasonable fact-finder could have found that A1C King: (1) did a certain overt act; (2) the act was done with the specific intent to view child pornography; (3) the act amounted to more than mere preparation; and (4) the act apparently tended to effect the commission

of the intended offense of viewing child pornography. *See MCM*, pt. IV, ¶ 4.b.

First, there is insufficient evidence for the fact-finder to reasonably find A1C King was the person who entered the search terms. The most the government's expert could testify to was that the searches were all conducted between September and November 2013. JA at 485. The government offered no direct evidence to show A1C King was the person who entered the charged search terms. Instead, the government inferred that A1C King was the user since he admitted to searching for pornography.[12] *See* JA at 415. Without some supporting evidence, which was absent in this case, this inference was unreasonable. *See Moreland*, 665 F. 3d at 154 ("Where a defendant shares custody and control of the computer with other persons and the prosecution has not produced further evidence of knowledge of and

[12] The only search terms even potentially related to child pornography or child erotica that A1C King admitted to entering were "little girl" and "dany camy." JA at 459 (14:28:00, 15:33:45). A1C King only searched for "dany camy" once or twice and did not know what it meant. *Id*. He searched for it because he saw it was associated with a picture he found. *Id*. A1C King also searched for "little girl" but it was mainly while he was looking for anime pictures and the only thing that came up as a result of the search was pictures of babies and clothed children. *Id*. at 14:39:00. A1C King never saw, or attempted to find, pornographic images of real children as a result of these searches. JA at 459.

access to the images, we must conclude that the proof of constructive possession is deficient.")

Second, assuming *arguendo* that A1C King was the user who entered the search terms, the evidence does not reasonably support the conclusion that he specifically intended to view child pornography. The fact that the search terms could return results for child pornography does not mean the user intended to view child pornography. *See United States v. Paris*, No. 201200301, 2013 CCA LEXIS 575 (N-M. Ct. Crim. App. July 30, 2013) (unpub. op.) ("we are not persuaded by the Government's argument that the appellant's Internet search terms in conjunction with his obvious interest in images of nude children is sufficient to prove that he specifically intended to access websites containing child pornography"). As the government's expert testified, it is possible that a user who likes anime (like A1C King) could be looking for cartoons but then real images of child pornography could be returned. JA at 399-400. In fact, "thousands of photos" of anime pornography and real pornography were discovered on the devices seized in this case– all of which is lawful to view and possess. JA at 139, 186. Finally, despite reviewing 34 devices, the government was

not able to show that A1C King visited a single known child pornography website (JA at 471), possessed any known child pornography (*id.*), or attempted to produce or distribute any child pornography (*id.*). Rather than overcoming the high burden of proof, the government's evidence clearly demonstrated there was no specific intent to view child pornography. The government's expert was even unable to tie the search terms to any images on the 34 devices. *See* JA at 485. Thus, no fact-finder could have reasonably found that A1C King specifically intended to view child pornography.

Third, even if A1C King was the user who entered the search terms, and even if he specifically intended to view child pornography, searching for those terms did not amount to more than preparation. Entering a search term into an internet search engine (such as Google or Bing) generally (by default) returns a list of links to websites.[13] JA at 329. But links to websites are not child pornography. In order to actually view child pornography, the user has to take additional action and click on the link to open up the webpage. As this Court noted in

[13] Although it is possible to do an image search [JA at 329], the government offered no evidence that the search terms in this case were entered as part of an image search instead of the default website search.

Navrestad, a hyperlink to a website is akin to an address. *See* 66 M.J. at 267-68. Thus, entering search terms into a search engine is merely a preparatory act because it only provides the virtual address where the criminal act can be completed. To amount to an attempt, the user would have to attempt to access that virtual address. But in this case, there was no evidence the user ever attempted to visit a child pornography website, and in fact, the evidence demonstrated the opposite. *See* JA at 471. Thus, no reasonable fact-finder could have found that the search terms amounted to anything more than mere preparation.

Fourth, even if A1C King was the user who entered the search terms specifically intending to view child pornography, and even if that act was more than mere preparation, the only reasonable conclusion is that A1C King voluntarily abandoned any alleged attempt. If A1C King was literally just a click away from the child pornography he allegedly sought, then there is no reasonable explanation for why he would not go ahead and click the link to view the image other than that he voluntarily abandoned the attempt. There is no evidence whatsoever that A1C King's supposed attempt was frustrated by law enforcement, a

coworker, or anybody else. Thus, no reasonable fact-finder could have concluded anything other than that A1C King voluntarily abandoned any alleged attempt to view child pornography.

Conclusion

This Court should adopt the rationale pronounced by several of the Federal Courts of Appeals and the CCAs regarding possession of child pornography (*i.e.* evidence of storage of child pornography images in the hard drive of a defendant's computer, without more, is insufficient to sustain a conviction for knowing possession of child pornography; the government must present additional evidence of the defendant's knowledge, access, and control of the child pornographic images) and apply that rationale to the offense of viewing child pornography. Such a holding would dictate that, in cases such as the instant case, the mere existence of child pornographic files on a computer would be insufficient to establish knowing viewing unless the government presented additional evidence which established the accused actually saw the images and his viewing was knowing and wrongful. Applying that holding to the facts of A1C King's case, the conviction is legally insufficient because the government did not offer

such additional evidence.

WHEREFORE, this Court should set aside and dismiss the findings of guilty to Charge I, Specification 1, and Charge III, Specification 2, and, order a rehearing on the sentence.

Respectfully Submitted,

DUSTIN J. WEISMAN, Capt, USAF
Appellate Defense Counsel
U.S.C.A.A.F. Bar No. 35942
Air Force Appellate Defense Division
1500 W Perimeter Road, Suite 1100
JB Andrews, MD 20762
Office: (240) 612-4770
dustin.j.weisman.mil@mail.mil

Counsel for Appellant

CERTIFICATE OF FILING AND SERVICE

I certify I electronically filed a copy of the foregoing with the Clerk of Court on August 30, 2018 and that a copy was served via electronic mail on the Air Force Appellate Government Division on August 30, 2018.

Respectfully Submitted,

DUSTIN J. WEISMAN, Capt, USAF
Appellate Defense Counsel
U.S.C.A.A.F. Bar No. 35942
Air Force Appellate Defense Division
1500 W Perimeter Road, Suite 1100
JB Andrews, MD 20762
Office: (240) 612-4770
dustin.j.weisman.mil@mail.mil

CERTIFICATE OF COMPLIANCE WITH RULE 24(d)

This Brief complies with the type-volume limitation of Rule 24(c) because this Brief contains 9,380 words. Additionally, this Brief complies with the typeface and type style requirements of Rule 37.

DUSTIN J. WEISMAN, Capt, USAF
Appellate Defense Counsel
U.S.C.A.A.F. Bar No. 35942
Air Force Appellate Defense Division
1500 W Perimeter Road, Suite 1100
JB Andrews, MD 20762
Office: (240) 612-4770
dustin.j.weisman.mil@mail.mil

Dated: August 30, 2018