UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES
Appellee

v.

Jeremiah L. KING, Airman First Class
United States Air Force, Appellant

No. 18-0288
Crim. App. No. 39055

Argued November 6, 2018—Decided January 4, 2019

Military Judge: L. Martin Powell

For Appellant: *Captain Dustin J. Weisman* (argued).

For Appellee: *Captain Zachary T. West* (argued); *Colonel Julie L. Pitvorec*, *Lieutenant Colonel Joseph Kubler*, and *Mary Ellen Payne*, Esq. (on brief).

Chief Judge STUCKY delivered the opinion of the Court, in which Judges RYAN, OHLSON, SPARKS, and MAGGS, joined.

Chief Judge STUCKY delivered the opinion of the Court.

In addition to other offenses, Appellant was found guilty of knowingly and wrongfully viewing three specific images of child pornography that were found in his computer's unallocated space and browser cache. We granted review to determine whether the evidence supporting his conviction for viewing child pornography was legally sufficient.[1] Given the very low threshold required to sustain a conviction for legal sufficiency, we answer that question in the affirmative.

I. Procedural History

A military judge sitting alone as a general court-martial convicted Appellant, contrary to his pleas, of one specifica-

[1] In his brief, Appellant argues that the evidence supporting his conviction for attempting to view child pornography suffers the same infirmity. However, this Court only granted review in the context of Appellant's guilty findings for *actually* viewing child pornography. As such, Appellant's challenges to his attempted viewing conviction are outside the scope of the granted issue.

tion of attempting to view child pornography, one specification of violating a lawful general regulation, and one specification of viewing child pornography, in violation of Articles 80, 92, and 134, Uniform Code of Military Justice (UCMJ), 10 U.S.C. §§ 880, 892, 934 (2012). For his offenses, the military judge sentenced Appellant to a dishonorable discharge, confinement for nine months, and reduction to the lowest enlisted grade. The convening authority approved the sentence, and the United States Air Force Court of Criminal Appeals (CCA) affirmed. *United States v. King*, No. ACM 39055, 2017 CCA LEXIS 501, at *1, 2017 WL 3297198, at *1 (A.F. Ct. Crim. App. July 26, 2017) (unpublished).

II. Background

Photobucket, an image-hosting website, flagged eight images of suspected child pornography that an individual with a username that included "jeremiahking" and an email address that included "jeremiah.king" had uploaded to his account using an Air Force Internet Protocol (IP) address. Photobucket sent those images to the National Center for Missing and Exploited Children (NCMEC). Through the IP address, NCMEC traced the source to a government computer at Eielson Air Force Base, where Air Force Office of Special Investigations (AFOSI) agents linked the "jeremiah.king" email address to Appellant's official Air Force email address.

Soon thereafter, Special Agent (SA) Benito Rodriguez interviewed Appellant. Appellant told him he would go onto Photobucket while at work, search for images he liked using terms such as "dany camy" and "preteen girls," save those images to his Photobucket user profile, and then go home and download them. Although he initially denied any wrongdoing, Appellant eventually admitted he looked at images of underage girls in nude poses. When pressed, he estimated that the girls he viewed were between twelve to thirteen years old. He claimed that he "was a little bit thrilled" by the images, and eventually admitted that he had masturbated to photos he found of young girls.

Following the interview, AFOSI agents obtained a search warrant, seized several media devices from Appellant's workstation and residence, and forwarded them to the De-

fense Computer Forensics Laboratory (DCFL). DCFL conducted a forensic data extraction and created a mirror-image hard drive of the source media which they sent back to AFOSI for review. The drive contained thousands of offensive photos. SA Rodriguez reviewed that digital copy, and, after consulting with prosecutors, helped select images for charging. DCFL then conducted a "deep dive" forensic analysis on those photos.

Based on the evidence derived from this investigation, Appellant was charged with attempting to view child pornography, violating a lawful general regulation, possessing child pornography, viewing child pornography, and communicating indecent language. After a trial on the merits, Appellant was convicted, in relevant part, of knowingly and wrongfully viewing three specific images: 01136627, 01136666, and 01173367.

All three images were found on Appellant's home desktop computer. Images 01136627 and 01136666 were found in a Google Chrome cache, while Image 01173367 was found in unallocated space. None of the images was found in logical space on Appellant's computer.

The Government brought in a computer forensic expert from DCFL, Bryce Blair, to explain the significance of the files' locations. Mr. Blair conducted the examination in Appellant's case and prepared a report on his findings. He testified that a computer has both physical and logical space. Physical space is "all the space that's available on the hard drive itself" while "logical space is space that's available to be written to; it's the space that you have access to." When something exists in logical space, that could either mean someone intentionally saved something, or that someone viewed something on the internet but did not intentionally save it.

In contrast, a user would not have access to unallocated space, which is "space that's not currently being used." Mr. Blair testified that if a file were present in unallocated space, its presence there would indicate that that particular file had once existed on the computer in logical space but had been deleted at some point. He testified that unallocated space may "contain files that previously existed, deleted

files, things like that." For images found in unallocated space, he could not determine where they came from or when the images were created, but noted that it was possible they came from Photobucket. He specifically noted that Image 01173367, which was found in unallocated space, existed in logical space at one time but was later deleted. He further testified that two duplicates of Image 01173367 were also found in unallocated space, meaning that the image had existed in logical space more than once.

Mr. Blair also explained how an internet cache works. He noted that "[i]nternet cache is used by the web browsers to ultimately reduce the time that it would take a user to get to a specific webpage again." As an automatic function that stores files locally to provide a faster loading time, it is completely outside a user's control. It is possible for a user to run a search query that returns unintended results, and for such unintended images to be cached to the computer without the user's knowledge. A cache may save pictures or whole webpages, and the length of time the captured data is retained is dependent on the web browser used.

Google Chrome has a built-in cache, which "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." Google Chrome's cache could "potentially capture images that are not on the user screen at that specific time."

DCFL's "deep dive" laboratory report noted that 01136627 and 01136666 were found in a Google Chrome cache within the user account "jeremiah." The report noted that "[t]he existence of these files within [certain] files suggest that at one time the files were viewed" and that they were then "automatically cached into their respective Chrome default cache folders." Mr. Blair agreed that Appellant may have seen the images, and testified that someone on Appellant's computer had navigated to a website containing these images.

Mr. Blair testified that there was no way to know if Appellant actually accessed the cached images. All he could tell was that Appellant "accessed a website at one time that resulted in th[ese] image[s] automatically being cached to his

system. There is no artifact[] that would show whether the user later accessed th[ose] file[s] ….” When asked if he saw “any indication” that Appellant knew the images were being saved to his computer or that Appellant later accessed the saved images, he responded in the negative. Mr. Blair further noted that there was no way of knowing from any forensic determination whether a user actually saw any of the charged images. He confirmed that while Appellant went to a website with the charged photos on it, he may not have seen the specific images as they could have been caching offscreen. Mr. Blair could, however, confirm that Appellant searched for several terms indicative of child pornography, including “skimpy preteen,” “sexy little girls,” and “Loli porn.”

III. Law and Discussion

We review questions of legal sufficiency de novo. *United States v. Kearns*, 73 M.J. 177, 180 (C.A.A.F. 2014). “ ‘The test for legal sufficiency is whether, after viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt.’ ” ‘*United States v. Gutierrez*, 73 M.J. 172, 175 (C.A.A.F. 2014) (quoting *United States v. Bennitt*, 72 M.J. 266, 268 (C.A.A.F. 2013)). “This legal sufficiency assessment ‘draw[s] every reasonable inference from the evidence of record in favor of the prosecution.’ ” *United States v. Robinson*, 77 M.J. 294, 298 (C.A.A.F. 2018) (alteration in original) (quoting *United States v. Plant*, 74 M.J. 297, 301 (C.A.A.F. 2015)). As such, “[t]he standard for legal sufficiency involves a very low threshold to sustain a conviction.” *United States v. Navrestad*, 66 M.J. 262, 269 (C.A.A.F. 2008) (Effron, C.J., joined by Stucky, J., dissenting). “The criterion thus impinges upon ‘jury’ discretion only to the extent necessary to guarantee the fundamental protection of due process of law.” *Jackson v. Virginia*, 443 U.S. 307, 319 (1979).

In order to convict an accused for viewing child pornography under Article 134, UCMJ, the prosecution must prove: (1) that the accused knowingly and wrongfully viewed child pornography; and (2) that under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring

discredit upon the armed forces. *Manual for Courts-Martial, United States* pt. IV, ¶ 68b.b.(1) (2012 ed.) (*MCM*).

In determining whether *any* rational trier of fact could have determined that the evidence at trial established guilt beyond a reasonable doubt, we are mindful that the term "reasonable doubt" does not mean that the evidence must be free from any conflict or that the trier of fact may not draw reasonable inferences from the evidence presented. *See United States v. Oliver*, 70 M.J. 64, 68 (C.A.A.F. 2011) (recognizing that the standard for legal sufficiency " 'gives full play to the responsibility of the trier of fact fairly to resolve conflicts in the testimony, to weigh the evidence, and to draw reasonable inferences from basic facts to ultimate facts' " (quoting *Jackson*, 443 U.S. at 319)). Moreover, this Court has long recognized that the government is free to meet its burden of proof with circumstantial evidence. *See Kearns*, 73 M.J. at 182 (noting that the government may prove intent via circumstantial evidence); *United States v. Young*, 64 M.J. 404, 407 (C.A.A.F. 2007) (relying on "evidence in the record indicating, or giving rise to an inference of," drug possession and distribution to uphold a conviction).

We recognize that the ability to rely on circumstantial evidence is especially important in cases, such as here, where the offense is normally committed in private. As the Government conceded at oral argument, direct evidence of the offense of viewing child pornography will be rare because the offense is usually committed in private. As a result, the government often will have to rely on circumstantial evidence in attempting to prove the offense.

Here, the Government presented a circumstantially strong case that Appellant had sought and viewed child pornography. Appellant password-protected his electronic devices, including his computers, and a search of his home desktop computer revealed thousands of offensive photos. Appellant searched for images in Google and Bing using terms that are indicative of child pornography, and Appellant freely admitted he viewed "thrilling" images of nude children.

Furthermore, while the forensics failed to conclusively determine that Appellant actually saw the three charged

images, they still gave rise to an inference that Appellant viewed the photos. For example, not only did Mr. Blair testify that someone on Appellant's computer visited a website containing the cached images, but the cached images were found on Appellant's password-protected home computer within the user account "jeremiah." Furthermore, the DCFL laboratory report explicitly noted that "[t]he existence of [Images 01136627 and 01136666] within the … files *suggest that at one time the files were viewed*." (Emphasis added.) Similarly, Mr. Blair testified that although Image 01173367 was found in unallocated space on Appellant's computer, it existed in logical space at one time and could have originated from Photobucket. Finally, the two duplicates of Image 01173367, while also found in unallocated space, permit the inference that Appellant visited a website containing child pornography on multiple occasions with an awareness of its contents from prior visits.

Relying on this evidence, and drawing all inferences in favor of the prosecution, a reasonable factfinder could have reached the conclusion that Appellant knowingly viewed the three charged files.[2]

In reaching this conclusion, we necessarily reject Appellant's attempts to cast the lack of conclusive forensic evidence as a fatal flaw. As support for his position, Appellant points to the *MCM*'s explanation of "wrongfulness," which counsels us to consider whether the images were unintentionally or inadvertently acquired, an analysis which takes into consideration "the method by which the visual depiction was acquired [and] the length of time the visual depiction was maintained." *MCM* pt. IV, ¶ 68b.c.(9).

While we concede that evidence found in an area of the computer with more indicia of user control (e.g., a user-created folder) would carry more weight than evidence found

[2] This Court recognizes that the quantity and character of the information that is ascertainable from files located in unallocated space is different from the information that is ascertainable from cache files. These distinctions may prove important in future cases. However, we are satisfied that in this case the record is legally sufficient to support Appellant's conviction related to Image 01173367.

in a cache or in unallocated space, we, like the United States Court of Appeals for the Eleventh Circuit, believe that "[e]vidence that a person has sought out—searched for—child pornography on the internet and has a computer containing child pornography images—whether in the hard drive, cache, or unallocated space—can count as circumstantial evidence that a person has 'knowingly receive[d]' [or, in this case, viewed] child pornography." *United States v. Pruitt*, 638 F.3d 763, 766 (11th Cir. 2011) (second alteration in original).[3] What weight the factfinder ascribes to that evidence is for the factfinder alone to determine. *See Oliver*, 70 M.J. at 68 (recognizing that the trier of fact bears the responsibility to weigh the evidence).

We similarly decline Appellant's invitation to apply our logic from *Navrestad*, 66 M.J. 262, a case concerning the distribution and possession of child pornography, to the offense of viewing child pornography. In *Navrestad*, this Court held that using a public computer to view images of child pornography in a Yahoo! Briefcase was legally insufficient to constitute possession of child pornography, as there was no indication the accused exercised the required dominion or control over the contraband images. *Id.* at 267. In reaching this conclusion, this Court noted that the appellant "could not access the computer's hard drive where the Briefcase images were automatically saved" and that there was no evidence the appellant even knew the images were being saved in the first place. *Id.* at 267–68.

The situation here is different. Possession differs in material ways from mere viewing, and here, unlike in *Navrestad*, the Government was not required to prove dominion or control. As such, the presence of the charged images in inaccessible space takes on less significance. While an accused's inability to access data may prove a fatal flaw in a possession case, it does not similarly cripple a viewing

[3] We note that the Government conceded at oral argument that the mere presence of child pornography on an accused's computer—without additional circumstantial evidence of the kind present in this case—would generally present "a far harder case" due to the "lack of surrounding circumstances indicating an intent to pursue [such] material."

charge, which only requires that, at some point, the accused knowingly and wrongfully viewed the image. As such, Appellant's appeal to *Navrestad* and other possession cases is unavailing.

In sum, we trust that a reasonable person could have "resolve[d] conflicts in the testimony, … weigh[ed] the evidence, … [drew] reasonable inferences," and ultimately determined that the evidence established Appellant's guilt beyond a reasonable doubt. *Oliver*, 70 M.J. at 68. As such, under the facts of this case, we hold that the evidence was legally sufficient.

IV. Judgment

The judgment of the United States Air Force Court of Criminal Appeals is affirmed.