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

Before
F.D. MITCHELL, J.A. FISCHER, M.K. JAMISON
Appellate Military Judges

UNITED STATES OF AMERICA

v.

SHANE A. NICHLOS
FIRECONTROLMAN SECOND CLASS (E-5), U.S. NAVY

NMCCA 201300321
GENERAL COURT-MARTIAL

Sentence Adjudged: 17 April 2013.
Military Judge: CDR John A. Maksym, JAGC, USN.
Convening Authority: Commander, U.S. Naval Forces Japan, Yokosuka, Japan.
Staff Judge Advocate's Recommendation: LCDR Maryann M. Stampfli, JAGC, USN.
For Appellant: Maj John J. Stephens, USMC.
For Appellee: Maj Paul M. Ervasti, USMC; Capt Matthew M. Harris, USMC.

18 September 2014

OPINION OF THE COURT

THIS OPINION DOES NOT SERVE AS BINDING PRECEDENT, BUT MAY BE CITED AS PERSUASIVE AUTHORITY UNDER NMCCA RULE OF PRACTICE AND PROCEDURE 18.2.

JAMISON, Judge:

A general court-martial composed of officer and enlisted members convicted the appellant, contrary to his pleas, of two specifications of knowingly possessing child pornography in violation of Article 134, Uniform Code of Military Justice, 10 U.S.C. § 934. The members sentenced the appellant to reduction to pay grade E-1, confinement for a period of six months, and a

Judge Jamison participated in the decision of this case prior to detaching from the court.

bad-conduct discharge. The convening authority (CA) approved the adjudged sentence.

The appellant alleges four assignments of error: (1) that the military judge abused his discretion in failing to suppress evidence obtained from the appellant's portable hard drive -- as well as all derivative evidence -- based on an unconstitutional seizure; (2) that his conviction for knowing possession of child pornography is legally and factually insufficient; (3) that his conviction for knowing possession of child pornography in Specification 2 is legally and factually insufficient because the digital images that served as the basis for his conviction do not meet the statutory definition of child pornography; and, (4) that the military judge committed plain error by failing to define the term "lascivious" in his instructions to the members.

After careful consideration of the record, the pleadings of the parties, and the excellent oral argument by both parties,[1] we find merit in part of the appellant's second assignment of error and conclude that the evidence is legally insufficient to support a conviction for knowing possession of child pornography under Specification 1 of the Charge. Thus, we will set aside the finding of guilty to Specification 1 and dismiss that specification in our decretal paragraph. Arts. 59(a) and 66(c), UCMJ.

I. Background

The appellant was stationed at U.S. Fleet Activities Sasebo, Japan, aboard USS ESSEX (LHD 2). Following his promotion, the appellant was required to find off-ship living accommodations. He secured a lease at an apartment building. While waiting for his lease to start, he stayed with a friend, Fire Controlman Second Class (FC2) SW. The appellant was given a spare bedroom in which to sleep and store his personal belongings. Other petty officers also stayed at FC2 SW's apartment. The apartment had a common area that was used as a "crash pad" and "an awful lot of people" would use the apartment as a place to "hang out." Record at 92.

Intelligence Specialist Third Class (IT3) MD, a good friend of FC2 SW, also stored personal belongings at FC2 SW's apartment. On Thursday, 12 May 2011, IT3 MD picked up his laptop computer, a computer game, and several portable computer hard drives from FC2 SW's apartment. This gear had been stored

[1] We granted and heard oral argument on the appellant's first assigned error.

in the common area of the apartment. One of the hard drives that he believed was his and took with him was made by Western Digital. He brought his laptop, the portable hard drives, and other electronic media to his new apartment.

A day or so later, IT3 MD wanted to watch a movie. Knowing that he had movies stored on his Western Digital hard drive, he accessed it and immediately realized it was not his hard drive, because he saw approximately 50 thumbnail images of young nude girls. He specifically recollected viewing an image of several young nude girls arranged in a cheerleader-type pyramid. Disturbed by the images he saw and initially thinking that he had inadvertently grabbed a portable hard drive belonging to FC2 SW, his good friend, IT3 MD accessed the root directory and ascertained that the hard drive belonged to the appellant.

The following Monday, still disturbed by the images he had seen, IT3 MD sought guidance from the ship's legalman chief and was advised to speak with the ship's security department. After informing security department personnel that he believed he had a portable hard drive with suspected child pornography, IT3 MD was told to retrieve the hard drive and bring it back to security department personnel.

Security department personnel contacted the Naval Criminal Investigative Service (NCIS) regarding IT3 MD's allegations and then turned the portable hard drive over to the NCIS. Special Agent LG received the Western Digital hard drive at approximately 1405 on Monday, 16 May 2011. At approximately 1430, IT3 MD signed a written sworn statement for Special Agent JP, who was working the case with Special Agent LG. *See* Appellate Exhibit IX.

At approximately 1730 that same day, NCIS agents interviewed the appellant. During that interview, the appellant gave consent to search his workspace aboard ESSEX, his living space at FC2 SW's apartment, and all his electronic media, to include his iPhone. He accompanied the NCIS agents to FC2 SW's apartment and cooperated fully throughout the process.

In addition to the Western Digital hard drive, NCIS agents seized the appellant's Alienware laptop and iPhone, along with other electronic media. The appellant's electronic media items were sent to the Defense Computer Forensic Laboratory (DCFL) for forensic analysis. Forensic analysis revealed video files and digital images of child pornography on the appellant's laptop. It also revealed digital images of child pornography on the

appellant's portable hard drive. Additional facts necessary for the resolution of particular assignments of error are included below.

II. Suppression of the Appellant's Portable Hard Drive

In his first assignment of error, the appellant argues that the military judge abused his discretion by failing to suppress the evidence obtained from the appellant's portable hard drive and all derivative evidence. Specifically, he argues that the military judge erred by relying on the inevitable discovery exception to the exclusionary rule in concluding that the evidence was admissible. The appellant argues that the inevitable discovery exception is not applicable under these facts because at the time of the seizure, the Government was not actively pursuing a case that would have inevitably led to the discovery of the evidence. Appellant's Brief of 21 Jan 2014 at 25. We disagree.

We review a military judge's denial of a suppression motion under an abuse of discretion standard and "consider the evidence 'in the light most favorable to the' prevailing party." *United States v. Rodriguez*, 60 M.J. 239, 246 (C.A.A.F. 2004) (quoting *United States v. Reister*, 44 M.J. 409, 413 (C.A.A.F. 1996)). We review the military judge's "factfinding under the clearly erroneous standard and [his] conclusions of law under the *de novo* standard." *United States v. Ayala*, 43 M.J. 296, 298 (C.A.A.F. 1995) (citations omitted). We will find an abuse of discretion if the military judge's "findings of fact are clearly erroneous or his conclusions of law are incorrect." *Id.*

Because the military judge did not make explicit findings of fact and conclusions of law, we accord him less deference. We begin our analysis by exploring whether the appellant had a reasonable expectation of privacy in the portable hard drive that he had left in the common area of FC2 SW's apartment.

1. *Reasonable Expectation of Privacy*

The Fourth Amendment protects the "persons, houses, papers, and effects" of individuals against unreasonable searches and seizures. U.S. CONST. amend. IV. "'Evidence obtained as a result of an unlawful search or seizure made by a person acting in a governmental capacity is inadmissible against an accused if: . . . The accused had a reasonable expectation of privacy in the person, place or property searched; the accused had a legitimate interest in the property or evidence seized when challenging a

seizure; or the accused would otherwise have grounds to object to the search or seizure under the Constitution of the United States as applied to members of the armed forces.'" *United States v. Salazar,* 44 M.J. 464, 466-67 (C.A.A.F. 1996) (quoting MILITARY RULE OF EVIDENCE 311(a), MANUAL FOR COURTS-MARTIAL, UNITED STATES (1995 ed.)).

To determine whether the appellant had a reasonable expectation of privacy in the contents of his portable hard drive, we apply "a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *United States v. Conklin*, 63 M.J. 333, 337 (C.A.A.F. 2006) (quoting *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)).

Despite the fact that the appellant had a bedroom at FC2 SW's apartment and stored his laptop there, he chose to leave his portable hard drive in an area where, by his own admission, "an awful lot of people" would "hang out" and access one another's electronic media. Record at 92. The hard drive was neither labeled nor password protected. It was also similar to other portable hard drives located in the common area, to include the hard drive belonging to IT3 MD as evidenced by the fact that he mistakenly took it. Additionally, the ease by which IT3 MD accessed the appellant's portable hard drive and its child pornography images is further evidence that the appellant did not have a reasonable expectation of privacy in this hard drive. *See United States v. Rader*, 65 M.J. 30, 34 (C.A.A.F. 2007) (stating that within the context of personal computers "courts examine whether the relevant files were password-protected or whether the defendant otherwise manifested an intention to restrict third-party access") (citation and internal quotation marks omitted)); *United States v. Barrows*, 481 F.3d 1246, 1249 (10th Cir. 2007) (holding that Barrows's "failure to password protect his computer, turn it off, or take any other steps to prevent third-party use" demonstrated a lack of subjective expectation of privacy).

Based on the facts of this case, we conclude that the appellant did not have a subjective expectation of privacy in his portable hard drive left in the common area of FC2 SW's apartment. Additionally, we conclude -- at least with regard to the various Sailors who had unfettered access to FC2 SW's apartment and common area -- that the appellant's expectation of privacy was not objectively reasonable.

In this case, the military judge appeared to conclude that at the time IT3 MD took the portable hard drive, the appellant had no expectation of privacy because he had left it in the common area. Record at 136. However, as the testimony and facts developed, the military judge appeared to conclude that once IT3 MD was directed to retrieve the appellant's hard drive, IT3 MD became a Government actor and this resulted in the appellant developing a reasonable expectation of privacy. *Id.* at 140. We disagree and hold that the appellant did not gain a reasonable expectation of privacy at the time IT3 MD was directed to deliver the hard drive to security personnel. We nonetheless continue our analysis, assuming *arguendo* that the appellant had a reasonable expectation of privacy in his hard drive and consider the appellant's argument that the seizure was unconstitutional and a violation of MIL. R. EVID. 316.

2. *Seizure of Portable Hard Drive*

A seizure is unlawful if it was conducted, instigated, or participated in by "[m]ilitary personnel or their agents and was in violation of the [United States] Constitution as applied to members of the armed forces." MIL. R. EVID 311(c)(1). Whether an individual is acting as a Government agent depends "'on the degree of the Government's participation in the private party's activities, a question that can only be resolved in light of all the circumstances.'" *United States v. Daniels,* 60 M.J. 69, 71 (C.A.A.F. 2004) (quoting *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 614-15 (1989)). More explicitly, there must be "clear indices of the Government's encouragement, endorsement, and participation . . . to implicate the Fourth Amendment." *Skinner,* 489 U.S. at 615-16.

The appellant correctly concedes that when IT3 MD initially accessed the appellant's hard drive, he did so as a private actor. Record at 128, 132. Accordingly, none of the appellant's constitutional or regulatory rights were violated at that point. *See United States v. Wicks*, 73 M.J. 93, 100 (C.A.A.F. 2014) (stating that it is "well-established" that "search and seizure rules do not apply to searches conducted by private parties") (citations omitted)).

The appellant instead argues that IT3 MD became a Government actor once he retrieved the portable hard drive and turned it over to the ship's security personnel at their request. The appellant further argues that, as a Government actor, IT3 MD performed an unlawful warrantless seizure of the hard drive as the appellant had a legitimate privacy and

possessory interest in the hard drive. Appellant's Brief at 24-25. We disagree.

The appellant premises his argument on the Government's concession at trial that IT3 MD became a Government actor and on the holding of the Court of Appeals for the Armed Forces (CAAF) in *Daniels*. *Id*. at 22-23. Our review of the record reveals that any concession by the Government came only after the military judge had ruled that IT3 MD had become a Government actor.[2] Record at 127-28.

As for the comparison to *Daniels*, we find the facts in that case clearly distinguishable. In *Daniels*, Seaman Apprentice (SA) V told his leading chief petty officer, Chief W, that the previous evening Daniels had held up a vial and told SA V that the vial contained cocaine. Daniels had then put the vial in the top drawer of his nightstand. Based on SA V's report, Chief W directed that he retrieve the vial. Within this context, it was Chief W's order that triggered SA V's seizure of the contraband from an area in which Daniels had a reasonable expectation of privacy.

Unlike *Daniels*, this case is not one in which contraband was seized following an order from a Government official; rather IT3 MD accessed the appellant's portable hard drive as a private actor and discovered what he believed to be contraband. At the time he reported his suspicions to security department personnel, IT3 MD had already independently collected the hard drive absent a request from Government officials to do so. The Government did not encourage, endorse, or participate in any of IT3 MD's actions and the ship's security department personnel only instructed IT3 MD to retrieve the hard drive from his apartment once he sought advice of what to do with an item that he believed contained contraband. Accordingly, we hold that the direction by the ship's security department personnel did not rise to the level of constituting "clear indices of Government encouragement, endorsement, and participation" in the challenged

---

[2] MJ: So, essentially what the Government is conceding here, to their credit, is that the Security Department say[s], "Go get this thing," right?
ATC: Yes, Your Honor.
MJ: All right.
ATC: And---
MJ: He's their agent.
ATC: Your Honor ---
MJ: He acts like an agent, he dressed like an agent, he's got the look of an agent. Guess what he is? An agent
Record at 127.

seizure.[3] *Daniels*, 60 M.J. at 71 (quoting *Skinner*, 489 U.S. at 615-16).

Assuming *arguendo* that IT3 MD did become an agent, we hold that the seizure was not unreasonable under these facts. First, it was reasonable for the ship's security personnel to direct IT3 MD to retrieve the hard drive from his apartment based on the fact that it contained suspected contraband. Second, it was temporary in nature and totaled no more than four hours before the appellant gave consent to its seizure and search.

The Fourth Amendment prohibits only "meaningful interference" with a person's possessory interests, not Government action that is reasonable under the circumstances. *See United States v. Place*, 462 U.S. 696, 706 (1983) (stating that "brief detentions of personal effects may be so minimally intrusive of Fourth Amendment interests that strong countervailing governmental interests will justify a seizure based only on specific articulable facts that the property contains contraband or evidence of a crime"); *United States v. Visser*, 40 M.J. 86, 90 (C.M.A. 1994) (holding a seven-day hold on Visser's military household goods shipment for purposes to obtain a civilian search warrant was reasonable Government action); *United States v. Garcia-Lopez*, 16 M.J. 229, 231 (C.M.A. 1983) (stating that "[l]aw enforcement authorities can properly take reasonable measures to assure that, until reasonable investigative steps can be completed, evidence is not destroyed, crime scenes are not disarranged, and suspects do not flee.") (quoting *United States v. Glaze*, 11 M.J. 176, 177 (C.M.A. 1981)) (additional citations omitted); MIL. R. EVID. 316 (d)(5) (authorizing "temporary detention of property on less than probable cause").

After careful consideration, we find that even assuming IT3 MD became a Government actor and seized the appellant's hard drive within the meaning of MIL. R. EVID. 316, the seizure was reasonable under the circumstances and did not violate the appellant's Fourth Amendment rights. We last address the military judge's ruling relying on the inevitable discovery exception to conclude that the evidence was admissible.

---

[3] During oral argument, the appellate defense counsel conceded that if IT3 MD would have brought the hard drive with him when he initially sought guidance from USS ESSEX personnel, there would have been no unconstitutional seizure. Based on the particular facts of this case, we do not find a legal distinction between the two situations because IT3 MD had already taken possession of the hard drive, examined it, and secured it in his apartment.

3. *Inevitable Discovery Exception to Exclusionary Rule*

In this case, the military judge apparently found that there had been an unreasonable seizure and that the appellant gained a reasonable expectation of privacy in his portable hard drive once IT3 MD became a Government actor. Finding a constitutional and regulatory violation of the appellant's rights, the military judge nevertheless ruled the evidence admissible based on the inevitable discovery exception to the exclusionary rule. Record at 147.

The appellant argues that the military judge abused his discretion because the inevitable discovery exception is not applicable under these facts. Appellant's Brief at 25. Citing various cases from our superior court that address the inevitable discovery exception, the appellant argues that there was no evidence that the Government was actively pursuing leads or evidence at the time IT3 MD was directed to retrieve the hard drive from his apartment. *Id.* We disagree.

Evidence obtained as a result of an unlawful seizure may be used when the evidence "would have been obtained even if such unlawful search or seizure had not been made." MIL. R. EVID. 311(b)(2). When routine procedures of a law enforcement agency would have discovered the same evidence, the inevitable discovery rule applies even in the absence of a prior or parallel investigation. *See United States v. Owens*, 51 M.J. 204, 210-11 (C.A.A.F. 1999). The inevitable discovery exception to the exclusionary rule exists to ensure that the Government is not placed in a worse position than it would have been had no law enforcement error taken place. *See Nix v. Williams*, 467 U.S. 431, 444 (1984) (holding that the Government must show by a preponderance of the evidence that Government agents would have inevitably discovered the evidence by legal means); *cf. Hudson v. Michigan*, 547 U.S. 586, 591 (2006) (stating that "[s]uppression of evidence, however, has always been our last resort, not our first impulse").

Once IT3 MD left the ship to retrieve the portable hard drive from his apartment, security department personnel contacted NCIS regarding IT3 MD's allegation. As a result, NCIS opened an investigation prior to having received the hard drive. Additionally, once IT3 MD returned with the hard drive, it was immediately turned over to Special Agent LG (at approximately 1400). At approximately 1430, IT3 MD provided a sworn statement to Special Agent JP. AE IX. No NCIS agent accessed the appellant's hard drive prior to interviewing either IT3 MD or

the appellant. Thus, there was no governmental search in this case until the appellant gave consent. Special Agent LG relied on information provided by IT3 MD as to how he obtained the hard drive, what he saw, and how he found out that it belonged to the appellant. Based only on the information he received from IT3 MD, Special Agent LG interviewed the appellant and requested his consent to search the hard drive and his other electronic media items.

Contrary to the appellant's argument, we find that under the facts of this case, the military judge did not abuse his discretion in applying the inevitable discovery exception to the regulatory exclusionary rule. MIL. R. EVID. 311(a)(2). The preponderance of the evidence establishes that once Special Agent LG was informed of IT3 MD's allegations that the appellant's portable hard drive contained suspected child pornography, which IT3 MD had discovered in his private capacity, NCIS began an investigation. Special Agent LG interviewed IT3 MD and about three hours later interviewed the appellant. But for the appellant's freely and voluntarily given consent, it is reasonable that NCIS would have requested a search authorization of the appellant's hard drive. In this regard, the appellant does not contend that IT3 MD's sworn statement was lacking in probable cause sufficient to secure a search authorization. In fact, he conceded this issue. Record at 132. We agree and find sufficient probable cause within IT3 MD's sworn statement that NCIS could and would have secured a search authorization.[4] MIL. R. EVID. 315; *see United States v. Bethea*, 61 M.J. 184, 187 (C.A.A.F. 2005) (stating that probable cause means that there is a "fair probability" that contraband "will be found in a particular place").

Accordingly, we find no error by the military judge in applying the inevitable discovery exception to the facts of this case.

III. Factual and Legal Sufficiency

In his second assignment of error, the appellant argues that his conviction for knowingly possessing child pornography is factually and legally insufficient. First, the appellant

[4] We note that Special Agent LG testified that he ultimately sought and received a search authorization subsequent to the appellant's Article 32, UCMJ, pretrial investigation. Record at 63. He sought a search authorization because he believed that the appellant may revoke his consent. *Id*.

argues that since the three charged video files from his Alienware laptop computer were found in unallocated space the evidence was insufficient to prove "knowing possession." Second, the appellant argues that because the digital images from his hard drive were found among nearly a thousand adult pornography images, this was insufficient to prove knowing possession. We address first the appellant's sufficiency argument with regard to the three video files found on his Alienware laptop (Specification 1) prior to moving to his sufficiency argument of the digital images recovered from his hard drive (Specification 2).

We review questions of legal and factual sufficiency *de novo*. *United States v. Winckelmann*, 70 M.J. 403, 406 (C.A.A.F. 2011). The test for legal sufficiency is whether any rational trier of fact could have found that the evidence met the essential elements of the charged offense, viewing the evidence in a light most favorable to the Government. *United States v. Turner*, 25 M.J. 324, 324 (C.M.A. 1987). The test for factual sufficiency is whether we are convinced of the appellant's guilt beyond a reasonable doubt, allowing for the fact that we did not personally observe the witnesses. *Id.* at 325.

The term "reasonable doubt" does not mean that the evidence must be free of any conflict. *United States v. Rankin*, 63 M.J. 552, 557 (N.M.Ct.Crim.App. 2006), *aff'd*, 64 M.J. 348 (C.A.A.F. 2007). When weighing the credibility of a witness, this court, like a fact-finder at trial, examines whether discrepancies in witness testimony resulted from an innocent mistake, including lapses in memory, or a deliberate lie. *United States. v. Goode*, 54 M.J. 836, 844 (N.M.Crim.Ct.App 2001). Additionally, the members may "believe one part of a witness's testimony and disbelieve another." *United States v. Harris*, 8 M.J. 52, 59 (C.M.A. 1979).

1. *Factual and Procedural Background*

Prior to conducting our sufficiency analysis, we need to recapitulate the factual and procedural background to frame the appellant's argument. While deceptively simple in appearance, the appellant's argument in combination with the Government's evidence and the military judge's variance instruction makes this a complicated issue requiring extensive contextual analysis. We begin with the Government's charging theory and move to the evidentiary posture of this largely circumstantial case.

The Government preferred three specifications alleging the appellant's knowing possession of child pornography on or about 16 May 2011:[5] three video files from the appellant's laptop (Specification 1); three digital images from the laptop (Specification 2); and, nine digital images from the appellant's portable hard drive (Specification 3). Following the presentation of the Government's case-in-chief, the appellant moved for a finding of not guilty under RULE FOR COURTS-MARTIAL 917, MANUAL FOR COURTS-MARTIAL, UNITED STATES (2012 ed.). Record at 1515. The appellant's argument was that the evidence was insufficient to prove knowing possession in that the video files and some of the digital images had been forensically retrieved from the unallocated space of the appellant's laptop and portable hard drive with no evidence as to when the files were created, accessed, or deleted.

The military judge partially agreed and acquitted the appellant of the three digital images that served as the basis for Specification 2. With regard to Specification 3, the military judge acquitted the appellant of seven digital images, which had been retrieved from the unallocated space on the appellant's portable hard drive.[6] Because only images 8 and 9 had been retrieved in allocated space, the military judge allowed the members to consider these two images and the members convicted the appellant of this specification.

With regard to Specification 1, the members asked several questions that required the court to reassemble. Following extensive deliberation, the members convicted the appellant of knowing possession of the three video files except for the words "16 May 2011" and substituting the words "3 March 2011."[7]

2. *Prosecution Theory and Evidence (Video Files)*

We first address Specification 1 and the three charged video files that were retrieved from unallocated space on the appellant's laptop. The appellant does not contest that the

[5] For reasons that will become apparent, the Government's decision to charge a date certain is critical to our analysis on the question of knowing possession.

[6] Following the motion for a finding of not guilty, original Specification 3 became Specification 2.

[7] As part of the instructions on findings, the military judge gave the members a variance instruction that the members could go back up to 150 days from the date alleged on the charge sheet. Record at 1774-75.

girl in the three video files is, in fact, a minor. Appellant's Brief at 7 n.26. Additionally, this minor is clearly involved in a sexual act and each video file is of the same minor girl.[8] The trial counsel played a fourth video file pursuant to MIL. R. EVID. 404(b) of the same minor girl. This movie clip had a superimposed annotation in the middle of the screen with the following: "Jenny 9yo all clips."[9] It was this linkage to "Jenny 9yo" that provided the strongest circumstantial evidence of the appellant's knowing possession of the three video files in unallocated space appearing to portray "Jenny 9yo."

The Government presented a circumstantially strong case that the appellant had, at some point, received, downloaded, and viewed child pornography videos. The Government called Ms. SH, a forensic expert with the Defense Computer Forensic Laboratory DCFL. In addition to her testimony, the Government relied on the forensic exploitation of the appellant's laptop, portable hard drive, and iPhone to present its case.

First, the Government offered Prosecution Exhibit 3, a DCFL forensic report of the appellant's iPhone. This exhibit contained three cookies revealing that on 24 December 2010, the appellant had used the Google search engine and searched for and accessed a website responsive to the appellant's search term: "9yo Jenny pics."[10]

---

[8] The charged video files depict a prepubescent girl, partially bound at her legs, performing oral sex on an adult male who is fondling her vaginal area. The files are twenty-one, twenty-six, and six seconds in length. *See* Prosecution Exhibit 1.

[9] The Government played this video file in its opening statement and the trial defense counsel subsequently stipulated that the video shown had the superimposed title "Jenny 9yo all clips." Record at 1438. As discussed *infra*, the three videos that form the basis of Specification 1 were not labeled.

[10] A cookie is a text file that is created when an individual uses e.g. the Google search engine. In this case, the appellant's iPhone contained three cookies that contained "9yo Jenny pics." *See* PE 3, Cookies 183, 366, and 374; Record at 1394-1400. One type of cookie is a UTMA cookie (# 183), which was placed on the appellant's iPhone when he visited the actual website. *Id.* at 1396. This cookie is updated with each subsequent visit and a UTMA cookie remains on the device for two years. *Id.* at 1397. The other type of cookie on the appellant's phone was a UTMZ cookie (# 366 and 374). This is a campaign cookie. This type of cookie is used to assist the web site to determine how the user accessed the web site, e.g. through Google or another type of search engine, because some search engines receive pay for facilitating digital searches. *Id.*

Second, the Government offered PE 4, a list of property files from LimeWire that contained the most recently downloaded files to the appellant's laptop.[11] These LimeWire property files were retrieved from unallocated space on the appellant's laptop; however, the search terms that the appellant entered and downloaded were highly indicative of child pornography and some of the downloaded files contained the unique naming convention "9yo Jenny" in various permutations. Because the LimeWire files were retrieved in unallocated space on the appellant's laptop, Ms. SH was not able to retrieve any digital files that matched the digital files from the LimeWire download.[12] Ms. SH testified that the file names in the LimeWire download were downloaded onto the appellant's laptop; however, because these files were retrieved from unallocated space, the only information attainable was the digital file names themselves.

Third, the Government offered PE 5, a list of the appellant's recently accessed video files. Ms. SH conducted a search of the appellant's laptop for the most recently viewed movie files in the .mov and .qt format.[13] Whenever a user accesses a movie or video file that contains the file extension .mov or .qt, a link file is automatically created by the program. Record at 1417. A link file creates a shortcut for the user and allows the user to "double-click" on that file to access and view that particular video file. Ms. SH testified that even if the underlying digital file is deleted, the link file still exists on the computer. Additionally, Ms. SH testified that although she was not able to find the underlying video files associated with the link files, she was able to testify that at some point in time, these files had been viewed.

---

[11] LimeWire is a file-sharing program that allows users to share files stored on their respective computers with other LimeWire users. *Arista Records LLC v. Lime Group LLC*, 715 F. Supp. 2d 481, 494 (S.D.N.Y 2010). When a LimeWire user wants to locate digital files or videos, the user enters "search criteria into the search function on LimeWire's interface." *Id.* LimeWire then searches the computers of the various users for files that match the search criteria and then the user downloads these files onto his or her computer. *Id.*

[12] The testimony of both the Government and the defense expert was that there appeared to be a mass download onto the appellant's laptop in 2009 using the LimeWire program and that at some point in 2009, the LimeWire program had been deleted. The 26 September 2009 date on PE 4 "indicates when LimeWire was last accessed. It does not indicate that's the date those files were downloaded." Record at 1506.

[13] Movie or video files that contain either the .mov or .qt file extension are for the software program QuickTime by Apple. Record at 1416-17.

Id. at 1418. Of the ten recently viewed files that contain the .mov extension, three of them include the title "9yo Jenny." PE 5.[14]

The Government's theory was that the appellant had an interest in child pornography and a particularly unusual interest in images or video files that contained "9yo Jenny," the same prepubescent girl depicted in the charged video files. Based on the evidence and expert testimony that the appellant had used his iPhone on 24 December 2010 to actively search for and access the website purportedly containing "9yo Jenny pics," this served as a circumstantial link to the charged video files of "9yo Jenny."

There is no question that the appellant possessed child pornography; the question is whether the appellant "knowingly possessed" child pornography *on* the charged date. Having concluded that the Government presented a circumstantially strong case that at some point in time while the appellant owned his laptop, he had received, downloaded, viewed, and knowingly possessed child pornography, we turn next to the Government charging decision. Although the Government's case as to knowing possession may have been circumstantially strong, the decision to charge "on or about 16 May 2011" became the Government's evidentiary Achilles heel.

3. *Unallocated Space and Knowing Possession (Video Files)*

Because of its charging decision, the Government was required to prove that the appellant "knowingly possess[ed]" the three charged video files (01864590.mpg; 01864588.mpg; and, 01864901.mpg) "on or about 16 May 2011." Accordingly, the critical issue we must now decide is not whether the appellant knowingly possessed these video files at any time from the date he acquired his computer until the date NCIS seized it. Instead, we must decide whether the appellant knowingly possessed the three charged video files retrieved from unallocated space on or about 16 May 2011. Based on binding precedent from the CAAF, we conclude that he did not. To support our conclusion, we first consider the technical aspects associated with unallocated space prior to considering whether a computer user can "possess" a digital file, either actually or constructively, if that file exists only in the unallocated space of a computer.

[14] The three link files with the .qt file extension also contains a reference to "9yo Jenny." That file is titled: 9yo dog full jenny mpg sucking, loli 11yo 20minute hard.qt. PE 5.

According to the Government's expert witness, Ms. SH, unallocated space is the location on the computer where files are stored after having been permanently deleted. When a user permanently deletes a digital file that file continues to exist on the computer; however, it exists in unallocated space until the file is overwritten. Once a digital file is in unallocated space, the metadata associated with that file is stripped away (e.g. its name, when it was accessed, when it was viewed, when it was created, or when it was downloaded). Record at 1391. Ms. SH's testimony is consistent with federal courts that have defined unallocated space. *See United States v. Hill*, 750 F.3d 982, 988 n.6 (8th Cir. 2014) ("Unallocated space is space on a hard drive that contains deleted data, *usually emptied from the operating system's trash or recycle bin folder*, that cannot be seen or accessed by the user without the use of forensic software") (quoting *United States v. Flyer*, 633 F.3d 911, 918 (9th Cir. 2011)); *United States v. Seiver*, 692 F.3d 774, 776 (7th Cir. 2012) (stating that when one deletes a file, that file goes into a "trash" folder; when one empties the "trash folder" the file has not left the computer because although the "trash folder is a wastepaper basket[,] it has no drainage pipe to the outside"; the file may be "recoverable by computer experts" unless it has been overwritten), *cert. denied sub nom Seiver v. United States*, 133 S. Ct. 915 (2013).[15]

The CAAF has defined what constitutes "knowing possession" for purposes of possession of child pornography. *See United States v. Navrestad*, 66 M.J. 262, 267 (C.A.A.F. 2008). To constitute "knowing possession" for purposes of child pornography, the CAAF imported the definition of possession from the President's definition of "possess" in Article 112a, UCMJ.[16]

---

[15] Digital files found in unallocated space or slack space have also been referred to as "orphan files" because "it is difficult or impossible to trace their origin or date of download." *United States v. Moreland*, 665 F.3d 137, 142 n.2 (5th Cir. 2011) (citing *United States v. Kain*, 589 F.3d 945, 948 (8th Cir. 2009) (stating that "[o]rphan files are files that were on the computer somewhere saved but were subsequently deleted, so the computer doesn't know exactly where they came from")).

[16] Following the presentation of the evidence, the military judge gave the following definition of "possession" to the members: "'Possessing' means exercising control of something. Possession may be direct physical custody like holding an item in one's hand or it may be constructive as in the case of a person who hides something in a locker or a car which the person may return to retrieve it. Possession must be knowing and conscious. Possession inherently includes the power or authority to preclude control by others. It is possible for more than one person to possess an item simultaneously, as when several people share control over an item." Record at 1758.

Id.; *see* MANUAL FOR COURTS-MARTIAL, UNITED STATES (2012 ed.), Part IV, ¶ 37c(2). Because Navrestad did not have actual possession or constructive possession of child pornography under that definition, the CAAF held that the evidence was legally insufficient. *Id.* at 268.

In this case, the Government presented no evidence that the appellant had the required forensic tools to retrieve digital files from the unallocated space of his computer. In fact, Ms. SH testified that once a digital file is in unallocated space, a user does not have the ability to access that digital file. Record at 1449. Because the appellant was unable to access any of the video files in unallocated space, he lacked the ability to exercise "dominion or control" over these files. *Navrestad*, 66 M.J. at 267; *see Flyer*, 633 F.3d at 919 (citing *Navrestad* and holding that evidence was legally insufficient to prove knowing possession on or about the date charged in the indictment); *see also United States v. Kuchinski*, 469 F.3d 853, 862 (9th Cir. 2006) (holding that in situation in which "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 those images. To do so turns abysmal ignorance into knowledge and a less than valetudinarian grasp into dominion and control"); *United States v. Moreland*, 665 F.3d 137, 154 (5th Cir. 2011) (holding that the evidence was legally insufficient to sustain conviction for possession of child pornography in which Government failed to prove dominion and control over the digital images and citing cases for the proposition that the evidence is legally insufficient to show constructive possession based solely on the fact that the accused possessed the computer, "without additional evidence of the [accused's] knowledge and dominion or control over the images").

Having defined "knowing possession" for purposes of child pornography as requiring the possession to be both "knowing and conscious," *Navrestad*, 66 M.J. at 267, we hold that the appellant did not "knowingly possess" any of the three charged videos on the date charged (16 May 2011).[17] Bound by *Navrestad*,

[17] Factually, this case is similar to *Flyer* in that all images of child pornography charged in Flyer's indictment had been retrieved from unallocated space. The *Flyer* court agreed with the general proposition that one way to exercise dominion and control over a digital file would be to delete that file; however, that alone was insufficient to prove knowing possession on the date indicated on the indictment. 633 F.3d at 919. Because the Government

we also conclude that the evidence was legally insufficient to prove constructive possession on the date charged. The CAAF has held that for the evidence to be legally sufficient on a constructive possession theory, a person must exercise "dominion or control" over the child pornography digital files.[18] *Id.* at 267. Based on the technical aspects associated with unallocated space, Ms. SH's testimony, and a lack of any evidence presented that the appellant was a sophisticated computer user in possession of the forensic tools necessary to retrieve digital files from unallocated space, we conclude that the evidence is legally insufficient to prove knowing possession on or about the charged date of 16 May 2011. We move next to evaluate the legal sufficiency of Specification 1 with regard to the 3 March 2011 date that the members substituted for the original date on the charge sheet.

4. *Members' Verdict*

Following the appellant's partially successful motion for a finding of not guilty under R.C.M. 917 with regard to proving "knowing possession" on the date reflected on the charge sheet, the Government requested a variance instruction. Record at 1708. The military judge was open to a variance instruction, but indicated that he would not go back two years (presumably to the 2009 LimeWire download). After some discussion, the military judge agreed to give the members a variance instruction that they could go back for up to 150 days from the date alleged on the charge sheet.[19] *Id.* at 1774-75. The 150-day variance supported the Government's theory that within this period, the appellant searched and accessed "9yo Jenny pics" based on his 24 December 2010 iPhone Google search and that this evidence

---

was unable to prove that on the date alleged in the indictment Flyer was able to access or retrieve any of the child pornography digital images, the evidence was legally insufficient.

[18] *But cf. United States v. Carpegna*, 2013 U.S. Dist. LEXIS 115002 at *14 (D. Mont. Aug. 14, 2013) (distinguishing Carpegna's acts of deleting contraband from the facts in *Navrestad* and *Flyer* based on the fact that Carpegna "knew enough about the presence of the images on the laptop to 'hit delete' after he was finished viewing them").

[19] "If you have any reasonable doubt relative to the time alleged on the charge sheet, 16 May 2011, but you are satisfied beyond any reasonable doubt that the offense was committed at a time that differs slightly from the exact date on 16 May 2011, you may make minor modifications in reaching your findings by what we call exceptions and substitutions, that is excepting or cutting out certain language in a specification or date, and substituting language or dates so long as the alteration of that date does not exceed more than 150 days prior to 16 May 2011." Record at 1774-75.

circumstantially proved constructive possession given the unique association with the "9yo Jenny" naming convention. PE 3.

Based on our review of the record, it is evident from the questions by the members during deliberation that the date on the charge sheet was a cause for concern. The members first asked the military judge whether Specification 1 required a specific time frame or whether they could remove the date "16 May 2011" entirely from Specification 1. AE CXXXV. The military judge responded by reiterating the 150-day variance instruction. Record at 1809. After further deliberation, the members asked the military judge to define the meaning of "on or about" and asked whether "on or about" in Specification 1 could encompass the time period from the date when the appellant reported to USS ESSEX until 16 May 2011. AE CXXXVI. In response, the military judge instructed the members that "on or about" means a short time period not to exceed 30 days and that any time period beyond 30 days would constitute variance. Record at 1815. Following additional deliberation, the members convicted the appellant by excepting the date "16 May 2011" and substituting the date "3 March 2011."

Having already concluded that the evidence was legally insufficient to convict the appellant for knowing possession on or about 16 May 2011, we must assess whether any evidence supports constructive possession of the video files on or about 3 March 2011. Based on our careful review of the record we conclude that it does not.

Because the 3 March 2011 date was not argued or emphasized by either party at trial, we are left to speculate how the members arrived at that particular date. Two possibilities emerge, one more likely than the other. The only evidence discussed on the record that references 3 March 2011 is within the context that this was the date the appellant password-protected or changed the password on his laptop. *Id.* at 1579. The more likely scenario is the fact that 3 March 2011 is referenced in the document containing the link files to the most recently viewed video file by the appellant. *See* PE 5. There was no discussion in the record as to the significance of the 3 March 2011 date in PE 5 as to what particular video files were viewed. A review of the record reveals that the significance of that date was that it represented "the most recent time any file of that type (.mov or .qt) was accessed, not when the specific files in question were accessed." *See* PE 6 for Identification at 12. Because there was no testimony or evidence presented regarding the 3 March 2011 date, we cannot rule out that the

members may have interpreted that particular date as the date that the appellant viewed every one of those video files containing the .mov format. If that were true, this case would be a much stronger case in terms of legal and factual sufficiency. That, however, is not an accurate premise. In fact, based on PE 6 for Identification, the 3 March 2011 date could be the most recent time that the appellant accessed *any* video file in the .mov file format. In this regard, the 3 March 2011 date, bereft of any evidentiary or testimonial linkage, fares no better than the charged date of 16 May 2011.

With regard to the 3 March 2011 date, no evidence was presented to demonstrate: (a) when the video files were deleted; (b) when or how the videos were downloaded; (c) when they were viewed; or, (d) whether the appellant knew enough about computers to understand that when one deletes a file, it is not permanently deleted, but exists in unallocated space. Ms. SH was only able to testify that the videos had been on the computer at some point and then deleted. Neither Ms. SH nor the defense expert were able to testify with any degree of scientific certainty when the videos had been deleted from allocated space on the appellant's laptop.

Accordingly, we hold that under the unique facts and circumstances of this case and bound by *Navrestad*, the evidence was legally insufficient to prove that the appellant knowingly possessed the three charged video files on the date alleged in the charge sheet or the date that the members found the appellant guilty by exceptions and substitutions. Accordingly, we will set aside the finding of guilty as to Specification 1.[20]

It is important to note that these results are predicated only upon *the particular facts of this case* and how the Government chose to charge the offense. In this case, the Government built a strong circumstantial web that the appellant searched for, downloaded, viewed, and possessed child

[20] Because we set aside the finding as to Specification 1 as legally insufficient, this obviates our need to consider whether the military judge gave a fatal variance instruction. *See United States v. Treat*, 73 M.J. 331 (C.A.A.F. 2014) (holding that the test for material variance is whether the variance "substantially changes the nature of the offense, increases the seriousness of the offense, or increases the punishment of the offense") (citation and internal quotation marks omitted).

pornography video files; however, the web contained no connective tissue to the specific date in question.[21]

5. *Images 8 and 9*

The appellant argues that because only two digital images of child pornography were found on his portable hard drive in allocated space amongst thousands of adult pornography images, the evidence is factually and legally insufficient to prove knowing possession. We disagree.

Based on our review of the record, the appellant's 2009 LimeWire download, the fact that he viewed videos in the .mov and .qt video format containing titles highly suggestive of child pornography, and the fact that he had four video files of child pornography that had at one point been extant on his computer, we conclude that images 8 and 9 were not inadvertently downloaded by mistake or through a massive download of adult pornography. Ms. SH testified that the images of child pornography on the portable hard drive had been downloaded from the appellant's laptop. Accordingly, we reject the appellant's argument that he did not knowingly possess Images 8 and 9, which were located in *allocated* space on his portable hard drive.

Factual and Legal Sufficiency of Images 8 and 9

In appellant's third assignment of error, he alleges that Images 8 and 9 found on the Western Digital hard drive do not meet the statutory definition for child pornography.

The Government charged that the appellant knowingly possessed child pornography in violation of Article 134, UCMJ, clause (2). Although it is not required to do so under clause (1) and (2), the Government chose to allege child pornography as defined by 18 U.S.C. § 2256(8), the Child Pornography Prevention Act (CPPA). The military judge instructed the members as to the definition of child pornography that mirrored 18 U.S.C. § 2256(8).[22]

---

[21] We express no opinion as to whether digital evidence found and retrieved in unallocated space can be used to circumstantially prove constructive possession.

[22] "Again, 'child pornography' is defined as means of any visual depiction including any photograph, film, video, picture or computer, or computer-generated image or picture, whether made or produced by electronic, mechanical or other means of sexually explicit conduct where: A. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.

In *United States v. Roderick*, 62 M.J. 425, 429 (C.A.A.F. 2006), the CAAF adopted the factors outlined in *United States v. Dost* in determining whether an image portrays a "lascivious exhibition."[23] We review the *Dost* factors with an overall consideration of the totality of the circumstances. *Roderick*, 62 M.J. at 430. Furthermore, it is the prerogative of the fact-finder to decide whether images of child pornography contain actual minors. *United States v. Wolford*, 62 M.J. 418, 423 (C.A.A.F. 2006). That decision may also be made based on a review of the images alone, without expert assistance. *Id.*

Image 8 in PE 1

Image 8 depicts a young girl who is clearly a minor receiving cunnilingus. It is clear from the young girl's physical and facial features that she is a minor. Additionally, it is apparent from the image that a sexual act is occurring and the image itself provides sufficient evidence to enable a reasonable fact-finder to find guilt beyond a reasonable doubt. *Wolford*, 62 M.J. at 423. The appellant concedes that image 8 depicts a sexual act. Expert testimony was not necessary for a panel of competent members to come to a conclusion that the female pictured in image 8 is a minor based on viewing the image

---

'Minor' and 'child' mean any person under the age of 18 years.

'Sexually-explicit conduct' means actual or simulated of the following:

> (a) Sexual intercourse or sodomy including genital-to-genital, oral-to-genital, anal-to-genital, or oral-to-anal, between persons of the same or opposite sex;
> (b) Bestiality;
> (c) Masturbation;
> (d) Sadistic or masochistic abuse; or,
> Lascivious (e) lascivious exhibition of the genitals or pubic area of any person."

Record at 1762.

[23] *United States v. Dost*, 636 F.Supp. 828 (S.D. Cal. 1986), *aff'd sub nom. United States v. Weigand*, 812 F.2d 1239 (9th Cir. 1987)). The "*Dost* factors" are: "(1) whether the focal point of the visual depiction is on the child's genitalia or pubic area; (2) whether the setting of the visual depiction is sexually suggestive, i.e. in a place or pose generally associated with sexual activity; (3) whether the child is depicted in an unnatural pose, or in inappropriate attire, considering the age of the child; (4) whether the child is fully or partially clothed, or nude; (5) whether the visual depiction suggests sexual coyness or a willingness to engage in sexual activity; (6) whether the visual depiction is intended or designed to elicit a sexual response in the viewer." *Roderick*, 62 M.J. at 429 (quoting *Dost*, 636 F. Supp. at 832).

and listening to the military judge's instruction on the definition of child pornography. We are likewise convinced beyond a reasonable doubt that the sexual act depicted in image 8 meets the CPPA definition of child pornography as defined by the military judge's instruction.

Image 9 in PE 1

Image 9 depicts at least four fully nude young girls with what appears to be two more nude girls bending over behind them forming a pyramid. The appellant concedes that the girls depicted are minors. From the manner in which the girls are positioned, their breasts and genital areas are clearly and fully displayed and their genitals appear to be the focal point of the image. We agree with the assertion of both parties that this appears be a cheerleader pyramid. *See* Appellant's Brief at 56-57; Government Brief of 21 Apr 2014 at 26. Furthermore, we agree with the Government's assertion that cheerleaders and school-age girls are well-known subjects of hypersexual fantasy and are widely depicted in various forms in adult pornography. Government's Brief at 26. Accordingly, image 9 satisfies the majority of the *Dost* factors and based on the "totality of the circumstances," *Roderick*, 62 M.J. at 430, a reasonable fact-finder could conclude beyond a reasonable doubt that the image meets the definition of "sexually explicit conduct" under the CPPA. Additionally, we are convinced beyond a reasonable doubt that image 9 meets the definition of child pornography.

Failure to Instruct on Definition of "Lascivious"

In his fourth assignment of error, the appellant argues that the military judge erred when he failed to further define the word "lascivious." Because the appellant did not object to the military judge's instruction, we review for plain error. *See United States v. Tunstall*, 72 M.J. 191, 193 (C.A.A.F. 2013). To meet his plain error burden, the appellant must show that: "(1) there was error; (2) the error was plain or obvious; and, (3) the error materially prejudiced [the appellant's] substantial right[s]." *Id.* at 193-94 (citation and internal quotation marks omitted). Under the facts of this case, the appellant cannot meet his burden of establishing plain error.

Our plain error analysis of the military judge's failure to provide a definition of "lasciviousness" begins with a determination of whether the omission was error. The military judge provided instructions to the members by reading the CPPA statutory definition of child pornography. Record at 1762. He

further instructed the members that they could ask any questions about definitions in his instruction. Absent any indication from the members that there was confusion on the specific term "lascivious," we find that there was no error on the part of the military judge for failing to *sua sponte* provide a definition of the term. Furthermore, the appellant provides no evidence that the term "lascivious" was outside the common understanding of the members. Thus, if error it was not obvious.

Assuming *arguendo* that the military judge erred in failing to provide a definition of "lascivious" and that it was obvious error, no substantial right of the appellant was materially prejudiced. Unlike the facts in *United States v. Barberi*, 71 M.J. 127, 129 (C.A.A.F. 2012), the appellant in this case never claimed at trial that the images in question were not child pornography. Trial defense counsel's theory at trial was that the images were downloaded accidentally as part of a mass download of adult pornography. Thus, the appellant cannot meet his burden to demonstrate plain error.

Sentence Reassessment

Because of our action on the findings and the principles outlined in *United States v. Moffeit*, 63 M.J. 40 (C.A.A.F. 2006), *United States v. Cook*, 48 M.J. 434, 438 (C.A.A.F. 1998), and *United States v. Sales*, 22 M.J. 305, 307-09 (C.M.A. 1986), conducting a reassessment of the sentence would not be an appropriate option within the context of this case. "A 'dramatic change in the penalty landscape' gravitates away from the ability to reassess" the sentence. *United States v. Buber*, 62 M.J. 476, 479 (C.A.A.F. 2006) (quoting *United States v. Riley*, 58 M.J. 305, 312 (C.A.A.F. 2003)).

We find that there has been a dramatic change in the penalty landscape and do not believe that we can reliably determine what sentence the members would have imposed. *Riley*, 58 M.J. at 312.

Conclusion

The finding of guilty to Specification 1 of the Charge is set aside and that specification is dismissed. The findings of guilty to the Charge and Specification 2 of the Charge are affirmed. The sentence is set aside. We return the record to

the Judge Advocate General for remand to an appropriate CA with a rehearing on the sentence authorized.

Chief Judge MITCHELL and Judge FISCHER concur.

For the Court

R.H. TROIDL
Clerk of Court