

UNITED STATES ARMY COURT OF CRIMINAL APPEALS

Before
KERN, ALDYKIEWICZ, and MARTIN
Appellate Military Judges

UNITED STATES, Appellee
v.
Specialist MICHAEL S. SPIESS
United States Army, Appellant

ARMY 20100229

Headquarters, U.S. Army Alaska
Mark A. Bridges, Military Judge
Lieutenant Colonel Randall J. Bagwell, Staff Judge Advocate

For Appellant: Lieutenant Colonel Imogene M. Jamison, JA; Captain Jennifer A. Parker, JA; Colonel Edye U. Moran, JA (on brief).

For Appellee: Major Amber J. Williams, JA; Major Katherine S. Gowel, JA; Captain Christopher S. Glascott, JA (on brief).

28 September 2012

OPINION OF THE COURT

ALDYKIEWICZ, Judge:

A military judge, sitting as a general court-martial, convicted appellant, contrary to his pleas, of violating a lawful general order and knowingly possessing child pornography in violation of Articles 92 and 134, Uniform Code of Military Justice, 10 U.S.C. §§ 892, 934 (2006) [hereinafter UCMJ]. The convening authority approved the sentence to a bad-conduct discharge, confinement for fourteen months, and reduction to the grade of E-1.

The case is now before this court for review pursuant to Article 66, UCMJ. Appellant alleges a single assignment of error: that the military judge abused his discretion by admitting evidence at trial that was obtained or derived from an illegal search of appellant's external hard drive. We agree that the military judge erred when he concluded that the search in this case was private in nature. However, we conclude that appellant was not prejudiced by this error because (1) the evidence from appellant's external hard drive would have been inevitably discovered, and (2)

appellant's allegedly derivative confession is sufficiently attenuated from the illegal search so as to be admissible in its own right.

A. BACKGROUND

Appellant was deployed to Iraq in support of Operation Iraqi Freedom and resided on Forward Operating Base (FOB) Warhorse in a two-person containerized housing unit (CHU). Appellant shared his CHU with a fellow soldier, Specialist (SPC) JC. Appellant's CHU was divided into two halves with each half separated by a wall locker that acted as a make-shift wall down the middle. The CHU was secured by lock and key.

1. The Initial Discovery of Child Pornography

On 22 February 2009, while appellant was on rest and recuperation (R&R) leave in the United States, appellant's roommate, SPC JC, was securing all the personal belongings in their CHU as part of corrective training requiring him to "live out of his rucksack." This training was directed by the soldiers' platoon sergeant, Sergeant First Class (SFC) DH, in response to the poor living conditions SFC DH previously observed in the CHU. Specialist JC decided to watch a movie while he secured the belongings in the CHU. Consistent with his clean-up plan, SPC JC took his laptop computer to appellant's side of the CHU and connected it to appellant's external hard drive to search for a movie to download and view. Specialist JC knew appellant had movies on the hard drive because on several prior occasions appellant transferred movies to SPC JC's laptop when SPC JC asked him to do so. On all prior occasions, however, appellant connected the hard drive to SPC JC's computer and appellant himself executed both the search for movies and the file exchange. Appellant never provided SPC JC the actual hard drive to execute either the search or file transfer himself, nor did appellant give SPC JC unfettered or carte blanche access to use appellant's hard drive whenever he so desired. Furthermore, while appellant and SPC JC occasionally shared military gear, they never shared personal items.

As SPC JC searched appellant's external hard drive files for a movie, he came upon a file name that caused him concern, specifically, a file named "15 year old on 21 year old" or words to that effect. Specialist JC suspected the video file contained child pornography. Not wanting to wrongly accuse his roommate of misconduct, SPC JC decided to view the file and confirm his suspicions. When the movie played, SPC JC saw "a little girl about 12 years of age and a male late twenties early thirties" who was talking to the girl and then "[the little girl] takes her top off."

2. The Search and Seizure of Appellant's External Hard Drive

The following day, 23 February 2009, SPC JC approached SFC DH in the motor pool. Specialist JC told SFC DH that he found what he thought was child pornography on appellant's external hard drive. Sergeant First Class DH told SPC JC that it was obviously against the law and that SPC JC had to give him the hard drive. Visibly bothered by what he found and the situation of accusing a "battle buddy," SPC JC asked SFC DH to come by his CHU and "confirm" his suspicions.

When SFC DH arrived at the CHU later that evening, SPC JC initially started to give SFC DH the hard drive and then changed his mind, asking SFC DH to view the video at issue and confirm his suspicions. Specialist JC then proceeded, as he had done the night before, to appellant's side of the CHU and connected his laptop to appellant's external hard drive. Specialist JC checked the recent files on his laptop computer in an attempt to find the video he saw the day before. When the recent files search proved unsuccessful, SPC JC started searching various file folders on appellant's external hard drive for the video. That also proved unsuccessful. After numerous failed attempts to locate the video from the day before, SFC DH showed appellant how to search for computer files by simultaneously holding down the "Control" key and letter "F." Sergeant First Class DH physically held down both keys that launched the search function. Specialist JC then used the computer's "Control-F" search function and attempted to locate the movie he saw the day before, but was unsuccessful. At this point, SFC DH suggested various search terms for SPC JC to use. Sergeant First Class DH told appellant to try using numbers to locate the movie. This technique resulted in the discovery of another video containing child pornography, albeit a video separate and distinct from the video seen by SPC JC the day before. Specialist JC minimized this video and continued, while in SFC DH's presence, to search appellant's hard drive for the video he discovered the day before. A short time later, after continued efforts to locate that specific video failed, SPC JC and SFC DH decided to "maximize" the video which was earlier minimized. Once maximized, SPC JC and SFC DH viewed several seconds of this video which showed a child, age ten to twelve years old, masturbating an adult male.

After observing obvious child pornography, SFC DH seized appellant's hard drive and immediately delivered it to the company First Sergeant (1SG), 1SG AD, who in turn gave it to the unit commander, Captain (CPT) AW.¹ First Sergeant AD told CPT AW that the hard drive contained suspected child pornography. Captain AW immediately sought legal guidance and was told by "JAG" to contact U.S. Army

¹ Captain AW appears in various documents in the record as CPT AG, as her last name changed between the initial seizure of appellant's hard drive and time of trial.

Criminal Investigation Command (CID), which she did. She advised CID that she was in possession of a hard drive with suspected child pornography and was told to secure the hard drive until CID agents arrived. Neither CPT AW nor 1SG AD searched the hard drive or viewed any of its contents.

On 24 February 2009, CID Special Agents (SA) CH and KB arrived at FOB Warhorse to investigate the child pornography allegations against appellant. After securing appellant's hard drive from CPT AW, the agents conducted a search of appellant's CHU. Appellant's roommate, SPC JC, consented to a search of his side of the CHU and all of his property. The commander, CPT AW, authorized a search of appellant's side and all of appellant's property. The search discovered nothing of any evidentiary value. Special Agent CH also took sworn statements from SPC JC and SFC DH detailing the facts and circumstances surrounding their search of appellant's external hard drive. Specialist JC had previously provided a sworn statement to his commander.

3. CID's Interview of Appellant and his Subsequent Confession

On 12 March 2009, appellant arrived at Balad Air Base, returning to Iraq from his R&R leave. When he arrived in Balad, appellant was advised that he would remain there and not travel. The next day, appellant was transported to the CID offices on Balad.

When appellant arrived at CID on 13 March 2009, SA KB advised appellant of his Article 31, UCMJ, rights and that appellant was suspected of possessing child pornography. Appellant waived his rights and agreed to talk to SA KB. Special Agent KB did not apprise appellant of any of the evidence obtained against him. According to SA KB, the only thing he told appellant, beyond reading him his rights, was that appellant should be truthful with him. Appellant then confessed in a two-page, typewritten statement to possessing and viewing child pornography.

4. The Suppression Hearing

Appellant's external hard drive was not forensically examined by CID until several months after appellant confessed. Upon examination of the external hard drive, experts found numerous files of child pornography.

At his court-martial, appellant moved to suppress the evidence found on his external hard drive, arguing the evidence was obtained as a result of an illegal search and seizure. Appellant further moved to suppress his confession as derivative of the illegal search. This motion was litigated at an Article 39(a), UCMJ, hearing.

Special Agent KB testified at this hearing about his interview of appellant. Although appellant's external hard drive was already in CID's possession, SA KB stated that he did not inform appellant that appellant's external hard drive had

already been searched by SPC JC and SFC DH and that child pornography was found. Appellant disputed SA KB's testimony. In support of his motion to suppress, appellant testified that SA KB said, "We've got your hard drive. We've got computer experts that are paid to look into this and they're going to find anything that's on there." Appellant also testified he would not have confessed but for CID's possession of his external hard drive and knowledge of its contents.

In addition to the above, the suppression hearing established that SFC DH would have pursued action to seize the hard drive had he not already seized it. The following colloquy occurred between the military judge and SFC DH regarding the handling of the hard drive in the event that SPC JC had refused to turn it over:

Q: What would you have done if SPC [JC] said, "I'm not going to bring the hard drive to you"?

A: Well, actually, Your Honor, he told me what he thought it was. And then I would have pressed the command. I mean, it's already-- if he told me, "Hey, there's drugs here and they're not mine," I would still go after the drugs, so----

Q: So you would have notified your Command?

A: Yes, I would have

Similarly, the suppression hearing established that CPT AW would have pursued a search of appellant's CHU for child pornography had she only been confronted with SPC JC's 22 February 2009 observation of child pornography on appellant's hard drive as opposed to having been brought the hard drive by 1SG AD. In response to questioning by the military judge the commander testified, in part, as follows:

A: Given the fact that I was told by Specialist--well, the First Sergeant that there was child pornography or some type of pornography that was on the hard drive of this soldier's computer--or this hard drive--it gave me probable cause, as a Commander, because pornography is illegal in theater. That-- now, before the [sic] action needs to be taken, we need to make sure that we sanitize the area and make sure that we sanitize-- anything that's--that's incorrect, we need to correct it. So whatever measure needs to be taken, i.e., following the track that I was issued--or given--that--from recommendations--from a Legal Office or CID, that's the track I took.

. . . .

Q: Had they not brought the hard drive to you, but just came to you with the information that they had seen child pornography on the hard drive, in the CHU, would you have authorized a search, based upon that information?

A: Of the CHU?

Q: Of the CHU.

A: Roger, sir. And the reason I base it [sic] is just like a soldier that comes through this main gate, if they got--if there's drugs in the car, there's probably drugs somewhere else. And if they live on--and reside on post, I would--I, as a Commander, would say, "Well, you caught him for that at the gate, why don't you check his room, also?" And I have probable cause, because if he has it there, to me, it may, you know be passed and possessed through--through the entire barracks area. So the two, to me, are linked. That is your area, where stuff is stored. And that hard drive was stored there. So I have probable cause.

When asked about the trustworthiness of SPC JC and SFC DH, the commander testified:

They are trustworthy. They've never given me a reason not to trust them. Sergeant [First Class DH] has been a very, very faithful Platoon Sergeant, who has dealt with soldier issues very well. And he rarely has soldier issues. And when he does, he's very, very meticulous in handling it. So I understood that if he came to me, it had to be serious.

Finally, SA CH testified that if the Company Commander did not already have possession of appellant's external hard drive suspected to contain child pornography, CID would have "searched for and seized that hard drive."

After considering the defense motion along with its enclosures, the government response, and the testimony on the motion, the military judge denied the suppression motion, noting he would later issue written findings to be appended to the record.

On 17 April 2010, the military judge entered written "Findings and Conclusions," specifically finding that while appellant had an expectation of privacy in his external hard drive, both the 22 February 2009 and 23 February 2009 searches were private in nature and thus did not implicate appellant's rights under the Fourth Amendment as there was no governmental intrusion. Alternatively, the military judge found the evidence at issue would have been inevitably discovered. Having

found both searches to be private in nature, the military judge's findings and conclusions did not specifically address the admissibility of appellant's 13 March 2009 confession. Furthermore, the military judge's findings are silent with regard to any credibility determination between the diametrically opposed testimony of SA KB and appellant on whether appellant was confronted by the fact that his hard drive had already been searched and seized.

B. LAW

The Fourth Amendment prohibits “unreasonable searches and seizures,” *United States v. Daniels (Daniels II)*, 60 M.J. 69, 70 (C.A.A.F. 2004). U.S. Const. amend IV. In the military justice system, “[a] search or seizure is ‘unlawful’ if it was conducted, instigated, or participated in by . . . [m]ilitary personnel or their agents and was in violation of the Constitution of the United States as applied to members of the armed forces.” Military Rules of Evidence [hereinafter Mil. R. Evid.] 311(c)(1). *See Daniels II*, 60 M.J. at 71. A search is not unlawful if it is authorized by competent military or civilian authority based upon probable cause, Mil. R. Evid. 315, or if it falls within certain exceptions, to include the limited circumstances found in Mil. R. Evid. 312, 313, 314, and 317. “Evidence obtained as a result of an unlawful search or seizure made by a person acting in a governmental capacity” is inadmissible at a court-martial. Mil. R. Evid. 311(a). Thus, a necessary trigger for any search implicating Fourth Amendment protections is “government intrusion into an individual’s reasonable expectation of privacy.” *Daniels II*, 60 M.J. at 71.

However, “[t]he Fourth Amendment and Mil. R. Evid. 311 are not violated when a military member acts in a purely private capacity.” *United States v. Sullivan*, 42 M.J. 360, 363–64 (C.A.A.F. 1995). Whether a military member acts in a private capacity or in an official capacity depends not on the actor’s motivation but on whether the individual acted as “an instrument or agent of the Government.” *Skinner v. Railway Labor Executives’ Ass’n*, 489 U.S. 602, 614 (1989).

Government intrusion in violation of Fourth Amendment rights, in and of itself, does not automatically result in exclusion of the uncovered evidence at court-martial, nor does it necessarily require exclusion of derivative evidence. If the evidence would have been inevitably discovered through proper means, then that evidence is admissible against an accused. Mil. R. Evid. 311(b)(2). “The doctrine of inevitable discovery creates an exception to the exclusionary rule allowing admission of evidence that, although obtained improperly, would have been obtained by another lawful means.” *United States v. Wallace*, 66 M.J. 5, 10 (C.A.A.F. 2008) (citing *Nix v. Williams*, 467 U.S. 431 (1984)).

“[A]fter an accused challenges the legality of a search, the prosecution must, by a preponderance of the evidence, establish to

the satisfaction of the military judge that when the illegality occurred, the government agents possessed, or were actively pursuing, evidence or leads that would have inevitably led to the discovery of the evidence and that the evidence would inevitably have been discovered in a lawful manner had not the illegality occurred.”

United States v. Dease, 71 M.J. 116, 122 (C.A.A.F. 2012) (quoting *United States v. Kozak*, 12 M.J. 389, 394 (C.M.A. 1982)).

Confessions derivative of an illegal search or seizure in violation of the Fourth Amendment are generally inadmissible, notwithstanding a proper rights advisement pursuant to *Miranda v. Arizona*, 384 U.S. 436 (1966), or Article 31, UCMJ. However, if the government can establish the prior violation is sufficiently distinguishable from the later confession, so as to purge any taint from the illegality, then the confession is still admissible against an accused. *Brown v. Illinois*, 422 U.S. 590 (1975).² In *Brown*, the Supreme Court identified three factors “to determine if *Miranda* warnings were sufficient to remove the taint of an unlawful search and allow a subsequent confession,” *United States v. Conklin*, 63 M.J. 333, 338 (C.A.A.F. 2006) (citing *Brown*, 422 U.S. at 603–04). The three factors are: “temporal proximity of the unlawful police activity and the subsequent confession, the presence of intervening circumstances, and, the purpose and flagrancy of the official misconduct.” *Id.*

C. DISCUSSION

At issue in this case is the military judge’s denial of a defense motion to suppress evidence of child pornography found on appellant’s external hard drive following two allegedly unlawful searches of appellant’s computer, the first on 22 February 2009 by SPC JC and the next on 23 February 2009 by SPC JC and SFC DH. Also at issue is the military judge’s denial of the defense motion to suppress appellant’s later confession as derivative of the alleged unlawful searches.

A military judge’s ruling on a suppression motion is reviewed for an abuse of discretion. *Dease*, 71 M.J. at 120. Findings of fact and conclusions of law are

² See *Kaupp v. Texas*, 538 U.S. 626 (2003); *Taylor v. Alabama*, 457 U.S. 687 (1982); *Dunaway v. New York*, 442 U.S. 200 (1979); *United States v. Conklin*, 63 M.J. 333 (C.A.A.F. 2006). But see *New York v. Harris*, 495 U.S. 14 (1990) (finding admission of evidence constitutionally permissible and declining application of *Brown*’s attenuation analysis where the defendant was illegally arrested but later confessed while in lawful custody).

reviewed under a clearly erroneous standard and de novo standard, respectively. *United States v. Rodriguez*, 60 M.J. 239, 246 (C.A.A.F. 2004). When considering a military judge’s ruling on a suppression motion, the court considers the evidence “in the light most favorable to the prevailing party.” *United States v. Reister*, 44 M.J. 409, 413 (C.A.A.F. 1996). “In order to find an abuse of discretion, we must find that the military judge committed a clear error in his conclusions.” *Dease*, 71 M.J. at 121.

1. Reasonable Expectation of Privacy

The military judge’s findings correctly reflect that appellant had a reasonable expectation of privacy in his external hard drive. The hard drive was stored in a secured CHU. The CHU was divided into two halves by a wall locker and the hard drive was kept on appellant’s side. While appellant and SPC JC occasionally shared military “gear,” they did not share personal belongings. Finally, appellant never gave SPC JC permission to use his hard drive nor did SPC JC believe that he had unfettered or carte blanche access to the drive. On all prior occasions where movies were transferred from appellant’s hard drive to SPC JC’s computer, appellant searched for and executed the file transfers. Accordingly, the military judge correctly concluded that appellant had a reasonable expectation of privacy in his external hard drive. *See Conklin*, 63 M.J. at 337.

2. Private Action or Governmental Intrusion

SPC JC’s Initial Discovery of Child Pornography

Specialist JC’s search of appellant’s external hard drive on 22 February 2009 did not amount to a government intrusion into appellant’s reasonable expectation of privacy. Specialist JC’s actions in searching appellant’s external hard drive for movies, resulting in the discovery of child pornography, was a private, non-governmental search. At the time of the search, SPC JC and appellant were the same rank and neither soldier held a position of authority over the other. The purpose of SPC JC’s search was to simply find a movie to watch as he cleaned their CHU. At the time of the search, SPC JC did not suspect his roommate of any criminal activity, did not suspect that the hard drive contained any items of a contraband nature, and was not engaged in any law enforcement or command directed activity focused on appellant or his hard drive. Nothing regarding SPC JC’s actions in connecting appellant’s hard drive to his personal laptop computer and subsequently searching the drive for a movie to watch has any indicia of official, governmental action. *See Daniels II*, 60 M.J. at 71 (citing *Skinner*, 489 U.S. at 615–16 (1989)). Accordingly,

the military judge correctly concluded SPC JC's actions did not violate appellant's Fourth Amendment rights.³

*SPC JC's and SFC DH's Subsequent Search
of Appellant's External Hard Drive*

Although the initial discovery of appellant's child pornography was not in violation of the Fourth Amendment, we conclude that the subsequent, unauthorized search of appellant's external hard drive was unlawful. *See* Mil. R. Evid. 313–315. Sergeant First Class DH's direction and participation in SPC JC's subsequent search of appellant's external hard drive amounted to a government intrusion into appellant's reasonable expectation of privacy. The military judge's findings of fact with regard to the 23 February 2009 search engaged in by SPC JC and SFC DH are supported by the record and as such are not clearly erroneous. However, in applying the law to these facts, the military judge erroneously concluded that SFC DH's involvement did not transform what was previously a private search by SPC JC into a governmental intrusion. In this respect, the military judge's application of the law to the facts was clearly erroneous.

On appeal, the government urges us to consider *United States v. Daniels (Daniels II)*, 60 M.J. 69 (C.A.A.F. 2004), in support of the military judge's finding of a private, non-governmental intrusion. The *Daniels* case turned on whether a government official encouraged, endorsed, or participated in a third party's search such that the third party became an agent for the government official. The government correctly notes the applicability of *Daniels* to the instant case, but a review of *Daniels* reveals that it does not support the government's argument of private action.

In *Daniels*, the appellant, Seaman Apprentice (Seaman) Daniels, placed a vial in his nightstand drawer and told his roommate, Seaman V, that the vial contained cocaine. *Daniels II*, 60 M.J. at 70. The following day Seaman V told their supervising instructor, Chief W, about the appellant's possession of the illegal substance. Chief W told Seaman V to retrieve the vial and bring it back to him. Notwithstanding his belief that Seaman Daniels was merely joking with his

³ Regarding the 22 February 2009 search, the military judge made one finding of fact unsupported by the record. The military judge found that the video observed by SPC JC depicted an adult man lying "down on the bed with the girl." This finding of an adult male in bed with the child is unsupported by the record. All other findings regarding the 22 February 2009 are supported by the record. More importantly, the military judge's application of the law to the supported factual findings, without consideration of the erroneous finding, is correct.

roommate, Chief W nonetheless submitted the vial for testing, testing that subsequently revealed the presence of cocaine and formed the basis of the appellant's conviction. *Id.* at 69–70. Prior to trial, the appellant moved to suppress this evidence, arguing that the retrieval of the vial from his nightstand violated the Fourth Amendment. *Id.* at 69. The military judge concluded the search was non-governmental in nature and denied the motion.

Seaman Daniels raised this same issue on appeal, and the Navy-Marine Corps Court of Criminal Appeals held that the retrieval of the vial from his nightstand was neither a search nor governmental action. The Navy Court based its decisions on the facts that Chief W did not actually suspect that the appellant had drugs in his room and that Seaman V's motivation in seizing the alleged drugs was privately motivated to protect his own personal interests. *United States v. Daniels (Daniels I)*, 58 M.J. 599, 604–06 (N.M. Ct. Crim. App. 2003).

The Court of Appeals for the Armed Forces (CAAF) disagreed, holding the Navy Court “erred on both accounts.” *Daniels II*, 60 M.J. at 71. In arriving at its decision, CAAF noted:

[T]he question of whether a private actor performed as a government agent does not hinge on motivation, but rather “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 circumstances.’” *Skinner*[, 489 U.S. at 614–15]. To implicate the Fourth Amendment in this respect, there must be “clear indices of the Government's encouragement, endorsement, and participation” in the challenged search. *Id.* at 615–16.

Daniels II, 60 M.J. at 71. CAAF concluded that Seaman V's actions amounted to governmental intrusion, as opposed to private action, because Seaman V did not, of his own accord, bring the suspected vial of cocaine to Chief W for consultation. Instead, Seaman V consulted with Chief W first and was then directed by Chief W to retrieve the vial. The court found “Chief [W's] specific order as a government official triggered [Seaman V's] actual seizure of the vial.” *Id.* Therefore, “Chief [W] clearly encouraged, endorsed, and participated in [Seaman] V's seizure of the vial and, accordingly, [Seaman V] acted as Chief [W's] agent when he seized the vial.” *Id.*

As in *Daniels*, the issue before this court is the degree of participation by a government official in a private party's search. Stated another way, the issue is to what extent, if any, did SFC DH encourage, endorse, and participate in the search of

appellant’s computer on 23 February 2009.⁴ In this respect, the military judge made an error similar to that made by the Navy Court in *Daniels*—he focused on the private party’s motivation for conducting the search instead of the government official’s encouragement, endorsement, and participation in that search.

In his written findings, the military judge noted that “[a]lthough SFC [DH] did suggest terms and methods for searching for files on the computer, those actions did not influence SPC [JC] in his own desire to find the video file and show it to SFC [DH].” The military judge then concluded that SFC DH did not encourage, endorse, or participate in the search. In our view, the facts do not support this conclusion. Like Chief W in *Daniels*, SFC DH directed SPC JC to give him the hard drive and when SFC DH arrived at appellant’s CHU, SPC JC initially provided SFC DH with the hard drive. However, SPC JC changed his mind and asked SFC DH to confirm his suspicions regarding the child pornography that he observed the day before. Sergeant First Class DH then proceeded to involve himself in SPC JC’s ensuing search of appellant’s hard drive. Had SPC JC immediately retrieved the file in question and simply displayed it to SFC DH or given SFC DH the hard drive, without any action by SFC DH, the military judge’s conclusion would be correct in that SFC DH would have had nothing more than a passive role, if any, in the search. The mere delivery, or in this case, display of contraband by one private party to a government official or law enforcement official does not convert an otherwise private act into governmental intrusion triggering Fourth Amendment protections. *Daniels II*, 60 M.J. at 71.⁵

⁴ Neither CAAF in *Daniels* nor the Supreme Court in *Skinner*, the case upon which *Daniels* relies, define “encourage, endorse, and participate”; however, the plain meaning of those words are adequate for resolution of the instant case. Black’s Law Dictionary 607, 1229 (9th ed. 2009), defines “encourage” as, “To instigate; to incite to action,” and it defines “participation” as, “The act of taking part in something, such as a partnership, a crime, or a trial.” Webster’s II New Riverside Dictionary (rev. ed. 1996), defines “encourage” as, “To support [or] foster”; “endorse” as, “To approve of publicly [or] support”; and “participate” as, “To join with others in something [or] take part.”

⁵ See, e.g., *United States v. Gregory*, 611 F.Supp. 1033, 1044 & n.35 (S.D.N.Y. 1985) (finding no Fourth Amendment violation where evidence was inspected by law enforcement officials when delivered by a private citizen) (citing *Walter v. United States*, 447 U.S. 649 (1980), *Burdeau v. McDowell*, 256 U.S. 465 (1921), and *United States v. McGuire*, 381 F.2d 306, 313 n.5 (2d Cir. 1967)); *State v. Buswell*, 460 N.W.2d 614 (Minn. 1990) (finding no Fourth Amendment violation where evidence was seized following the search of a motor vehicle delivered to law enforcement personnel); *State v. Lamb*, 224 S.E.2d 51 (Ga. Ct. App. 1976) (finding no Fourth

(continued . . .)

Specialist JC, however, did not simply retrieve the suspect file and show it to a passive, noncommissioned officer who was in the CHU pursuant to the invitation of one of its two lawful occupants. Sergeant First Class DH specifically went to the CHU to retrieve suspected evidence of child pornography, and when he arrived, SPC JC began a confirmatory search of appellant's external hard drive. When SPC JC could not find the suspected child pornography that he had observed the day prior, SPC JC engaged in a detailed search of appellant's hard drive, a search conducted in the presence of SFC DH. Furthermore, SFC DH did more than sit idly by; SFC DH himself, not SPC JC, manipulated the keyboard of the laptop to launch the search engine. When SPC JC was still unable to locate the suspected child pornography, SFC DH suggested search terms to use, terms that eventually discovered a separate and distinct file containing child pornography. Contrary to the military judge's written findings, SFC DH's actions in launching the search tool necessary to search appellant's computer, and then suggesting search terms, amounted to more than a passive role in the search of appellant's computer. The fact that SPC JC typed the search terms suggested to him by SFC DH is less than compelling in evaluating SFC DH's actions.

On the facts of this case, we find that SFC DH encouraged, endorsed, and participated in the search of appellant's external hard drive. Therefore, SPC JC's and SFC DH's search was a government intrusion into appellant's reasonable expectation of privacy, and the military judge's conclusion to the contrary is clearly erroneous.

3. Inevitable Discovery Exception to the Exclusionary Rule

Although SPC JC's and SFC DH's unauthorized search violated the Fourth Amendment, we nonetheless conclude appellant was not prejudiced by the military judge's ruling to the contrary. We hold that the child pornography found on appellant's external hard drive pursuant to the unlawful search would have been inevitably discovered and was therefore admissible against appellant at his court-martial.

As previously noted, SPC JC's actions on 22 February 2009 were private in nature and thus did not trigger Fourth Amendment protections for any of the information discovered during that search. Thus, the evidence discovered by SPC JC in his private capacity could have been lawfully used to support a search

(. . . continued)

Amendment violation where marijuana was delivered to law enforcement personnel by a dormitory supervisor).

authorization—assuming it established probable cause—which, in turn, could have led to the lawful search and seizure of appellant’s hard drive. However, absent probable cause to believe appellant’s computer contained child pornography, “there could be no application of the doctrine of inevitable discovery in this case.” *Dease*, 71 M.J. at 121–22 (citations omitted).

Probable cause is “a fair probability that contraband or evidence of a crime will be found in a particular place.” *United States v. Williamson*, 65 M.J. 706, 712 (Army Ct. Crim. App. 2007) (quoting *Illinois v. Gates*, 462 U.S. 213, 238 (1983)). In the context of military search authorizations, probable cause is defined as “a reasonable belief that the person, property, or evidence sought is located in the place or on the person to be searched.” Mil. R. Evid. 315(f)(2). The Military Rules of Evidence further note that “[a] search authorization may be based upon hearsay evidence in whole or in part.” *Id.* A file name alone may be sufficient to establish probable cause. See *United States v. Yammine*, 69 M.J. 70, 75 (C.A.A.F. 2010) (citing *United States v. Leedy*, 65 M.J. 208, 215–18 (C.A.A.F. 2007)).

The information conveyed by SPC JC to his platoon sergeant, SFC DH, went well beyond a single file name that might be indicative of child pornography. On 22 February 2009, SPC JC, acting in a purely private capacity, observed suspected child pornography on the external hard drive of appellant’s computer. The military judge found the video “was of a man and little girl entering a bedroom.” The little girl, estimated by SPC JC to be “eleven to twelve” years of age, was wearing a swimsuit and being followed from behind by an adult male. Specialist JC observed the girl “take her top off.” He also saw the adult male start to “lay down.” At that point, SPC JC stopped watching the video. Specialist JC recalled the file name of the video to be “15 on 21 or something like that.” Specialist JC’s observations establish probable cause to believe that appellant’s external hard drive contained child pornography.

The record further establishes that had the external hard drive not been seized, appellant’s commander, CPT AW, would have authorized a search of his CHU, and the external hard drive would have been seized and eventually processed by appropriate law enforcement officials. In *United States v. Wallace*, 66 M.J. 5 (C.A.A.F. 2008), our superior court applied the doctrine of inevitable discovery in an analogous situation. In *Wallace*, the appellant’s computer was initially seized pursuant to invalidly obtained consent; however, CAAF held that the evidence found on that computer would have been inevitably discovered: “[H]ad Appellant not ultimately consented to the seizure of the computer, the [Air Force Office of Special Investigations] would have sought and obtained a search authorization based upon probable cause. . . . [T]he files containing child pornography would have been inevitably discovered through this valid search.” *Id.* at 10. Cf. *Dease*, 71 M.J. 116.

In the instant case, SFC DH already “possessed” evidence that established probable cause to suspect appellant’s external hard drive contained child pornography and he, along with the appellant’s commander, CPT AW, articulated unequivocally, along with SA CH, what would have occurred—the external hard drive would have been seized and eventually searched for child pornography by law enforcement personnel. Accordingly, we hold the evidence at issue would have been inevitably discovered and was therefore properly admitted against appellant at his court-martial.

4. Derivative Evidence and the Presumption of Prejudice

Although the evidence ultimately discovered on appellant’s hard drive was properly admitted into evidence, there remains a question as to whether appellant’s confession was also properly admitted. In this case, appellant claims that his confession was derivative of the underlying unlawful search by SFC DH on 23 February 2009 and should have been excluded as “fruit of the poisonous tree.” We disagree. Applying the *Brown* factors to appellant’s case, we conclude that appellant’s confession was sufficiently attenuated from the unlawful search so as to make appellant’s properly warned confession independently admissible.

A causal connection alone between an unlawful search and the alleged derivative evidence, in this case appellant’s confession, does not make the derivative evidence per se inadmissible. *United States v. Murphy*, 39 M.J. 486, 487 (C.M.A. 1994) (citing *Nardone v. United States*, 308 U.S. 338 (1939)). “As a matter of good sense . . . such connection may have become so attenuated as to dissipate the taint.” *Nardone*, 308 U.S. at 341. In *Wong Sun v. United States*, 371 U.S. 471 (1963), the Supreme Court noted:

We need not hold that all evidence is “fruit of the poisonous tree” simply because it would not have come to light but for the illegal actions of the police. Rather, the more apt question in such a case is whether, granting establishment of the primary illegality, the evidence to which the instant objection is made has been come at by exploitation of that illegality or instead by means sufficiently distinguishable to be purged of the primary taint.

Wong Sun, 371 U.S. at 487–88 (internal citations and quotation marks omitted). To make this determination, we consider three factors: “temporal proximity of the [constitutional violation] and the confession, the presence of intervening circumstances, **and, particularly**, the purpose and flagrancy of the official misconduct.” *Brown*, 422 U.S. at 603–04 (emphasis added). See *United States v. Conklin*, 63 M.J. 333, 338 (C.A.A.F. 2006).

The first *Brown* factor, temporal proximity, favors the government. The unlawful search in this case occurred, as previously noted, on 23 February 2009 when SFC DH and SPC JC searched appellant's external hard drive in an effort to find and review the child pornography seen the day prior by SPC JC. On 23 February 2009 appellant was out of the theater of operations on R&R leave. Between 10 and 11 March 2009, appellant returned to theater, and on 13 March 2009, appellant met with CID. After being properly advised of and waiving his Article 31, UCMJ, rights, appellant admitted to possessing child pornography. At the time of appellant's meeting with CID he "didn't think anything of it, because I had previously talked to CID. They had questions about something in the past; and I told them."⁶ Excluding both the day of the illegal search as well as appellant's confession, seventeen days elapsed between the constitutional violation in appellant's case and his confession.⁷

The second *Brown* factor, the existence of intervening circumstances, favors the government as well. The 23 February 2009 search was executed by a platoon sergeant and subordinate. Law enforcement personnel were not involved, either directly or indirectly in the illegal search. When Balad CID agents, SA CH and SA KB, became involved on 24 February 2009, they sought and obtained a valid search authorization from appellant's commander.⁸ The second intervening circumstance is

⁶ Although the facts and circumstances surrounding appellant's prior contact with CID are not developed in the record, it is clear that appellant's prior contact with CID was unrelated to the charges at issue.

⁷ Compare *United States v. Taylor*, 2 M.J. 863 (A.C.M.R. 1976) (appellant's confession was not tainted by an illegal search conducted two days earlier), and *United States v. Patino*, 862 F.2d 128 (7th Cir. 1988) (appellant's second confession was not tainted by an illegal search conducted six days earlier), with *Kaupp v. Texas*, 538 U.S. 626 (2003) (no substantial time between illegal arrest and confession favors defendant), *Taylor v. Alabama*, 457 U.S. 687 (1982) (six hours between "investigatory arrest without probable cause" and confession favors defendant), *Brown v. Illinois*, 422 U.S. 590 (1975) (less than two hours between illegality and confession favors defendant), and *United States v. Conklin*, 63 M.J. 333 (C.A.A.F. 2006) (less than three hours between illegal search of appellant's computer and subsequent consent favors appellant).

⁸ Of note, on 26 May 2009, SA CH also sought and obtained a magistrate's authorization to search appellant's external hard drive seized from his CHU for "Text, graphics, electronic mail messages, which are read, unread or unopened, and other data including deleted files and folders pertaining to the online solicitation of minor(s), and/or material related to the sexual exploitation of minors; and/or

(continued . . .)

that appellant was interviewed following a proper Article 31, UCMJ rights advisement, which he waived. More importantly, he was not confronted by the fact that his computer had been searched and seized. Contrary to appellant's testimony on the suppression motion, SA KB, the CID agent who interviewed appellant, noted appellant was only told to tell the truth. The following colloquy between the military judge and SA KB focused specifically on what appellant was told vis-à-vis any evidence the government might have on appellant establishing his guilt for possession of child pornography:

Q. When you advised the accused about why he was there, what did you tell him?

A. I explained to him that there's allegations of--that he's in possession of child pornography, sir.

Q. Did you make any reference to any evidence which had been seized in the case?

A. No, sir, I did not.

Q. Were you aware that a hard drive had been seized from the accused's room?

A. Correct, sir. I--I was there, when we--we seized it, sir.

Q. But you did not mention that to the accused, when you talked to him?

A. No, sir. No.

Q. You just told him that there [are] allegations----

A. That's correct.

Q. ----that he possessed child pornography?

A. Yeah. And he needed to be truthful about it. And which he was, sir.

(. . . continued)

material depicting apparent or purported minors engaged in sexually explicit conduct; and data and/or information used to facilitate access to, production, distribution, and/or production of such material.”

Q. So you never went into any of the evidence, whatsoever, that you already had against the accused?

A. That's right, sir. No, sir.

In the case at bar, SPC JC's observations provided law enforcement personnel a legitimate basis to interrogate appellant. When interviewed by SA KB, appellant was not confronted by any illegally obtained evidence nor was he aware that CID already had his computer. After a proper rights advisement and waiver thereof, appellant provided a written statement confessing to possession of child pornography.

The third *Brown* factor, "the purpose and flagrancy of the official misconduct," also favors the government. On 23 February 2009, SFC DH already had probable cause to believe appellant's external hard drive contained child pornography; SPC JC was very clear on what he observed the day before. Sergeant First Class DH went to appellant's CHU in response to a request from SPC JC, and only after SPC JC decided not to turn over the hard drive but instead show SFC DH the pornographic file did a search begin. At first, SFC DH sat as a passive observer waiting for SPC JC to retrieve the file that SPC JC observed the day before. Only after SPC JC's efforts to search the external hard drive proved futile did SFC DH encourage, endorse, and participate in the search. The evidence fails to establish that either SFC DH knew he was violating appellant's constitutional rights or that, armed with this knowledge, he chose to engage in an unconstitutional search anyway. *See United States v. Khamsouk*, 57 M.J. 282, 293 (C.A.A.F. 2002). Unlike the actions of the officers in *Brown*, the "impropriety" of the constitutional violation was not obvious. *Brown*, 422 U.S. at 605.

Similarly, unlike the *Brown* officers, SFC DH did not "embark upon this expedition for evidence in the hope that something might turn up." *Id.* SFC DH went to appellant's CHU to retrieve a hard drive containing child pornography. When he arrived, appellant's roommate refused to turn over the hard drive and instead asked SFC DH to confirm what he, SPC JC, had seen the day before. When the video file in question could not be located, SFC DH participated in a search for that file and when he and SPC JC found a suspected file containing child pornography, the computer was immediately turned off, seized and provided to the chain of command.

There is no evidence to conclude that SFC DH or any member of appellant's chain of command acted in bad faith on 23 February 2009. In fact, when asked by the military judge what he, SFC DH, would have done had SPC JC not turned over the hard drive, rather than seize the hard drive immediately, SFC DH indicated he would have used the chain of command and pursued legal action to obtain the hard drive. Regarding the actions of the CID agents, SA CH and SA KB, there is no evidence that they acted in bad faith or with any intention to circumvent the

mandates of the Fourth Amendment. Quite the contrary, everything they did was in accordance with the mandates of both the Fourth Amendment and the Military Rules of Evidence. On 24 February 2009, CID agents sought authorization to search appellant's CHU and a magistrate's authorization was sought prior to conducting any forensic analysis of appellant's external hard drive. Before interviewing appellant, nearly three weeks after the discovery of child pornography, CID agents informed appellant of his Article 31, UCMJ, rights. Finally, there is no evidence either CID agent was even aware of the constitutional violation.

Applying all three *Brown* factors to the facts and circumstances of appellant's case, we find any taint from the 23 February 2009 illegal search of appellant's external hard drive sufficiently attenuated. We further find no deterrent value in application of the exclusionary rule to the facts and circumstances of this case. As our superior court noted in *Khamsouk*:

“The primary justification for the exclusionary rule . . . is the deterrence of police conduct that violates Fourth Amendment rights.” *Stone v. Powell*, 428 U.S. 465, 486[](1976)
However, despite its broad purpose, “the rule does not ‘proscribe the introduction of illegally seized evidence in all proceedings or against all persons,’ . . . but applies only in contexts ‘where its remedial objectives are thought most efficaciously served.’” *Penn. Board of Probation and Parole v. Scott*, 524 U.S. 357, 363[](1998) (quoting *Stone v. Powell*, 428 U.S. at 486[]). . . .

. . . .

Thus, in determining whether invocation of the rule is warranted, the Court insists that lower courts strike a balance between “the public interest in determination of the truth at trial” and the “incremental contribution that might [be] made to the protection of Fourth Amendment values” *Stone*, 428 U.S. at 488[].

Khamsouk, 57 M.J. at 291–92. Accordingly, the military judge did not abuse his discretion in admitting appellant's confession.

D. CONCLUSION

In sum, SPC JC's 22 February 2009 search of appellant's external hard drive was non-governmental in nature, making any evidence discovered during this search independently admissible against appellant. Additionally, the evidence discovered established probable cause to believe appellant possessed child pornography. Contrary to the military judge's conclusion, the subsequent, 23 February 2009, search of appellant's external hard drive by SPC JC and SFC DH was governmental in nature and as such, illegal. Notwithstanding the military judge's erroneous

characterization of the 23 February 2009 search as private in nature, the evidence found on appellant's external hard drive was admissible against appellant as the evidence would have been, as the military judge correctly found, inevitably discovered. Finally, appellant's 13 March 2009 confession was sufficiently attenuated from the illegal search making appellant's confession independently admissible from the evidence found on appellant's external hard drive.

On consideration of the entire record, we hold the findings of guilty and sentence as approved by the convening authority correct in law and fact. Accordingly, the findings of guilty and the sentence are AFFIRMED.

Senior Judge KERN and Judge MARTIN concur.



FOR THE COURT:

A handwritten signature in black ink, which appears to read "Malcolm H. Squires, Jr.", is written over the printed name.

MALCOLM H. SQUIRES, JR.
Clerk of Court