

This opinion is subject to administrative correction before final disposition.

United States Navy - Marine Corps
Court of Criminal Appeals

Before
CRISFIELD, HITESMAN, and GASTON
Appellate Military Judges

UNITED STATES
Appellant

v.

Samuel W. CROCKER
Lance Corporal (E-3), U.S. Marine Corps
Appellee

No. 201900226

Decided: 16 March 2020

Appeal by the United States pursuant to Article 62, UCMJ

Military Judge:
Keaton H. Harrell

Arraignment: 8 April 2019 before a general court-martial convened at
Marine Corps Base Camp Lejeune, North Carolina.

For Appellant:
Major Kerry E. Friedewald, USMC;
Captain Brian L. Farrell, USMC;
Lieutenant Timothy C. Ceder, JAGC, USN.

For Appellee:
Lieutenant Commander Christopher Riedel, JAGC, USN.

Senior Judge HITESMAN delivered the opinion of the Court, in which
Chief Judge CRISFIELD and Judge GASTON joined.

PUBLISHED OPINION OF THE COURT

HITESMAN, Senior Judge:

This case is before us as an interlocutory appeal taken by the Government. Appellee is charged with one specification of sexual abuse of a child and one specification of viewing child pornography in violation of Articles 120b and 134, Uniform Code of Military Justice [UCMJ], 10 U.S.C. §§ 920b, 934 (2012). At a pretrial hearing, the military judge granted, in part, a Defense motion to suppress evidence resulting from a search of Appellee’s cell phone. The Government appeals the military judge’s ruling “which excludes evidence that is substantial proof of a fact material in the proceeding.” Article 62(a)(1)(B), UCMJ. The Government contends the military judge abused his discretion by suppressing both evidence from the search and Appellee’s subsequent confession. We conclude the military judge did not abuse his discretion and deny the Government’s appeal.

I. FACTUAL AND PROCEDURAL BACKGROUND

A. Factual Background

On 3 December 2018, Appellee reported to the Criminal Investigation Division [CID], Camp Lejeune, North Carolina, as a victim of a larceny. He had proof that Lance Corporal [LCpl] DW had obtained access to his bank account and had stolen money from him. CID Agent MS interviewed Appellee who explained that LCpl DW owed Appellee money and had asked for the Appellee’s bank account information so that LCpl DW’s father could transfer money directly to Appellee’s account. Appellee said he and LCpl DW only used the Facebook Messenger application to exchange messages.¹ Appellee said LCpl DW then used the information provided by Appellee to steal money from his bank account. Appellee showed Agent MS the Facebook Messenger exchanges with embedded screenshots, between Appellee and LCpl DW. LCpl DW sent the screenshots to Appellee depicting brief text exchanges between LCpl DW and his father supporting the need to obtain Appellee’s bank account information. Agent MS knew the messages he was shown were contained within the Facebook Messenger application.

¹ Throughout the record of trial, the terms “texts,” “text messages,” “messages,” “Facebook messages,” and “Facebook Messenger messages” are used interchangeably.

Agent MS did not suspect Appellee of any offense at the time of the initial interview. Agent MS asked Appellee for the messages he was shown. Specifically, he asked, “I’d like to get those texts from him because that shows that he like asked for the security questions and stuff. Are you OK with me like getting that information from you?”² Appellee responded, “I don’t care.”³ Agent MS explained, “OK. Alright, the way we do it, we have a form right here. I just need some initials from you.”⁴ Agent MS then went through the Permissive Authorization for Search and Seizure [PASS] form⁵ with Appellee. The PASS clearly indicates that Appellee permitted “CID, law enforcement” to search his “android ZTE Axon 7 mini” for evidence relating to “fraud [and] larceny.”⁶ Agent MS used a Universal Forensic Extraction Device [UFED] to extract and copy all of the data from Appellee’s phone before he returned it to Appellee. Later, Agent MS used additional software to sort and view the data extracted from Appellee’s phone.

Agent MS did not attempt to limit his search to folders specifically related to the Facebook Messenger application. Instead, he first looked for “communications between [Appellee] and [LCpl DW] as well as any evidence of the fraud and larceny” by searching the short message service [SMS] folder of the extraction⁷ where he expected to find only text messages. Agent MS did not find the Facebook messages in the SMS folder, so he next searched the multimedia messaging service [MMS] folder, believing it might contain the messages and screenshots. Agent MS did not find the conversations he was shown between Appellee and LCpl DW in either of these folders, so he then decided to search the images folder. Agent MS did not attempt to use any filters, but rather he decided to manually scroll through and look at more than 43,000 thumbnail images. While scrolling through the images looking for text messages and screenshots of text messages, Agent MS observed two thumbnail images that he suspected were child pornography depicting “full frontal nudity of what appeared to be seven or eight-year-old girls.”⁸ Without opening or enlarging the thumbnail images, Agent MS stopped his search and no-

² App. Ex. VIII at 3.

³ *Id.*

⁴ *Id.*

⁵ *Id.*

⁶ App. Ex. III at 18.

⁷ Record at 35-36.

⁸ *Id.* at 43-44.

tified the Naval Criminal Investigative Service [NCIS] because child pornography falls within their investigative purview.

The following day, Agent MS brought the UFED extraction report of Appellee's phone data to NCIS Special Agent SI and told her that while looking through a file on a phone in a separate case involving fraud, he discovered some images that appeared to be child pornography. Agent MS informed Special Agent SI that he had obtained a PASS for the phone but he did not provide any details regarding the scope of Appellee's consent. Special Agent SI looked in the images folder of the UFED report and found several images of suspected child pornography. Special Agent SI opened and enlarged several thumbnail images to reveal full sized images to confirm her suspicions that the images could be child pornography. Later that day, Special Agent SI interviewed Appellee. She advised him of his Article 31(b), UCMJ, rights and told him that he was suspected of possessing child pornography. Appellee waived his rights and admitted to viewing and possessing child pornography as well as sexually abusing his four-year-old nephew. Appellee provided a sworn statement of his admissions and granted NCIS agents a PASS to search his laptop and barracks room.

On 7 December 2018, several days after obtaining Appellee's confession and additional PASS authorizations, Special Agent SI obtained a Command Authorization for Search and Seizure [CASS] from Appellee's commanding officer. Special Agent SI requested authorization to seize Appellee's phone and search it for child pornography, citing "four" images in detail that she observed when NCIS agents reviewed the UFED extraction report of Appellee's phone data with Agent MS. Special Agent SI did not tell Appellee's commanding officer that she had already interrogated Appellee and obtained a confession. The CASS-authorized search revealed an additional 268 images of suspected child pornography, four of which were eventually identified as known child victims.

None of the Facebook messages nor any of the embedded screenshots pertinent to Appellee's larceny claim were ever found anywhere on Appellee's phone.

B. Motion to Suppress Evidence

At an Article 39(a), UCMJ, hearing, the Defense moved to suppress the evidence found on Appellee's phone as well as his confessions. Agent MS and Special Agent SI both testified and the Defense and Government submitted several pieces of evidence to include CID and NCIS interim reports, video recordings of Appellee's interviews with Agent MS and Special Agent SI, and the PASS and CASS for Appellee's cell phone.

The military judge issued a 36-page written ruling containing ten and a half pages of detailed findings of fact. The most significant findings relate to the conversation and understanding of both Appellee and Agent MS as to what evidence Agent MS wanted and where on Appellee's phone that information was located. These key findings of fact are:

The accused explained that LCpl [DW] made multiple fraudulent transactions after asking the accused for and receiving the answers to the security questions for the accused's bank account.

. . . [T]he accused said in response to a question by Agent [MS], "I'm going to show you a text message . . . Yeah, right here," and he placed his phone in front of Agent [MS]. The accused showed Agent [MS] messages between the accused and LCpl [DW] on the Facebook Messenger application. Agent [MS] picked up the accused's phone and read the messages. Within the messages in the Facebook Messenger application were screenshots that LCpl [DW] sent to the accused.

The accused did not show Agent [MS] anything from the images or photographs folder on his cell phone.

At various moments . . . the accused read aloud from and referenced messages from the Facebook Messenger application on his cell phone

. . . .

Agent [MS] [said] "Alright so what I'd like to do, if it's OK with you, I'd like to get those texts from him because that shows that he like asked for the security questions and stuff. Are you OK with me like getting that information from you?"

Accused [replied,] "I don't care."

Agent [MS] [then said,] "OK. Alright, the way we do it, we have a form right here. I just need some initials from you."

Agent [MS] placed in front of the accused a document titled, "Permissive Authorization for Search and Seizure" (PASS). . . .

After initialing a few places . . . the accused stated, "The only way I f[***]in used [to] like communicate with [LCpl DW] was through Facebook because like there's no service over in Romania."

Although this was the first explicit reference to Facebook during the interview, Agent [MS] knew that the messages de-

scribed and showed to him by the accused were from the Facebook Messenger application.

Agent [MS] did not respond in any way to the accused's statement about only communicating with LCpl [DW] via Facebook. Instead, Agent [MS] immediately continued with the PASS, stating, "OK, so, I need your initials before the F in 'fraud' and after the Y in 'larceny.' That's obviously what we're investigating here."

. . . .

. . . Agent [MS] [later] asked the accused, "Why did you give your security question answers to LCpl [DW]?" The accused answered, "Because according to the Facebook messages, his father needed access like [to] my bank account So he could reimburse me for the money I gave to [LCpl DW]."⁹

Agent MS could only vaguely describe the two images he initially observed. "He described the images as depicting full frontal nudity of two girls of an estimated age of seven to eight years, with no breast development or pubic hair."¹⁰ Special Agent SI erroneously testified that after she confirmed that "several" of the images that Agent MS showed her were in fact child pornography, she obtained a CASS from Appellee's commanding officer before she interviewed Appellee.¹¹ In fact, Special Agent SI interviewed Appellee on 4 December 2018, obtained a confession for possessing child pornography and sexually abusing his four-year-old nephew, and obtained a PASS to search Appellee's barracks room and seize and search his laptop three days before asking Appellee's commanding officer for a CASS on 7 December 2018.¹² Additionally, in her affidavit in support of her request for a CASS, she generally relied upon the images discovered by Agent MS but described in detail *four* images.¹³

The military judge suppressed Appellee's admissions and all evidence obtained from Appellee's cell phone beyond the two images initially observed by

⁹ App. Ex. VIII at 2-3, 7 (paragraph numbers omitted) (final ellipsis in original).

¹⁰ *Id.* at 8.

¹¹ *Id.* at 11; Record at 79-80

¹² App. Ex. VIII at 11.

¹³ *Id.*

Agent MS.¹⁴ He determined that a reasonable observer would have understood the scope of Appellee's consent to search to extend only to the messages between Appellee and LCpl DW from the Facebook Messenger application. The military judge ruled that Agent MS exceeded the scope of consent when he searched the images folder of the UFED report. Therefore, that search was unlawful and the suspected images of child pornography he discovered in the images folder were not in plain view. The military judge ruled that NCIS continued the illegal search and that even if Agent MS found the initial images in plain view, the follow-on actions of NCIS were not done to merely confirm the nature of the images but to expand the scope of the search by identifying several additional suspect images. Immediately after NCIS discovered additional images of suspected child pornography, Appellee was brought in for questioning and admitted to possessing child pornography and to sexually abusing his nephew. However, the military judge ruled that Appellee would not have made these confessions if he had not been confronted with the illegally obtained evidence. The military judge, *sua sponte*, determined that the evidence of suspected child pornography found on Appellee's phone would not have been inevitably discovered because at the time of the unlawful searches, law enforcement was not pursuing any leads or evidence that would have inevitably led to the discovery of the images in a lawful manner. Finally, after balancing the deterrence of future unlawful searches or seizures against the costs to the military justice system of excluding the evidence, the military judge found that exclusion of the two images unlawfully discovered by Agent MS would not appreciably deter future unlawful searches.¹⁵ However, with respect to the additional evidence discovered by Special Agent SI, the military judge found that Special Agent SI compounded Agent MS's unlawful conduct and that resulted in recurring negligence, at best, that must be deterred even at high cost to the justice system. Upon balancing, he found that the appreciable deterrence of further unlawful searches or seizures and the benefits of such deterrence outweigh the costs to the justice system.

¹⁴ *Id.*

¹⁵ This aspect of the military judge's ruling does not exclude evidence that is substantial proof of a fact material in the proceeding. Accordingly, we view this part of the military judge's ruling as not subject to the Government's appeal under Article 62(a)(1)(B), UCMJ, and therefore not an issue before this Court.

II. DISCUSSION

A. Standard of Review

In this appeal, we may act only with respect to matters of law. Article 62(b), UCMJ; Rule for Courts-Martial 908(c)(2). We review a military judge's ruling on a motion to suppress evidence for an abuse of discretion. *United States v. Keefauver*, 74 M.J. 230, 233 (C.A.A.F. 2015). We are bound by the military judge's factual determinations unless they are clearly erroneous, but we conduct a de novo review of conclusions of law. *Id.* “[W]e consider the evidence in the light most favorable to the prevailing party.” *Id.* (alteration in original) (quoting *United States v. Reister*, 44 M.J. 409, 413 (C.A.A.F. 1996)).

The military judge's findings of fact are well supported by the record. Neither the Government, nor the Defense contend otherwise, and we use those findings for purposes of our analysis. We do not add findings of fact or substitute our own interpretation of what happened—we merely apply the appropriate legal tests to the facts established by the military judge.

“The abuse of discretion standard is a strict one, calling for more than a mere difference of opinion. The challenged action must be arbitrary, fanciful, clearly unreasonable, or clearly erroneous.” *United States v. McElhaney*, 54 M.J. 120, 130 (C.A.A.F. 2000) (citation and internal quotation marks omitted). Applying this standard of review, we affirm the military judge's ruling for the reasons explained below.

B. Applicable Law of Search and Seizure

The Fourth Amendment guarantees “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures” U.S. CONST. amend IV. A warrantless search is “per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.” *Katz v. United States*, 389 U.S. 347, 357 (1967). Data stored within a cell phone falls within the Fourth Amendment's protection. *United States v. Wicks*, 73 M.J. 93, 99 (C.A.A.F. 2014). Evidence obtained from a government search of cell phone data generally will be inadmissible unless the search was conducted pursuant to a search authorization or a recognized exception to that requirement. *Id.* Voluntary consent to search is one recognized exception to the warrant requirement. *Schneckloth v. Bustamonte*, 412 U.S. 218 (1973).

1. Scope of search

The Government contends that Appellee gave consent to an expansive, general search of his entire phone. Appellee, on the other hand, contends that

he limited the scope of his consent to only the Facebook messages between LCpl DW and himself.

While “[t]he scope of a search is generally defined by its expressed object,” it cannot exceed the scope of the actual consent given. *Florida v. Jimeno*, 500 U.S. 248, 251 (1991) (citing *United States v. Ross*, 456 U.S. 798, (1982)). “The standard for measuring the scope of a suspect’s consent . . . is that of ‘objective’ reasonableness—what would the typical reasonable person have understood by the exchange between the officer and the suspect?” *Id.* A person giving consent to search may limit his consent by placing limitations on “time, place, or property.” Mil. R. Evid. 314(e)(3). While a person’s subjective intent to limit the scope does not control alone, “investigators [must] account for any express or implied limitations on a consent to search.” *United States v. Wallace*, 66 M.J. 5, 8 (C.A.A.F. 2008). The Government must prove consent by clear and convincing evidence. Mil. R. Evid. 314(e)(5).

The scope of consent given by Appellee is determined by “objective reasonableness”—what “the typical reasonable person” would have understood by the entire dialogue and interaction between Agent MS and Appellee. *Jimeno*, 500 U.S. at 251.

The Government relies on *United States v. Wallace*, 66 M.J. 5 (C.A.A.F. 2008), and *United States v. Spinoza*, No. 201700236, 2019 CCA LEXIS 40 (N-M. Ct. Crim. App. 4 Feb 2019) (unpub. op.), *review denied*, 79 M.J. 137 (C.A.A.F. 2019), to argue that because Appellee signed the PASS, he consented to a broad general search of his cell phone data. In *Wallace*, the accused signed a PASS that allowed agents to search and seize his computer. The accused argued that he gave his consent while he was under the impression that agents would only take copies of certain emails between himself and the child victim. The agents informed Staff Sergeant Wallace that they intended to search his computer for evidence. There is no mention of any contemporaneous statements by the accused and the Court of Appeals for the Armed Forces [CAAF] in *Wallace* notes that the accused’s “supposed impression” does not control the objective reasonableness of his consent. The CAAF relied on the express language of the PASS to find that the accused had in fact consented to a broad search and that a reasonable person could conclude that the accused consented to search and seizure, to include removal of the accused’s computer. Moreover, *Wallace* did not hinge on the scope of consent issue. Rather, the case was decided on the inevitable discovery doctrine. The CAAF found that the evidence in question would have been inevitably discovered even after the accused withdrew his consent because government agents had probable cause, prior to the accused’s consent, to obtain command authorization to conduct a broad, general search of the computer. *Wallace*, 66 M.J. at 15-16.

In an unpublished opinion, *Spinoza*, this Court found that the search of Lieutenant [LT] Spinoza's cell phone was reasonable pursuant to a PASS and in light of the contemporaneous discussion between the accused and an NCIS special agent. The NCIS special agent explained that he intended to look for digital evidence of the relationship between LT Spinoza and his accuser, including information contained in applications on his phone and anything that pertained to the investigation. Although no evidence was discovered pertaining to the initial accuser, evidence of misconduct was discovered in texts with another person. We found that it was reasonable for the special agent to search for witnesses through text conversations that occurred during the specific period alleged by LT Spinoza's accuser. We rejected LT Spinoza's subjective belief that he limited the scope of his consent to only his communications with his accuser. Considering the PASS in light of the entire discussion between LT Spinoza and the special agent, we concluded that the search occurred within the scope of the consent granted by LT Spinoza. *Spinoza*, 2019 CCA LEXIS 40 at *18-19.

In another unpublished opinion of this Court, *United States v. Gitto*, No. 201800164, 2019 CCA LEXIS 6 (N-M. Ct. Crim. App. 8 Jan 2019) (unpub. op.), we also found that the accused consented to a broad search because of the dialogue between LCpl Gitto and NCIS special agents while discussing the PASS to search his cell phone. LCpl Gitto approached NCIS as a victim of extortion by a former sexual partner. He consented to an NCIS search of his cell phone that revealed evidence of LCpl Gitto's sexual relationship with a minor. During discussions prior to signing the PASS, two NCIS special agents briefly explained the "breadth of the search" they expected to conduct, to include "dump[ing] everything on the phone" and taking all the data, text messages, photographs, and videos. *Id.* at 22-24. The NCIS special agents also explained that if they encountered any sexually explicit photos, they would report that to LCpl Gitto's chain of command. *Id.* at 23. Finally, the special agents explained, "they would have to investigate further if they found any evidence of child pornography or murder." *Id.* at 23. Based on the PASS and the entire exchange between LCpl Gitto and the agents, this Court found that a reasonable observer would expect the agent to perform a thorough search of all of the cell phone data and "investigate any new-discovered illegality—especially child sex offenses—as he warned he would do." *Id.* at 24.

The Air Force Court of Criminal Appeals [AFCCA] considered similar circumstances in *United States v. Osorio*, 66 M.J. 632 (A.F. Ct. Crim. App. 2008). Air Force Office of Special Investigations (OSI) agents were investigating a sexual assault that occurred at a party that Senior Airman [SrA] Osorio attended. SrA Osorio was not a suspect, but he had taken photos at the party and OSI agents wanted to get that evidence from his laptop. SrA Osorio voluntarily brought his external hard drive to OSI and signed a PASS. The

AFCCA found that the PASS was broad and expansive, but the entire interaction between SrA Osorio and the agents showed that consent was limited to the party photos taken on the day of the party.

The Government argues that similar to *Wallace*, the PASS was clear and expansive and that we should find that Appellee, like Staff Sergeant Wallace, consented to a broad, general search of all of his cell phone data. We disagree. Because there was no additional dialogue between the agents and Staff Sergeant Wallace to better inform the scope of consent, the PASS in that case was the only evidence regarding the scope of consent. The CAAF noted nothing contradictory to the standard boilerplate language of the PASS other than Staff Sergeant Wallace's mistaken impression of what the agents intended to do. *Wallace*, 66 M.J. at 7-8. In this case, there is much more than the mere subjective impression of Appellee. There was a running dialogue in which Appellee said, "I'm going to show you a text message"; Agent MS asked Appellee for "those texts" and "that information" that he had been shown; Appellee responded that he did not care; and then during their review of the PASS, Appellee explicitly stated that he only used Facebook Messenger to communicate with LCpl DW. Finally, when asked why he gave LCpl DW his security information, Appellee reiterated, "[A]ccording to the Facebook messages, his father needed access like to my bank account . . . [s]o he could reimburse me for the money." Agent MS only asked for "those texts" and "that information" that Appellee had shown him, he did not account for this "express or implied limitation" on Appellee's consent, and as he testified, he already knew the only evidence he was looking for came from the Facebook Messenger application.

The Government also asserts that *Spinoza* should lead us to find Appellee consented to a general search of his phone because we rejected LT Spinoza's subjective belief that he was limiting the scope of his consent to only his texts with his accuser. We disagree. LT Spinoza asked the NCIS special agent if he was just going to look at the text messages between LT Spinoza and his accuser, and the special agent informed LT Spinoza of the wide breadth of the search he intended to conduct, to include searching the applications and texts on his phone for "any evidence." *Spinoza*, 2019 CCA LEXIS 40, at *16-17. Even though the agent was only able to search the text message exchanges manually, he specifically limited his search to the period alleged by LT Spinoza's accuser when he found incriminating evidence regarding a second alleged victim. Here, while Agent MS did not tell Appellee how or where he would be searching, he said he only wanted to get "those texts" and "that information," meaning the messages he was shown by Appellee. Agent MS knew the text message exchange he wanted occurred in the Facebook Messenger application even before Appellee specifically told him so. Also, in *Spinoza*, the agent had to scroll through the text messages on the actual phone

because the UFED software did not produce usable information. Whereas the agent in *Spinoza* lawfully found incriminating text messages on LT Spinoza's phone in the text message application where he was most likely to find text messages, Agent MS did not find the evidence he was looking for while searching for the messages in the SMS and MMS folders. He only found the suspect images while searching in a place where the messages and their embedded screenshots would *not* reasonably be found: the images folder. When Agent MS was not able to find the Facebook message exchange that he had been shown, rather than stop and ask Appellee for his phone so he could conduct a manual search of the Facebook Messenger application or find some other reasonable way to limit his search to what Appellee had consented to, Agent MS decided to rummage through more than 43,000 images.

Unlike the agents in *Spinoza* and *Gitto*, Agent MS did not explain or inform Appellee that he intended to conduct a thorough search for digital evidence of "anything that pertains to the investigation," not just Facebook messages between LCpl DW and Appellee. When Appellee reiterated that he communicated with LCpl DW only using Facebook while in Romania, Agent MS did not disavow that he would only be looking at "those texts" and "that information." Instead, Agent MS simply did not respond and proceeded to instruct Appellee where to initial the PASS.

Like *Wallace*, *Spinoza*, *Gitto*, and *Otorio*, the PASS was broad and expansive and authorized the search of Appellee's "Android ZTE Axon 7 mini." However, as explained in those opinions, the PASS must be considered in light of the entire conversation between Appellee and Agent MS. Neither the subjective intentions of Appellee nor the boilerplate language of the PASS solely control the scope of consent. Rather, it is the objective reasonableness determined by "what would the typical reasonable person have understood by the exchange between" Agent MS and Appellee. *Wallace*, 66 M.J. at 8.

Although law enforcement agents are not required to explain the technical details of how a cell phone search will be conducted, the explanation, or the lack of one, is considered in determining what a reasonable person would conclude about the scope of consent. In this case, Agent MS did not indicate that he would be looking through all of the data on Appellee's phone. To the contrary, the only evidence of Agent MS's intent was that he requested to get "those texts" and "that information" regarding the Facebook message exchanges that Appellee had shown him. The entire conversation between Agent MS and Appellee before and during review of the PASS would lead a reasonable person to think that Appellee consented to searching his phone for the Facebook messages that he showed Agent MS. It did not authorize a broad general search of his entire phone data, and the Government did not prove otherwise by clear and convincing evidence.

2. Unlawful search

Whereas the Government concedes the search conducted by Special Agent SI was unlawful, they argue it was reasonable for Agent MS to look in the images folder because Appellee showed him Facebook messages that contained screenshots and screenshots might be found in the images folder. *See United States v. Richards*, 76 M.J. 365, 379 (C.A.A.F. 2017) (“[T]here may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders, and that is true whether the search is of a computer file or physical files. It is particularly true with image files.”). We disagree for multiple reasons.

Agent MS did not look in any folder named “facebook” or even attempt to filter the data with the term “facebook.” However, we find that his initial investigative path was reasonable because he first looked in the SMS folder which contained text only files and would potentially contain any text messages between Appellee and LCpl DW even though it would not contain any screenshots. In fact, Agent MS found some recent text messages between the two Marines but they were not the Facebook messages he was looking for. Rather, they were basic telephone number based text messages. Because the UFED report does not separate messages by their source application, it was somewhat reasonable, at this point, for Agent MS to look in the SMS folder for the messages between Appellee and LCpl DW. Not finding the messages he was looking for in the SMS folder, Agent MS next looked in the MMS folder where mixed text and media files are located. Even though he did not find any messages between Appellee and LCpl DW in the MMS folder, it was logically reasonable to look in that folder because the specific messages he was looking for contained both text and media (screenshots).

Agent MS’s investigative action became unreasonable when he decided to look through over 43,000 thumbnail images in hopes of finding just the screenshots that Appellee had shown him in the Facebook Messenger application on his phone. Rummaging through the images folder would be reasonable only if Appellee had taken the screenshots of his own screen or if he had manually saved the individual screenshots as images. However, Agent MS knew that Appellee received, not sent, the screenshots images. Even if there was some illogical way that the screenshots ended up in the images folder, there was no reason for Agent MS to believe screenshots embedded in text messages would appear in the images folder. Agent MS testified that Appellee did not open the photos folder on his phone and show him anything. He knew the messages he saw were from the Facebook Messenger application and not Appellee’s photos or images folder. Moreover, Agent MS was not looking for just the screenshots alone. He wanted the messages *with* their embedded screenshots because they showed the complete picture of how LCpl DW was able to get Appellee’s financial information. Since he already was

unable to find just the text only parts of the messages he wanted, the screenshots alone would not be sufficient evidence and searching for just the screenshots was unreasonable given the scope of consent. Further, Agent MS had other “practical substitutes” available in lieu of conducting the sort of “free-for-all general search[] the Fourth amendment was designed to prevent.” *Id.* He could have asked Appellee for his phone so that, as the agent did in *Spinoza*, he could manually search for the Facebook Messages he was seeking. He also could have just asked Appellee for additional authorization to look in the images folder of the UFED report. Instead, he decided to painstakingly scroll through 43,000 images hoping to find Facebook messages and embedded screenshots that would not logically be found in the images folder of the UFED report. We find this free-for-all general search to be unreasonable given the circumstances. Agent MS exceeded the scope of Appellee’s consent, and to the extent the search went beyond that consent, it was unlawful.

3. Plain view

“Law enforcement officials conducting a lawful search may seize items in plain view if [the officials] are acting within the scope of their authority, and . . . they have probable cause to believe the item is contraband or evidence of a crime.” *United States v. McMahon*, 58 MJ 362, 367 (C.A.A.F. 2003) (alterations in original) (citation and internal quotation marks omitted). Evidence may be seized when “[t]he person while in the course of otherwise lawful activity observes in a reasonable fashion property or evidence that the person has probable cause to seize.” Mil. R. Evid. 316(c)(5)(C). “[I]n order for the plain view exception to apply: (1) the officer must not violate the Fourth Amendment in arriving at the spot from which the incriminating materials can be plainly viewed; (2) the incriminating character of the materials must be immediately apparent; and (3) the officer must have lawful access to the object itself.” *Richards*, 76 M.J. at 371 (citing *Horton v. California*, 496 U.S. 128, 136-37 (1990)).

The Government argues that the images of suspected child pornography were in plain view because they were present in a folder reasonably containing screenshots. As we determined above, Agent MS exceeded the scope of Appellee’s consent when he bypassed other practical and lawful alternatives and elected to search through over 43,000 thumbnail images for messages with embedded screenshots that Appellee had already shown him were easily accessible on the phone itself. When Agent MS began looking for Facebook messages in the images folder, he exceeded Appellee’s scope of consent and “violate[d] the Fourth Amendment in arriving at the spot from which the incriminating materials [could] be plainly viewed.” *Id.* Thus, Agent MS was not acting “in the course of . . . lawful activity” when he discovered the two images of suspected child pornography. Since the plain view doctrine requires that

law-enforcement agents be acting within the scope of the authorization at the time of discovery, the doctrine is inapplicable under the facts of this case.

4. Exclusionary rule

“Evidence obtained as a result of an unlawful search or seizure made by a person acting in a governmental capacity is inadmissible” if there is a timely motion to suppress, the accused had a reasonable expectation of privacy in the property searched, and “exclusion of the evidence results in appreciable deterrence of future unlawful searches or seizures and the benefits of such deterrence outweigh the costs to the justice system.” Mil. R. Evid. 311(a).

As discussed above, the images of suspected child pornography observed by Agent MS and Special Agent SI were obtained as a result of an unlawful search by persons acting in a governmental capacity. Appellee had a reasonable expectation of privacy in the contents of his cell phone, and he made a timely motion to suppress.

The issue here is whether exclusion will result in deterrence of future unlawful searches and whether the benefits of such deterrence outweigh the cost to the military justice system. The cost to the military justice system is that the guilty may go free. *See Herring v. United States*, 555 U.S. 135, 141 (2009). The military judge balanced these competing interests and found that excluding the two images discovered by Agent MS would not deter future unlawful searches because Agent MS’s conduct amounted to simple negligence, and exclusion in the face of marginal deterrent effect would not outweigh the cost to the justice system.¹⁶ However, the military judge concluded the same was not true for the continued search of Appellee’s cell phone data by Special Agent SI. Special Agent SI compounded the already unlawful search by specifically searching for child pornography and then exploiting the unlawfully obtained evidence to obtain admissions from the accused. Whereas Agent MS initially strayed into areas where he was not authorized to search, Special Agent SI, an experienced and educated NCIS special agent, should have known or ascertained the original object of the search to avoid such scope of consent issues, and yet she chose to expand an already precarious search. She then exploited the fruits of her recurring, unlawful, and at least negligent search to obtain confessions from Appellee and a command authorization from Appellee’s commanding officer. We find that when a victim of a crime

¹⁶ As stated above, because this aspect of the military judge’s ruling does not exclude evidence that is substantial proof of a fact material in the proceeding, we view this part of the military judge’s ruling as not subject to the Government’s appeal under Article 62(a)(1)(B), UCMJ, and therefore not an issue before this Court.

approaches law enforcement with specific evidence to support their allegations and law enforcement then unnecessarily and illegally obtains other evidence and exploits that evidence against the victim, strong deterrence is warranted to prevent the chilling effect on victims and their willingness to report crime and cooperate with law enforcement. We affirm the military judge's decision to apply the exclusionary rule and suppress all images beyond the two images negligently discovered by Agent MS. The military judge applied the correct test and determined that based on this recurring negligent police conduct the appreciable deterrence of future unlawful searches outweighs the cost to the military justice system. We agree and find that the military judge's ruling was reasonable and not an abuse of discretion.

5. Inevitable discovery doctrine

The Government now contends that the military judge erred by not applying the inevitable discovery exception to the exclusionary rule under Military Rule of Evidence 311.¹⁷ “To take advantage of [the inevitable discovery] doctrine, the prosecution must establish, by a preponderance of the evidence, ‘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. Hoffmann*, 75 M.J. 120, 124-25 (C.A.A.F. 2016) (emphasis in original) (quoting *United States v. Dease*, 71 M.J. 116, 122 (C.A.A.F. 2012)).

Agent MS did not suspect Appellee of any crime or see any contraband while operating within the scope of the consent to search granted by Appellee. Agent MS found suspicious images only after unlawfully exceeding the scope of consent. At the last point where Agent MS was operating within the scope of consent granted by Appellee, there was no probable cause to justify a command authorization to search and seize evidence of a crime from Appellee's cell phone. Therefore, there was no real possibility that law enforcement agents would have otherwise discovered the images of suspected child pornography on Appellee's phone. This applies to the evidence found first by Agent MS and to the follow-on evidence found by Special Agent SI. There is no evidence in the record that “the government agents possessed, or were ac-

¹⁷ The Defense briefed the issue in their Motion to Suppress, App. Ex. III, and argued the issue before the military judge. The Government, on the other hand, did not address the issue in their response, App. Ex. IV, nor argue the issue before the military judge.

tively pursuing, evidence or leads that would have inevitably led to the” lawful discovery of that evidence. *Id.*

The Government argues that Agent MS discovered the two initial images of suspected child pornography in plain view; thus, the exclusionary rule should not apply in this case because the evidence found by Special Agent SI would have been inevitably discovered. We disagree. As discussed above, when Agent MS began looking for Facebook messages in the images folder, he exceeded Appellee’s scope of consent and was therefore not acting “in the course of . . . lawful activity” when he discovered the images at issue, the doctrine of plain view is inapplicable under the facts of this case. Even if we were to sanction Agent MS’s discovery of the two images as occurring in plain view, the ensuing handoff to NCIS was so abysmally handled that we would still find the follow-on search to be illegal, as the Government concedes, and apply the exclusionary rule to the evidence.

When Agent MS discovered what he thought might be child pornography, he stopped his search and contacted NCIS because child pornography is in their investigative purview. That was the right decision. Ideally, Agent MS should have frozen the scene, documented the computer screen with pictures or photo names and numbers, called NCIS to come and verify what he just viewed, and then NCIS should have taken the lead and contacted the Staff Judge Advocate to coordinate obtaining an immediate CASS. Instead, Agent MS called NCIS, set up a meeting for the next day, brought over the UFED report on an external disk and looked through the data with Special Agent SI.

As the Government concedes, this search was illegal, and the Government produced no evidence at all that they possessed “or were actively pursuing, evidence or leads that would have inevitably led to the discovery of the evidence . . . in a lawful manner.” *Hoffmann*, 75 M.J. at 124-125 (citation and internal quotation marks omitted). NCIS obtained a CASS three days later, but it was based on the illegally obtained evidence from Special Agent SI’s exploitation of the illegal search. What NCIS would have done based only on the two images reported by Agent MS is speculative at best, especially since we know what NCIS actually did after Agent MS correctly stopped his investigation and turned it over to Special Agent SI, the head Agent of the NCIS unit tasked with investigating child pornography cases. Rather than merely confirm that the two images identified by Agent MS were possibly child pornography, Special Agent SI conducted her own more expansive search reviewing additional images and eventually listing the details of four images in her affidavit in support of the CASS. The Government produced no other evidence to meet their burden on this issue. For these reasons, even if we found that Agent MS discovered the images in plain view, the inevitable discovery doctrine does not apply to the evidence suppressed by the military judge.

6. *Fruit of the poisonous tree derivative evidence*

“Evidence derivative of an unlawful search, seizure, or interrogation is commonly referred to as the ‘fruit of the poisonous tree’ and is generally not admissible at trial.” *United States v. Conklin*, 63 M.J. 333, 334 (C.A.A.F. 2006). While not all derivative evidence is necessarily inadmissible, that which “come[s] by exploitation of the [law enforcement] illegality” and not “by means sufficiently distinguishable to be purged of the primary taint” is inadmissible. *Wong Sun v. United States*, 371 U.S. 471, 487-88 (1963). Here, the Government concedes that Special Agent SI’s search was unlawful. She then used her knowledge of what she saw on Appellee’s phone to obtain his confession to viewing and possessing child pornography. She then used the connection between child pornography and an inferred sexual interest in children to obtain an admission from Appellee that he recently touched the penis of his four-year-old nephew. Although Appellee made the admission, his phone contained no data regarding the molestation of any child and he would not have even been pressed about his sexual interest in children if it were not for Special Agent SI’s exploitation of the images found during her unlawful search of the phone data.

In *Brown v. Illinois*, 422 U.S. 590 (1975), the Supreme Court used three factors to determine if Miranda warnings were sufficient to remove the taint of an illegal search on a confession. The CAAF has used the framework to consider whether consent to search was obtained by exploitation of an unlawful search. *United States v. Khamsovuk*, 57 M.J. 282, 290 (C.A.A.F. 2002). “[T]he question of whether such a confession is a an act of free will must be answered on the facts of each case looking at the 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.” *Conklin*, 63 M.J. at 338 (citing *Brown*, 422 U.S. at 603-04).

Applying the *Brown* three-prong test to the facts of this case, we determine that all three prongs favor Appellee. First, the illegal search of the cell phone data was close in time to the NCIS actions that led to Appellee’s admissions. Appellee was interrogated, made admissions, and consented to further searches within hours of Special Agent SI’s unlawful search while reviewing the UFED report with Agent MS. Second, there were no intervening circumstances sufficient to remove the taint from the initial illegal search. Special Agent SI “would not have been interested in talking to [Appellee] but for the information” obtained as a result of the unlawful search that had just taken place. *See id.* at 339. “There were no intervening events or circumstances that would sever the causal connection between the” illegal search and Appellee’s admissions. *Id.* The third factor requires examination of the Government’s conduct. Agent MS’s actions were improper because he knew exactly what messages he wanted and yet chose to explore areas of the UFED

report well beyond where the Facebook messages and their embedded screenshots would reasonably be found when he had other lawful options. Special Agent SI continued the unlawful search and further exceeded the scope of consent by searching for possible child pornography and expanding additional thumbnails in addition to those reported by Agent MS. Special Agent SI did not merely confirm that what Agent MS discovered was likely child pornography; she engaged in her own search of the data to discover several images that she suspected were child pornography and she expanded those images to confirm her own suspicions. Special Agent SI also had other options to include stopping the search after becoming aware of the suspicious images and seeking broader search authorization from either Appellee or from a command search authority.

Applying the *Brown* framework to the facts of this case, we conclude that Appellee's confession and additional consent to search were not sufficiently attenuated from the taint of the illegal search of Appellee's cell phone data first by Agent MS and then by Special Agent SI. But for Special Agent SI's exploitation of the illegally obtained evidence, Appellee would not have admitted to the misconduct. Therefore, Appellee's admissions and consent to other searches while under interrogation by Special Agent SI are derivative of the unlawful search of his phone data.

Finally, we conclude the results of the subsequent command-authorized search of Appellee's phone are also fruit of the same poisonous tree and must be suppressed. Special Agent SI sought and received the CASS for this search based on the images she had already unlawfully obtained from Appellee's phone. This derivative evidence was obtained by exploitation of the earlier illegality and not "by means sufficiently distinguishable to be purged of the primary taint." *Wong Sun*, 371 U.S. at 487-88. It is therefore inadmissible.

C. The Military Judge Did Not Abuse His Discretion

The military judge issued written findings of fact supported by the record, not clearly erroneous, and uncontroverted by either party. The military judge applied the correct legal principles to the facts before him and issued a detailed written ruling. "The abuse of discretion standard is a strict one, calling for more than a mere difference of opinion. The challenged action must be arbitrary, fanciful, clearly unreasonable, or clearly erroneous." *McElhaney*, 54 M.J. at 130 (citation and internal quotation marks omitted). We do not ask whether we "might disagree with the trial court's findings, but whether those findings are 'fairly supported by the record.'" *United States v. Burris*, 21 M.J. 140, 144 (C.M.A. 1985) (quoting *Marshall v. Lonberger*, 459 U.S. 422, 432, (1983)). Applying this standard of review, we find that the military judge did not abuse his discretion and we uphold his ruling.

III. CONCLUSION

After carefully considering the military judge's findings of fact, principles of law, and conclusions of law, the appeal of the United States is hereby **DENIED**. The military judge's ruling is affirmed and the record of trial is returned to the Judge Advocate General for remand to the convening authority and delivery to the military judge for further proceedings.

Chief Judge CRISFIELD and Judge GASTON concur.



FOR THE COURT:

A handwritten signature in blue ink, reading "Rodger A. Drew, Jr.", is written over the typed name.

RODGER A. DREW, JR.
Clerk of Court