UNITED STATES ARMY COURT OF CRIMINAL APPEALS

Before
CAMPANELLA, BURTON, and SALUSSOLIA
Appellate Military Judges

UNITED STATES, Appellee
v.
Private First Class JONATHAN P. MORALES
United States Army, Appellant

ARMY 20150498

Headquarters, Fort Bragg
Deidra J. Fleming, Military Judge
Colonel Michael O. Lacey, Staff Judge Advocate

For Appellant: Captain Joshua B. Fix, JA (argued); Lieutenant Colonel Christopher D. Carrier, JA; Major Andres Vazquez, Jr., JA; Captain Matthew D. Bernstein, JA (on brief); Lieutenant Colonel Melissa R. Covolesky, JA; Captain Katherine L. DePaul, JA; Captain Matthew D. Bernstein, JA (on brief in response to specified issues); Captain Cody D. Cheek, JA.

For Appellee: Captain Austin L. Fenwick, JA (argued); Colonel Mark H. Sydenham, JA; Lieutenant Colonel A.G. Courie III, JA; Major Cormac M. Smith, JA; Captain John Gardella, JA (on brief and brief in response to specified issues); Major Michael E. Korte, JA.

13 December 2017

OPINION OF THE COURT

CAMPANELLA, Senior Judge:

The Fourth Amendment and Rules for Courts-Martial protect soldiers against unreasonable searches and seizures. Here, it was unreasonable for law enforcement to search the entire contents of appellant's cell phone even though the search was conducted pursuant to a search authorization. A search and seizure conducted pursuant to a search authorization can still be unreasonable if the search and seizure are not supported by probable cause. While appellant's phone was lawfully seized, the information presented to a military magistrate only provided probable cause to search the phone for text messages. Thus, a search for photographs on the phone, which revealed digital photographs of appellant's crime, was unreasonable. We therefore conclude the military judge abused her discretion at trial by not granting a

defense motion to suppress these digital photographs. We also hold that the good faith exception and plain view doctrine do not apply to save the fruits of the government's unreasonable and unlawful search.

A panel composed of officer and enlisted members sitting as a general court-martial convicted appellant, contrary to his pleas, of abusive sexual contact, indecent viewing, and indecent recording, in violation of Articles 120 and 120c, Uniform Code of Military Justice, 10 U.S.C. §§ 920, 920c (2012 & Supp. I 2014). The convening authority approved the adjudged sentence of a bad-conduct discharge and confinement for eighteen months.

We review this case under Article 66, UCMJ. Upon consideration of the matters personally raised by appellant pursuant to *United States v. Grostefon*, 12 M.J. 431 (C.M.A. 1982), that the military judge abused her discretion by denying the defense motion to suppress, this court specified issues pertaining to the lawfulness of the government's search and the military judge's discretion. Oral argument was subsequently held on these issues.[1] Given our findings with regard to the issues specified in this case, we do not make a determination regarding any other allegations of error.

BACKGROUND

Specialist AC's Report to Law Enforcement

On 11 February 2014, Specialist (SPC) AC reported to law enforcement that appellant sexually assaulted her. Specialist AC stated she and appellant were close friends and it was common for him to stay at her off-post house. It was also common for appellant to give SPC AC body massages. Specialist AC, however, had made it clear to appellant they were just friends and she was not interested in a sexual relationship.

On 9 February 2014, appellant spent the night at SPC AC's house. Specialist AC took cold medication before going to bed. After SPC AC laid down to go to sleep, appellant began massaging her legs. According to SPC AC, she fell asleep and woke up when appellant penetrated her vagina with his fingers. Upon awakening, she confronted him and asked what he was doing. He apologized and left the room.

[1] Oral argument in this case was heard in Los Angeles, California on 27 September 2017 at the University of Southern California Gould School of Law as part of the Outreach Program of the United States Army Court of Criminal Appeals.

Shortly after he left, SPC AC sent appellant text messages at 0026, 10 February 2014, expressing her discomfort and telling him he had "crossed the line." He responded via text stating he thought she was awake during the massage, but also admitted he had touched her really close to her genitalia.

During the investigation, SPC AC provided Special Agent (SA) Rachel Grawn screen shots of the entire text message conversation.

During her interview, SPC AC also reported that a month prior, she confronted appellant after seeing a nude photograph of herself on appellant's phone. She had not given the photo to appellant and recognized the photograph as a personal one saved on her laptop. When confronted, appellant admitted to her he had transferred the image from her laptop to his cellphone using a USB connection. She returned the phone to appellant and told him to delete the image.

Application for the Search Authorization

Based on SPC AC's report, SA Grawn sought a search authorization to search appellant's phone. Special Agent Grawn presented Captain NM, a part-time military magistrate, with a request for a search authorization and a supporting affidavit that was incorporated by reference into the authorization. Special Agent Grawn's affidavit stated appellant was being investigated for sexual assault and the offense of indecent viewing, visual recording or broadcasting, against SPC AC–offenses alleged to have occurred between 9 - 10 February 2014. Notably, the affidavit did not mention the photograph SPC AC saw on appellant's phone.

The authorization provided a summary of SPC AC's interview prepared by SA Grawn. The summary included the text message conversation between SPC AC and appellant at 0026, 10 February 2014, which read:

> [SPC AC:] Idk what or how to say this really . . . I don't want you to respond or come try to talk to me . . . I feel like you crossed the line and have made me uncomfortable . . . I was sound asleep once you started to massage my legs . . . I don't know why or what woke me up . . . but I felt like you were taking advantage of me sleeping not thinking I would wake up with all the meds in my system . . . I felt your hands on and extremely to close to my vag . . . I feel like if I wouldn't have woken up you would have tried to do more . . . please don't ever touch me again . . . and maybe I'm over thinking but I honestly don't feel like I am . . . I don't understand what you think or don't understand about friends only . . . if this makes you mad or upset I'm sorry but this is how I feel

> [Appellant] responded to SPC [AC's] text message with the following:
>
> I thought you were still awake I'm sorry I do admit I got really close to your vag and I'm sorry I won't touch you ever again.

The affidavit stated SA Grawn sought:

> [t]o conduct a digital forensic examination of the phone, SIM, and SD Micro Card to include any videos, images, photographs, other graphics, text messages, electronic mail messages, instant messages, short message service (SMS), multimedia message service (MMS), internet data files, deleted files, screen names, email accounts, user names, phone contact lists, calls, electronic account names concerning the exposing, creating, uploading, distributing, sending, deleting of any depiction of SPC AC between the time/date group 0000, 9 F[e]b 14 and 0900, 25 Feb 14.

Special Agent Grawn requested a search authorization for "Personal cellphones, digital media devices, and any other materials that may assist in the resolution of this investigation." The military magistrate struck through the portion of the request regarding "any other materials . . ." on the affidavit and signed the warrant authorizing a search and seizure as follows:

> All [c]ellphones and/or hard drives and any physical evidence concerning digital communication pertaining to the sexual assault of SPC AC, and subsequent digital forensic examination of the collected items.

At the suppression hearing, the military magistrate testified he only considered the affidavit submitted to him by SA Grawn and did not consider verbal communications or other documentation. The military magistrate also acknowledged there was no indication that photos were taken that pertained to the sexual assault; however, there was probable cause to search for images, asserting as follows:

> . . . [T]here was certainly *a possibility that evidence of the alleged crime would be found on the phone and what type of format that evidence may take certainly could not have ruled out the possibility of evidence of the crime being in the form of a photo*, a text message, an SMS, a phone contact, log, registry, e-mail, and things of that nature because the phones, the way they–the way cellphones

> work it enables them to–enables them to transmit that type of data in various format[s].
>
> And there that certainly–while there was no allegation at the time other than the fact that they're–the government appeared to be investigating not only the 120 offense of the digital penetration, but also the broadcasting that *certainly there could be evidence of broadcasting in the form of photos as attachment or something of that nature.* And there had already been communication between [appellant] and the alleged victim on a cellphone. So, it was certainly reason[able] to believe there could be probative evidence on that cellphone that could take the form of any of those various media formats.

(emphasis added).[2]

The Digital Forensic Examination

After seizing appellant's cellphone, SA Grawn provided appellant's phone to SA Jessica Jacob to conduct a digital forensic examination. She also provided SA Jacob with a copy of the search warrant and incorporated affidavit. At the suppression hearing, SA Jacob testified she only reviewed the warrant and did not read the incorporated affidavit describing the crimes being investigated.

Special Agent Jacob believed the warrant allowed her to search all the contents of the device and as a result, she placed no limitations on her search and extracted all the data from the phone. This is critical to our plain view determination because it means that SA Jacob actually searched for pictures, not that she happened upon them later.

Special Agent Jacob explained a search of a phone occurs in two steps. First, data is extracted two separate times using two different forensic software programs, Lantern and Cellebrite. According to SA Jacob, Lantern has the ability to discriminate among data types and can therefore limit the extraction to categories of information such as text messages, images, videos, media, etc. Cellebrite does not

[2] Although we quote the magistrate's testimony at the suppression hearing extensively, our analysis relies on the facts of his statements rather than his opinions. We cite his views of probable cause to search for photographs to highlight how mistaken the probable cause review was in this case, relying on mere possibilities.

have a similar capability and can only extract all of the data. After the data is extracted, each data set is arranged into a readable format by the respective program, allowing SA Jacob to examine the data.

During the search of appellant's cell phone, SA Jacob found nothing relevant to the investigation using Cellebrite. Although Lantern did not reveal any text messages between appellant and SPC AC on the phone, it did allow SA Jacob to find photographs pertinent to the investigation. Special Agent Jacob extracted all the photographs from the phone and displayed them in a list view with metadata next to each image. The metadata included the time, date, filepath, and GPS information. Among the images, SA Jacob found three photos of a hand grabbing buttocks, pulling the buttocks' cheeks apart, and exposing genitalia. The images were dated 9 February 2014 at 23:49:23, corresponding with the time of the reported assault. Given the report of SPC AC and the date-time stamp of the photographs, the images appear to be of appellant assaulting SPC AC. Special Agent Jacob determined the three images were originally located within a photo editing application, PicSayPro, before being extracted and placed in a list view. Special Agent Jacob was also able to determine the three pictures in question had not been uploaded or transmitted to anyone.

The Military Judge's Analysis

In her findings of fact and conclusions of law, the military judge found the magistrate "had probable cause to issue the warrant for the scope he provided in the search affidavit." The military judge determined the warrant was not invalidated by the location where the pictures were seized, namely within the picture-editing application. The military judge found that while the forensic examination exceeded the scope of the search contemplated by the magistrate, the digital images at issue were found within the scope of what the magistrate believed he was authorizing.

The military judge further held that although the actual search authorization was qualified by the term "digital communication," the pictures were not excluded as a "communication," which focuses on the "process of bringing an idea to another's perception" rather than on the actual transmission of the photographs.

The military judge ruled that even if the search was unreasonable, the good faith exception applied. The military judge acknowledged SA Jacob did not read the entire warrant, but reasoned SA Jacob would have still been objectively reasonable in her execution of the search had she read the accompanying affidavit. Ultimately, the military judge determined this case was a "close call" and resolved it in favor of the magistrate.

On appeal, appellant asserts the military judge abused her discretion by denying his motion to suppress the photographs. We agree.

LAW AND ANALYSIS

We first address whether there was a substantial basis to conclude probable cause existed for the military magistrate to issue a warrant that included a search of appellant's phone for any picture or "depiction" of SPC AC. Although evidence supporting probable cause to search for photographs existed, it was not presented to the magistrate. We therefore hold that the military magistrate did not have a substantial basis to conclude probable cause existed to search for any photographs.

We next address the scope of the magistrate's authorization and conclude the term "digital communication" did not include pictures under the facts of this case.

Finally, we address the good faith and plain view exceptions and find they do not apply.

Standard of Review

We review a military judge's denial of a motion to suppress for an abuse of discretion. *United States v. Nieto*, 76 M.J. 101, 105 (C.A.A.F. 2017) (citing *United States v. Hoffmann*, 75 M.J. 120, 124 (C.A.A.F. 2016)). We review a magistrate's probable cause determination as to whether the military "magistrate had a substantial basis for concluding that probable cause existed." *Id.* (citing *United States v. Rogers*, 67 M.J. 162, 164-65 (C.A.A.F. 2009)). "A magistrate has a substantial basis to issue a warrant when, based on the totality of the circumstances, a common-sense judgment would lead to the conclusion that there is a fair probability that evidence of a crime will be found at the identified location." *Rogers*, 67 M.J. at 165 (citing *Illinois v. Gates*, 462 U.S. 213, 238 (1983); *United States v. Leedy*, 65 M.J. 208, 213 (C.A.A.F. 2007)).

Probable cause requires a *sufficient nexus* between the alleged crime and the item to be seized. *Nieto*, 76 M.J. at 106 (citing *Rogers*, 67 M.J. at 166; *United States v. Gallo*, 55 M.J. 418, 421 (C.A.A.F. 2001)) (emphasis added). "The question of nexus focuses on whether there was a 'fair probability' that contraband or evidence of a crime will be found in a particular place." *United States v. Clayton*, 68 M.J. 419, 424 (C.A.A.F. 2010) (quoting *Leedy*, 65 M.J. at 213). A nexus may "be inferred from the facts and circumstances of a particular case," including the type of crime, the nature of the items sought, and reasonable inferences about where evidence is likely to be kept. *Id.*; *Gallo*, 55 M.J. at 421.

The Military Magistrate's Probable Cause Determination

We find there was probable cause to search for text messages on appellant's phone but no probable cause to look for photographs.

This court gives "'great deference' to the magistrate's probable cause determination because of 'the Fourth Amendment's strong preference for searches conducted pursuant to a warrant.'" *Nieto*, 76 M.J. at 105 (quoting *Gates*, 462 U.S. at 238). "However, this deference is 'not boundless,' and a reviewing court may conclude that 'the magistrate's probable-cause determination reflected an improper analysis of the totality of the circumstances.' *Id.* (quoting *United States v. Leon*, 468 U.S. 897, 915 (1984)). "Sufficient information must be presented to the magistrate to allow that official to determine probable cause; *his action cannot be a mere ratification of the bare conclusions of others*." *Hoffmann*, 75 M.J. at 125-26 (quoting *Gates*, 462 U.S. at 239) (emphasis added). Courts do not view probable cause determinations with hindsight. *Guzman v. City of Chicago*, 565 F.3d 393, 396 (7th Cir. 2009).

The military magistrate based his probable cause determination solely on the four corners of the paperwork presented to him; thus, our review is limited to this same paperwork. The affidavit details SPC AC's account of the sexual assault and appellant's subsequent text message exchange. The search request does not mention appellant's alleged transfer of a nude photograph from SPC AC's laptop without her consent to appellant's phone. While this evidence *could have* formed the basis for probable cause to search the phone for photographs, this information was not conveyed to the military magistrate.

In her affidavit, SA Grawn requests authorization to search for evidence of ". . . any depiction of SPC [AC] between the time/date group 0000, 9 F[e]b 14 and 0900, 25, 25 Feb 14." There are, however, no facts in the affidavit to support this request–only the assertion that probable cause exists to believe evidence of indecent viewing, visual recording, or broadcasting is on appellant's phone. Any reliance on this assertion would be a ratification of a bare conclusion. The request to search appellant's phone for a depiction presupposes that the general nature of sexual assault is such that photographic documentation of this crime would be found on appellant's phone. Our superior court disavowed a similar proposition in *Hoffmann*. 75 M.J. at 126-27. It would be an inferential fallacy to assume without evidence that someone committing sexual assault would also photograph evidence of the crime on their phone. *See Id.* at 127 (quoting *United States v. Falso*, 544 F.3d 110, 122 (2d Cir. 2008)). Here, the facts and circumstances presented to the magistrate do not establish a nexus between photos and the sexual assault. *See Nieto* at 107-08.

Even granting "great deference" to the magistrate, we hold he did not have a substantial basis to determine probable cause existed to believe photographs of the sexual assault would be found on appellant's phone. The only nexus known to the military magistrate between the phone and the sexual assault were appellant's text message admissions. We, therefore, conclude the military magistrate only had a substantial basis for determining that appellant's phone contained text messages

between appellant and SPC AC evidencing the averred sexual assault–not photographs.

The Search Authorization

The Fourth Amendment requires warrants and search authorizations to particularly describe the place to be searched and things to be seized so that the search will be carefully tailored to its justifications. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

The search warrant, probable cause, and particularity requirements serve two constitutional protections:

> First, the magistrate's scrutiny is intended to eliminate altogether searches not based on probable cause. The premise here is that any intrusion in the way of search or seizure is an evil, so that no intrusion at all is justified without a careful prior determination of necessity. The second, distinct objective is that those searches deemed necessary should be as limited as possible. Here, the specific evil is the "general warrant" abhorred by the colonists, and the problem is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings. The warrant accomplishes this second objective by requiring a "particular description" of the things to be seized.

Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971) (internal citations omitted).

"The test for determining the adequacy of the description of the location to be searched is whether the description is sufficient 'to enable the executing officer to locate and identify the premises with reasonable effort, and whether there is any reasonable probability that another premise might be mistakenly searched.'" *United States v. Lora-Solano*, 330 F.3d 1288, 1293 (10th Cir. 2003) (citation omitted). This test "ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *United States v. Richards*, 76 M.J. 365, 369 (C.A.A.F. 2017) (quoting *Garrison*, 480 U.S. at 84).

Today's digital era complicates the application of the Fourth Amendment. With regard to cell phones, the Supreme Court, in *Riley v. California*, instructs: "modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy. . . [as] a significant majority of American adults now own such

phones." 134 S. Ct. 2473, 2484 (2014). The Supreme Court's conclusion is equally forceful: "[m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.' The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." *Id.* at 2494-95.

Here, the government's search authorization runs afoul of the probable cause and particularity requirements of the Fourth Amendment.

The warrant authorized a search and seizure of:

> All [c]ellphones and/or hard drives and any physical evidence concerning digital communication pertaining to the sexual assault of SPC [AC], and subsequent digital forensic examination of the collected items.[3]

The use of the term "digital communication" was imprecise and open to interpretation. Special Agent Grawn admitted when she drafted the warrant to obtain "digital communication" she was referring to text messages between SPC AC and appellant. Despite her intent, SA Grawn used the term "digital communication" in the search authorization rather than text messages. Resultantly, the military magistrate authorized a search for a broader, less precise, category of information, which led to confusion. Regardless of who drafts the authorization it is the military magistrate's responsibility to ensure particularity. Although not required, it will often be useful for a magistrate to understand law enforcement's search capabilities, the intended method of search, and the technical language endemic to a particular field of investigation. This understanding will help ensure an authorization is crafted such that is both clear and "expansive enough to allow investigators access to places where incriminating materials may be hidden, yet not so broad that they become the sort of free-for-all general searches the Fourth Amendment was designed to prevent." *Richards*, 76 M.J. at 370.

The forensic investigator thought the term "digital communication" limited the type of items investigators could seize, meaning once a device capable of communicating was seized, she could then search the entire device. The military judge broadly found that the term "digital communication" focused on the "process of bringing an idea to another's perception" rather than on the actual transmission of data.

[3] We find no probable cause to search and seize any "hard drives."

Again, the purpose of the Fourth Amendment particularity requirement is to prevent general searches. A warrant must describe the things to be seized with sufficiently precise language so that it informs the officers how to separate the items that are properly subject to seizure from those that are irrelevant. *Davis v. Gracey*, 111 F. 3d 1472, 1478-79 (10th Cir 1997). Stated another way, nothing is left to the discretion of the officer executing the search. *Marron v. United States*, 275 U.S. 192, 196 (1927). Here, the government finds broad meaning in the term "digital communication."

That said, we find that an authorization to search for evidence of a digital communication would not authorize a search for all photographs on a phone wherever located. This is because not all photographs constitute communications. Here, SA Jacob specifically testified she did not narrow or confine her search to transferred or received communications. She did, however, determine the three photographs at issue were not transmitted–they were drawn from a picture editing program. We conclude under the facts of this case, the photographs at issue are not "digital communication."[4]

The Good Faith Exception

Once a court determines that a search violates the Fourth Amendment, the exclusionary rule demands that evidence obtained from that search be suppressed unless an exception applies. The good faith exception to the exclusionary rule is applicable when investigators "act with an objectively 'reasonable good faith belief' that their conduct is lawful." *Davis v. United States*, 564 U.S. 229, 238 (2011) (citing *Leon*, 468 U.S. at 909). The test is "whether a reasonably well-trained officer would have known that the search was illegal" in light of "all of the circumstances." *Herring v. United States*, 555 U.S. 135, 145 (2009) (citing *Leon*, 468 U.S. at 922, n. 23). This standard takes into account the officer's training and experience, but not his or her subjective intent. *Id*. at 145-46. In application, the

[4] The government argues the authorization in this case is substantially similar to the authorization in *United States v. Richards*, which our superior court determined to be a valid authorization. 76 M.J. 365. In *Richards* police found child pornography on the unallocated space of a drive within a "pictures" folder. *Id.* at 368. The authorization in *Richards* allowed law enforcement to seize "all electronic media and power cords for devices capable of transmitting or storing online communications" between Richards and a minor. *Id.* at 367-68. However, despite the similarity in authorizing searches for "communications," *Richards* is factually distinct. In this case, the agent did not just look for communications. The agent specifically looked for photographs as evidence of the sexual assault–she was not looking at the photographs to find text messages.

good faith exception applies to conduct involving only "simple, isolated negligence," but not to conduct amounting to a deliberate, reckless, or grossly negligent disregard of Fourth Amendment rights. *Davis*, 564 U.S. at 238. The good faith exception recognizes that the exclusionary rule "cannot be expected, and should not be applied, to deter objectively reasonable law enforcement activity." *Leon*, 468 U.S. at 918-19.

The President, exercising his authority under Article 36, UCMJ, promulgated a military good faith exception rule. Evidence that was obtained as a result of an unlawful search or seizure may be used if:

> (A) The search or seizure resulted from an authorization to search, seize or apprehend issued by an individual competent to issue the authorization under Mil. R. Evid. 315(d) or from a search warrant or arrest warrant issued by competent civilian authority;
>
> (B) The individual issuing the authorization or warrant had a substantial basis for determining the existence of probable cause; and
>
> (C) The officials seeking and executing the authorization or warrant reasonably and with good faith relied on the issuance of the authorization or warrant. Good faith shall be determined using an objective standard.

Mil. R. Evid. 311(c)(3).

Military Rule of Evidence 311(c)(3) embodies the good faith exception as articulated in *Leon* and *Massachusetts v. Sheppard*, 468 U.S. 981 (1984), which specifically address the scenario when officers rely on a subsequently invalidated search warrant. *United States v. Carter*, 54 M.J. 414, 421 (C.A.A.F. 2001).[5] The *Leon* exception to the exclusionary rule, however, does not extend to situations involving the unlawful execution of a valid warrant. *Leon*, 468 U.S. at 918 n. 19; *see also United States v. Maxwell*, 45 M.J. 406, 421 (C.A.A.F. 1996). Further, when officers do not rely on another's mistake, but instead commit the mistake themselves by exceeding the scope of an explicit and valid warrant, the good faith exception does not apply. *United States v. Angelos*, 433 F.3d 738, 744-46 (10th Cir. 2006).

[5] In *Carter* and *Hoffmann* the CAAF analyzed Mil. R. Evid. 311(b)(3), which was subsequently moved in 2013 to Mil. R. Evid. 311(c)(3). *See* Exec. Order No. 13,643, 78 Fed. Reg. 29,559, 29,567 (21 May 2013).

The government has the burden of proving, by a preponderance of the evidence, the requirements of the good faith exception have been met. Mil. R. Evid. 311(d)(5). Here, there is no issue with the military magistrate's authority to issue a search warrant, but we hold the government has not met its burden with respect to the two other requirements.

In *Carter*, our superior court determined that with respect to prong (B) of Mil. R. Evid. 311(c)(3), the phrase "substantial basis" does not have the same meaning as the term "substantial basis" in *Illinois v Gates*.[6] 54 M.J. at 421. Rather, "substantial basis" as an element of good faith "is satisfied if the law enforcement official has an objectively reasonable belief that the magistrate had a 'substantial basis' for determining the existence of probable cause." *Id*. at 422. Here, the affidavit provided no factual predicate to establish its request to search for any "depiction of SPC [AC] between the time/date group 0000, 9 F[e]b 14 and 0900 25 Feb 14" and no factual basis to conduct an open-ended search of the phone's entire contents. The affidavit was bare bones with respect to such authorizations as the only nexus between the phone and the alleged crimes described was appellant's text message admissions. An objectively reasonable law enforcement official executing the warrant would have believed the military magistrate had a substantial basis for determining probable cause with respect to a search for messages between appellant and SPC AC. Though police officers need not interpret a warrant in an unduly narrow fashion, they must exercise common sense in assessing the warrant's scope. *United States v. Fogg*, 52 M.J. 144, 148 (C.A.A.F. 2010). An objectively reasonable agent would have believed this included text messages sent between appellant and SPC AC and the metadata associated with these particular messages. It did not reasonably include a search for any and all pictures and videos nor for that matter did it allow an open-ended search.

With respect to prong (C) of Mil. R. Evid. 311(c)(3), the evidence indicates either SA Jacob failed to read the entire authorization which included the affidavit, or was not given the entire authorization, only the first page. The first page referenced the incorporated attachment. Regardless, SA Jacob did not ask the magistrate for guidance or clarification regarding what was authorized. Special Agent Jacob admittedly assumed it authorized an open-ended search based on her read of only the first page of the authorization. In this case, to understand what was

[6] In *Nieto*, the CAAF noted a tension between its analysis of prong (B) of the good faith doctrine in *Carter*, and *Hoffmann*. 76 M.J. at 108, n. 6. Our superior court declined to resolve this tension in a case where neither standard was satisfied. Similarly, we need not resolve the conflict between *Carter* and *Hoffmann* as the good faith exception fails here, even under the more government-friendly standard of *Carter*.

authorized, SA Jacob should have read the entire authorization to include the affidavit to put the authorization in context. In failing to do so, she executed a broader search than was authorized. Because not all photographs constitute digital communications, she exceeded the scope of the authorization. Additionally, SA Jacob searched outside the date range noted in the authorization. Accordingly, we do not find the government has met their burden that SA Jacob was objectively reasonable.

As the government has failed to meet its burden with respect to both prong (B) and (C), the good faith exception to the exclusionary rule is, therefore, inapplicable.

The Plain View Doctrine

Military Rule of Evidence 316(c)(5)(C) recognizes the plain view exception allows the seizure of evidence where an agent is in a lawful position to observe evidence that he has probable cause to seize. Our superior court has recognized this exception to the exclusionary rule and has held the plain view doctrine is an exception to the suppression of evidence. "[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 plain view doctrine does not give carte blanche for law enforcement to conduct searches beyond the scope of a given warrant. "A prerequisite for the application of the plain view doctrine is that law enforcement must have been conducting a lawful search when they stumbled upon evidence in plain view." *United States v. Gurczynski*, 76 M.J 381, 388 (C.A.A.F. 2017). Here, the evidence was obtained based on an affidavit that was missing key facts, a search authorization that was overbroad, and a search that was conducted without reading the entire authorization. It was the government's burden to show that law enforcement were lawfully in the spot where the evidence was in plain view. Given the tripartite failure, the government has not met its burden.

While it is possible that a valid search executed in a reasonable manner would have discovered this evidence, we are not persuaded this occurred. By her own testimony, SA Jacob was conducting a general unfettered search of the phone.[7] This

[7] Assuming the extraction of all of the files contained on the phone was a reasonable way to conduct this search, and assuming the digital forensic examiner was allowed

(continued . . .)

search as conducted by SA Jacob was unsupported by probable cause and went beyond any reasonable interpretation of the scope of the warrant. In short, we cannot determine whether SA Jacob found the photos in plain view while lawfully looking for text messages, or whether she found the photos because she was looking for them. It is the government's burden to establish facts to support the plain view exception.

Accordingly, we find the plain view doctrine inapplicable.

CONCLUSION

We hold the military judge abused her discretion by failing to grant the defense motion to suppress the pictures. The findings of guilty and the sentence are SET ASIDE. A rehearing is authorized.

Senior Judge BURTON and Judge SALUSSOLIA concur.

FOR THE COURT:

MALCOLM H. SQUIRES, JR.
Clerk of Court

(. . . continued)
to look at thumbnails or meta-data, further assuming the examiner was not allowed by the search authorization to open the subject file, once SA Jacob found a picture file that had not been "communicated," but the photo was relevant to the investigation because it was taken during the date and time of the reported assault, she should have obtained a new search authorization before opening the file and continuing to search for other picture files that had not been communicated. Furthermore, the government conceded at oral argument that inevitable discovery did not apply to the facts of this case. We accept this concession.