UNITED STATES AIR FORCE
COURT OF CRIMINAL APPEALS

No. ACM 39793

UNITED STATES
Appellee

v.

Travis S. BECK, Jr.
Airman First Class (E-3), U.S. Air Force, *Appellant*

Appeal from the United States Air Force Trial Judiciary

Decided 21 April 2021

Military Judge: Jennifer E. Powell.

Sentence: Sentence adjudged on 22 June 2019 by GCM convened at Ellsworth Air Force Base, South Dakota. Sentence entered by military judge on 13 October 2019: Dishonorable discharge, confinement for 14 years and 6 months, forfeiture of all pay and allowances, reduction to E-1, and a reprimand.

For Appellant: Major Benjamin H. DeYoung, USAF.

For Appellee: Lieutenant Colonel Brian C. Mason, USAF; Lieutenant Colonel Matthew J. Neil, USAF; Major Jessica L. Delaney, USAF; Mary Ellen Payne, Esquire.

Before POSCH, RICHARDSON, and MEGINLEY, *Appellate Military Judges*.

Judge MEGINLEY delivered the opinion of the court, in which Senior Judge POSCH and Judge RICHARDSON joined.

MEGINLEY, Judge:

A general court-martial composed of a military judge sitting alone found Appellant guilty, consistent with his pleas, of one specification of attempted receipt of child pornography and two specifications of attempted sexual abuse of a child, in violation of Article 80, Uniform Code of Military Justice (UCMJ), 10 U.S.C. § 880; and one specification of possession of child pornography and one specification of producing or transmitting child pornography as assimilated under 18 U.S.C. § 2251, both in violation of Article 134, UCMJ, 10 U.S.C. § 934. Contrary to his pleas, the military judge found Appellant guilty of one specification of attempting to patronize a prostitute, in violation of Article 80, UCMJ, 10 U.S.C. § 880;[1] one charge and specification of sexual assault in violation of Article 120, UCMJ, 10 U.S.C. § 920; and one charge and one specification of receiving obscene visual depictions of a minor, as assimilated under 18 U.S.C. § 1466A, in violation of Article 134, UCMJ, 10 U.S.C. § 934.[2] Appellant was sentenced to a dishonorable discharge, confinement for 14 years and 6 months, forfeiture of all pay and allowances, reduction to the grade of E-1, and a reprimand. The convening authority took "no action" on the adjudged sentence.[3]

Appellant raises five issues on appeal: (1) whether the military judge erred in denying a defense motion to suppress evidence; (2) whether Appellant's speedy trial rights under the Sixth Amendment[4] and Rule for Courts-Martial (R.C.M.) 707 were violated; (3) whether Appellant is entitled to appropriate relief due to the convening authority's failure to take action on his sentence as required by law; (4) whether the Government was preempted from charging an assimilated Article 134, UCMJ, offense, in violation of 18 U.S.C § 1466A, because prosecution for conduct of this nature is preempted by the enumerated

---

[1] Appellant was found not guilty of one other specification of attempting to patronize a prostitute.

[2] All references in this opinion to the punitive articles of the Uniform Code of Military Justice (UCMJ), are to the *Manual for Courts-Martial, United States* (2016 ed.). The charges and specifications were referred to trial after 1 January 2019; as such, all other references to the UCMJ and Rules for Courts-Martial (R.C.M.) are to the *Manual for Courts-Martial, United States* (2019 ed.). *See* Exec. Order 13,825, §§ 3 and 5, 83 Fed. Reg. 9889, 9890 (8 Mar. 2018).

[3] In the convening authority Decision on Action memorandum, dated 22 August 2019, the convening authority denied Appellant's request for deferment of reduction in rank. Appellant was beyond the expiration of his term of service when the convening authority denied Appellant's request for waiver of automatic forfeitures of pay.

[4] U.S. CONST. amend. VI.

Article 134, UCMJ, offense of receiving child pornography; and (5) whether the language used by the convening authority in Appellant's reprimand made his sentence inappropriately severe.[5] After careful consideration, regarding the part of issue (2) concerning whether Appellant's Sixth Amendment rights were violated, and issues (3) and (5), we have determined those issues do not warrant further discussion nor relief.[6] *See United States v. Matias*, 25 M.J. 356, 361 (C.M.A. 1987). With regard to the remaining issues, we find no prejudicial error to a substantial right of Appellant, and we affirm the findings and sentence.

I. BACKGROUND

KL met Appellant in either late March 2017 or early April 2017 on the social media dating application, Tinder, and later the two began text messaging before eventually meeting in person. Approximately a week after meeting Appellant in person, KL and Appellant entered into a sexual relationship. As their relationship progressed, KL stated her sexual experiences with Appellant became rougher and more aggressive. When things would get to be too rough, KL would let Appellant know by telling him "no" or "stop." According to KL, Appellant would respect her wishes when this occurred. However, at the end of April 2017, KL decided to end the sexual aspect of her relationship with Appellant when she started dating someone else.

On 11 May 2017, Appellant sent KL a text message stating he needed to talk. KL found his text message concerning, as Appellant had previously confided in her of some suicidal ideations. KL went to Appellant's house and talked with Appellant on his bed about a new relationship Appellant had entered and how he "wasn't receiving certain things in his [new] relationship and he was unhappy about that." After talking for about five minutes, Appellant pushed KL on to the bed, took off her pants, and inserted his penis in KL's vagina. KL told Appellant "no" and tried to push him off her; however, Appellant did not stop. KL testified Appellant pinned her wrists down and stated, "Keep fighting me, b*tch." After five or six minutes, Appellant ejaculated in KL. After he finished, Appellant asked KL, "Did I do what I think I just did?" KL responded, "Yes," put her clothes on, and left Appellant's residence.

---

[5] Appellant personally raised issues (4) and (5) pursuant to *United States v. Grostefon*, 12 M.J. 431 (C.M.A. 1982).

[6] Regarding issue (2), we find Appellant's Sixth Amendment rights were not violated. Regarding issue (3), consistent with the respective opinions of the judges of this panel in *United States v. Barrick*, No. ACM S32579, 2020 CCA LEXIS 346 (A.F. Ct. Crim. App. 30 Sep. 2020) (unpub. op.), and subsequent opinions, we find no error in the convening authority's decision to "take no action on the sentence in this case."

Later that day, Appellant sent KL a message through Snapchat, a social media messaging application, telling KL that, "We need a safety word [ ]. That was 100 not okay. I feel terrible." After Appellant's message, KL responded:

> [KL:] It's okay. You didn't know.
>
> [Appellant:] Probably part of why I reacted that way after[.] And yes I did know! You said no!
>
> [KL:] /:
>
> [Appellant:] I'm so sorry [KL]… I understand if you can't even look at me right now, that was so f*cked up.
>
> [KL:] Don't apologize. It's fine.
>
> [Appellant:] Are you absolutely sure you're ok?
>
> [KL:] Not absolutely but I'll be fine.

KL stated she sent this message because she "didn't want to come to terms quite yet with what happened, and [she] just wanted to get the conversation over with."

On 26 May 2017, KL reported to the Box Elder (South Dakota) Police Department (BEPD) (near Ellsworth Air Force Base, South Dakota), that she had been sexually assaulted by Appellant. The Air Force Office of Special Investigations (AFOSI) was notified by BEPD of the allegation, and after obtaining jurisdiction, agents opened an investigation. AFOSI agents reviewed KL's cell phone, and saw the text messages and Snapchat messages exchanged between KL and Appellant.

On 16 June 2017, Appellant was interviewed by AFOSI agents. After being advised by Special Agent (SA) CR that he was suspected of sexual assault and read his rights under Article 31, UCMJ, 10 U.S.C. § 831, Appellant acknowledged his rights and invoked his right to counsel. SA CR advised Appellant that AFOSI agents had received verbal authorization to seize Appellant's cell phone. Agents then asked Appellant if his phone was password protected. Appellant responded it was password protected. The agents then asked Appellant to disable the passcode on his cell phone, which Appellant did.[7] The verbal authorization was later reduced to writing that same day. A search of Appellant's

[7] An AFOSI agent told Appellant, "[J]ust so you are fully aware on your rights on this, the passcode is going to be up to you whether or not you want to disable it . . . what it does is it saves us time in the long run, so if you disable it now, we can go from there . . . otherwise, we'll have to go back to the approval authority, we'll apply for . . . a compulsion letter and they will force you to unlock it. So it is whether or not you want to do it now or have us go through (becomes inaudible)."

phone after the seizure revealed no additional misconduct, and AFOSI closed its investigation in August 2017.

One charge with a single specification alleging sexual assault was preferred against Appellant in October 2017. As trial counsel was preparing for Appellant's Article 32, UCMJ, 10 U.S.C. § 832, preliminary hearing, he interviewed KL and learned more about her communications with Appellant. In January 2018, the Government received a second search authorization to search Appellant's social media accounts, and after another search of Appellant's phone, alleged child pornography and obscene anime material were discovered. In February 2018, the Government sought and received a third search authorization, and sent the phone to the Department of Defense Cyber Crime Center/Cyber Forensics Laboratory (DC3/CFL). After the DC3/CFL forensic examiner discovered evidence of additional misconduct, in April 2018 the Government sought and received a fourth search authorization, and a subsequent search of Appellant's phone in April 2018 revealed additional misconduct, which indicated Appellant engaged in conversations with people of many different ages, and reached out to users he believed to be 15 to 17 years old. The April 2018 search revealed Appellant attempted to sexually abuse children, as he sent a photo of his penis to an individual who claimed to be a 15-year-old girl, and communicated indecent language to her, including sexually explicit language. Appellant engaged in another lewd conversation with another girl, whom he believed was 15 years of age, and sent her messages about his penis. There was also evidence Appellant possessed child pornography and that he patronized a prostitute.

II. DISCUSSION

A. Motion to Suppress Evidence

1. Additional Background[8]

a. The first search authorization (June 2017)

On 16 June 2017, another AFOSI agent, SA WV, submitted a written affidavit in support of an application to search and seize "[Appellant]'s cell phone for text message conversations between [Appellant] and [KL] from 1 May [20]17 to present." Specifically, the supporting affidavit stated that Appellant and KL met through the phone application, Tinder, and KL had screenshots of messages exchanged between herself and Appellant relevant to her sexual assault allegation.

[8] The military judge made extensive findings of fact regarding this motion. Except as otherwise noted, this court adopts her findings of fact.

According to SA CR, the purpose of the 16 June 2017 search authorization was to search for text messages between Appellant and KL and to corroborate what KL had provided to law enforcement. At the time, SA CR was under the impression that messages sent through Snapchat disappeared immediately after being read by the recipient, and he believed that Snapchat messages between Appellant and KL no longer existed. A local military magistrate, Lieutenant Colonel (Lt Col) KE, determined there was probable cause to believe that relevant communications were contained on Appellant's cell phone and authorized the search of Appellant's phone. This would be the first of the four search authorizations issued for Appellant's phone.

At the time of Appellant's AFOSI interview, the local AFOSI detachment was able to conduct an extraction of Appellant's phone using Cellebrite's Universal Forensic Extraction Device (UFED) only if the phone was unlocked or not password protected.[9] After seizing Appellant's cell phone, a third AFOSI agent, SA MH, utilized Cellebrite software to conduct an extraction on 22 June 2017, limiting his search to the scope of the 16 June 2017 search authorization. The text messages extracted provided no evidence of other misconduct.[10]

Had Appellant not provided his passcode in June 2017, neither the local AFOSI detachment, nor DC3/CFL, had the capability to unlock Appellant's device in house. However, Cellebrite Advanced Services (CAS) had the ability to support "brute force identification" of the screen lock and extraction of the complete file system data on Appellant's cell phone seized by AFOSI. Since DC3/CFL did not have the capability to access such devices, it had a policy of asking the requesting agency if it wanted to pay for CAS to unlock a device. If the requesting agency approved and paid for the service, DC3/CFL then transported the relevant device to a local CAS office. DC3/CFL did not obtain CAS technology and proprietary software in its own facility until March 2018.[11] The local AFOSI detachment did not consult AFOSI's Digital Forensic Consultants

---

[9] The court takes judicial notice under Mil. R. Evid. 201(b)(2) that Cellebrite is a company that develops digital intelligence platforms. According to Cellebrite's website, a UFED is used to access digital device data and allows users to "bypass locks, perform advanced unlocks, perform logical/full file system/physical extractions, perform selective extraction of apps data and cloud tokens." Cellebrite UFED Product Overview, https://cf-media.cellebrite.com/wp-content/uploads/2020/06/ProductOverview_Cellebrite_UFED_A4.pdf (last visited 2 Apr. 2021).

[10] According to SA CR, only text message communications were extracted.

[11] According to Mr. TH, a digital forensics investigator with the DC3/CFL who testified at Appellant's trial, a cell phone extraction service at Cellebrite cost between $1,500.00 and $2,000.00 in June 2017.

(DFC), DC3/CFL, or Cellebrite regarding an extraction of Snapchat messages between Appellant and KL, nor was there a plan to consult those entities.

AFOSI closed its investigation into Appellant's alleged sexual assault of KL in August 2017, distributed its report, and awaited case disposition. On 30 August 2017, the United States Court of Appeals for the Armed Forces (CAAF) published *United States v. Mitchell*, holding that the Government violated the appellant's Fifth Amendment[12] rights (as protected by *Edwards v. Arizona*, 451 U.S. 477 (1981)) when agents asked the appellant, in the absence of counsel, to enter his phone's passcode.[13] 76 M.J. 413, 415 (C.A.A.F. 2017).

Prior to the Article 32, UCMJ, preliminary hearing, Captain (Capt) MM, a local judge advocate, interviewed KL; the primary trial counsel for the case, Capt MN, was not present for the interview because he was on temporary duty (TDY) at another installation. During this interview, KL said she and Appellant communicated primarily through Snapchat, and told counsel that she knew Appellant saved messages and pictures between the two of them because he "gray[ed] them out."[14] Although she did not normally screenshot her messages or interactions with Appellant, KL had taken a screenshot of the Snapchat conversation with Appellant where he apologized for what he did.[15]

On 5 January 2018, the charge and specification relating to KL were referred to general court-martial. On 10 January 2018, after Capt MN returned from his TDY, he conducted another interview with KL, where she stated that Appellant used "a function on [S]napchat that allows a message to be locked and not disappear . . . [and] turn gray on her [S]napchat application." The Government wanted to find the Snapchat message saved between Appellant and KL on Appellant's cell phone, and concluded they needed to expand the June 2017 search authorization, as that authorization covered only "text messages" and not "other platforms."

b. *The second search authorization (January 2018)*

---

[12] U.S. CONST. amend. V.

[13] Agents at the local Ellsworth AFB AFOSI detachment subsequently received training on how to move forward based on the new law.

[14] According to KL, when Appellant "grayed out" messages she and Appellant had exchanged, KL had an indication Appellant saved those messages to his phone. According to SA CR, KL understood that "grayed out" Snapchats meant they had been saved.

[15] The messages between Appellant and KL were highlighted in gray, which indicate that Appellant had saved the conversation. Accordingly, when KL opened the conversation in the application, the messages were saved and remained visible.

On 24 January 2018, AFOSI agents sought an expanded search authorization to search Appellant's cell phone for social media communications. SA CR also requested search authorization to look at screenshots, based on KL's interview with trial counsel. At this time, AFOSI agents remained focused on Appellant's alleged sexual assault of KL. That same day, SA CR submitted an affidavit in support of a second application to search "[Appellant's] cell phone for any communications between [Appellant] and [KL] from 1 May 2017 to 16 June 2017, to include any data stored on the phone from social media messaging applications and/or screenshots of such communications." On 24 January 2018 and based on SA CR's affidavit, a military magistrate, Colonel (Col) JN, found probable cause to search Appellant's cell phone, and authorized a written order for the search and seizure of Appellant's cell phone.[16]

Relying on the 24 January 2018 search authorization, on 29 January 2018, SA MH searched the saved images in the photographs folder on Appellant's cell phone to identify screenshots of Snapchat communications between Appellant and KL. The military judge found as fact that SA MH was "specifically looking at data previously pulled from [Appellant]'s cellular phone lawfully seized from [Appellant] in June 2017 for Snapchat messages that may have been saved as screen shots in the photograph folder on [Appellant]'s cell phone." While looking for screenshots of Snapchat messages in the folder, SA MH discovered "anime," or animated images of "children and adolescents performing various sexual acts or having various sexual acts performed on them in various poses of undress." Once he saw these images, SA MH contacted the legal office.[17] He then drafted a new search authorization for the military magistrate and contacted DC3/CFL, as DC3/CFL was "better equipped to address suspected child pornography than AFOSI."

c. The third search authorization (February 2018)

On 2 February 2018, SA MH submitted another affidavit in support of a third search authorization, this time to search "[Appellant's] cell phone for any child pornography depicting animated or real children, [I]nternet search terms associated with child . . . pornography, and any social media communications

---

[16] The military judge's ruling references the date of this search authorization as 28 January 2018. However, the date on the document is 24 January 2018.

[17] SA MH testified he reached out to the Chief of Military Justice at the legal office and "explained to him what [he] was doing and what [he] had found. [He] asked him to come over and take a look at it with [him]." The Chief of Military Justice went to AFOSI to look at the alleged contraband. SA MH stated, "We looked at the images. We talked about it. He said, yeah, it looks like, you know, they look like they could be children. . . . [F]ollowing our conversation, I did proceed to draft an additional affidavit and search authority to expand the warrant on the phone that we had of [Appellant]."

with discussions or photographs related to child pornography." A military magistrate, Col JN, determined there was probable cause to believe there was relevant evidence on the phone of such content, and issued a written order authorizing the search. However, due to the local AFOSI detachment's limited in-house capabilities, agents were unable to extract Snapchat messages or data from other social media applications from Appellant's phone as authorized by the military magistrate's February 2018 authorization. As a result, AFOSI agents sent Appellant's cell phone to DC3/CFL for further extraction and analysis.

On 20 March 2018, Mr. TH from DC3/CFL contacted AFOSI agents regarding the scope of the search of Appellant's cell phone. According to the DC3/CFL Form 1,[18] Mr. TH was advised that the scope of the search was limited to communications between Appellant and KL during the time frame outlined in the January 2018 search authorization, to include communications via Snapchat and other social media applications. Government agents, both from the legal office and law enforcement, informed Mr. TH of the February 2018 search authorization regarding child pornography; however, the Government told Mr. TH it was not actively pursuing those allegations at the time based on what AFOSI uncovered and "that the February 2018 search authorization was not relevant." At the time Mr. TH received Appellant's cell phone in March 2018, DC3/CFL had obtained in-house CAS capability.

The CAS system DC3/CFL used worked only if the cell phone was locked. The Cellebrite system would attempt a "brute force" identification, systematically attempting every possible four- or six-digit numerical combination until the passcode was identified. Therefore, to accomplish a full extraction of Appellant's cell phone, Mr. TH relocked Appellant's cell phone and set a personal identification number (PIN). Because Mr. TH entered the PIN into the Cellebrite system, he was able to successfully gain access on the first try. Mr. TH testified it would take the system no more than two days to identify an unknown PIN on Appellant's device, and because of a finite number of digit combinations, the chance of success was 100 percent. When asked by trial counsel if he ever had the passcode to Appellant's phone, he answered, "No," and stated he did not need it.

On 28 March 2018, while reviewing social media applications from 10 May 2017 to 12 May 2017 for deleted messages between KL and Appellant, Mr. TH discovered a chat thread on the social media application, Whisper, close in time to the alleged sexual assault. The message was between Appellant and "Nerd,"

---

[18] According to SA MH, a DC3/CFL Form 1 is a form that contains a summary of the investigation, the authorities for searching the device in question, and what investigators are asking DC3/CFL to review or search.

who messaged Appellant, stating, "I'm only 15*!" Mr. TH saw Appellant had solicited this contact for photographs and that Appellant sent a photograph of his penis to "Nerd" via Whisper. Mr. TH did not continue his search because the conversation was not between KL and Appellant but relayed his discovery to the Government. Mr. TH noted that in his experience, "[P]eople migrate from one application to another and generally, they start on Whisper and then, they migrate into usually Snapchat or Kik [another social media application]; that's in every case I've ever worked with Whisper." Mr. TH further opined that it would be appropriate to open the images folder to look for communications because in his experience "[p]eople screenshot things all the time."

d. The fourth search authorization (April 2018)

On 2 April 2018, SA CR submitted another affidavit in support of a fourth search authorization to search "[Appellant's] cell phone for text or social media communications with purported minors to include sexual communications via text or photographs." A military magistrate, Lt Col KE, determined there was probable cause to believe that relevant communications were contained within the device, and issued a written search authorization.

On 19 April 2018, AFOSI agents initiated a new investigation into Appellant's conduct based on the evidence Mr. TH discovered. Specifically, AFOSI began its investigation based on evidence that Appellant requested and received nude images and engaged in sexually explicit conversations with a known minor, sent images of his genitalia, and engaged in sexual explicit conversations with a known minor and other individuals suspected to be minors.

e. Federal search authorization of Appellant's home and property

On 6 June 2018, agents from AFOSI submitted an affidavit to the United States District Court for the District of South Dakota in support of an application to search Appellant's off-base residence and seize certain property. That same day, a United States Magistrate Judge issued a search and seizure warrant for Appellant's property, including computer and electronic storage devices. On 7 June 2018, AFOSI agents conducted a search and seizure of Appellant's property.

2. Motion to Suppress

At trial, the Defense moved to suppress, on Fourth[19] and Fifth Amendment grounds, all data, information, statements, and evidence that were obtained from the four searches of Appellant's cell phone. Trial defense counsel argued that Appellant's Fifth Amendment rights were violated when Appellant was

[19] U.S. CONST. amend. IV.

asked to enter his cell phone's passcode after he had invoked his right to counsel and refused to answer questions posed to him by AFOSI agents. Trial defense counsel argued a Fourth Amendment violation arose from the Government's failure to establish probable cause for the second January 2018 search authorization, as the search authorization did not describe the scope of the search with sufficient particularity, and that the scope of the search was too broad. Trial defense counsel also challenged the fourth April 2018 search authorization, arguing that the inclusion of SA MH's observations from his January 2018 search in the affidavit was improper and was overly broad in expanding the search to "all social media communications." The military judge made two rulings to Appellant's motion to suppress. In her initial ruling of 13 June 2019, the military judge granted Appellant's motion to suppress in part, as to SA MH's 29 January 2018 search and the subsequent February 2018 search, but denied Appellant's remaining request for relief. After her initial ruling caused some confusion among the counsel, the military judge issued a supplemental ruling on 17 June 2019 to Appellant's motion to suppress, denying Appellant's motion to suppress the searches of his phone in full.

a. Military Judge's initial ruling

The military judge found that Appellant was in custody when he was interviewed by AFOSI agents, that he invoked his right to counsel, and that he needed to have an attorney present before AFOSI agents asked him to unlock his phone by entering his passcode. The military judge found that the agents violated Appellant's Fifth Amendment rights as protected by *Miranda v. Arizona*, 384 U.S. 436 (1966), and *Edwards v. Arizona*, 451 U.S. 477 (1981); however, she noted that the agents involved did not act in bad faith, and that *Mitchell* had not been decided at the time of the interrogation. 76 M.J. at 413.

The military judge found Appellant's phone was seized pursuant to lawful authorization prior to the *Edwards* violation, or any other Fifth Amendment violation, and the phone itself "d[id] not constitute evidence derived from the illicit interrogation." The military judge further found the contents of Appellant's phone were admissible, because the Government would have inevitably discovered the evidence, as agents "possessed, or were actively pursuing, evidence or leads that would have inevitably led to the discovery of the evidence in a lawful manner."

However, in this initial ruling, the military judge suppressed "the evidence resulting from SA MH's unlawful search on 29 January 2018 and the subsequent [third] 2 February 2018 search authorization."[20] She concluded that SA MH had looked at an extraction from Appellant's phone that was accessed through the AFOSI agents' June 2017 *Mitchell* violation,[21] yet AFOSI agents "had not yet pursued avenues in which to overcome the initial *Mitchell* violation," and therefore SA MH was "not lawfully there despite attempting to follow a lawful search authorization."

In addressing whether probable cause existed to search Appellant's phone, specifically the January 2018 search authorization, the military judge concluded that law enforcement was not precluded from modifying the initial search authorization once "new evidence [wa]s presented to support a new search authorization." The military judge concluded the January 2018 search authorization was supported by probable cause and the military magistrate had a substantial basis for this determination. The military judge also concluded that the January 2018 search authorization was adequately scoped in time, type and individuals, and that law enforcement had not been given "carte blanche to rummage in [Appellant's] iPhone."

With respect to the 2 April 2018 search authorization, the military judge severed that provision of the AFOSI affidavit that included SA MH's discovery of animated images of underage females. She concluded the military magistrate had a substantial basis for determining probable cause existed to search Appellant's phone, even without the evidence proffered from SA MH's January 2018 search. Also, the military judge stated that Mr. TH, who was not present for the January 2018 search, limited his March 2018 search of Appellant's phone within the restraints of the January 2018 search authorization, and accessed the content of Appellant's phone "independently from the access achieved through AFOSI's initial *Mitchell* violation in June 2017." Also, given Mr. TH's professional experience, he established the necessary nexus required under the Fourth Amendment and case law between the type of crime, nature of items sought, and reasonable inferences about where evidence is likely to be kept. The military judge also found the scope of the military magistrate's search authorization was sufficiently tailored "to ensure that it was reasonable under the facts and circumstances in this case." Finally, the military judge

---

[20] The military judge did not identify the evidence she suppressed, but the court can surmise she suppressed SA MH's discovery of the anime videos.

[21] The military judge's ruling refers to the "*Mitchell* violation" when the AFOSI agents asked Appellant to disable his passcode on his cell phone after invoking his right to counsel. According to her ruling, "At the moment when interrogation occurred, the violation of [Appellant's] rights under *Edwards* was complete."

found no evidence suggesting the military magistrate's April 2018 search authorization was "anything but impartial, neutral, and detached."

The military judge also found that inevitable discovery applied in this case, as the Government possessed, or was actively pursuing evidence or leads that would have inevitably led to the discovery of the evidence in a lawful manner. The military judge concluded AFOSI agents did not have the capability to extract Snapchat messages from Appellant's phone in reliance on the January 2018 search authorization, so AFOSI agents needed to submit Appellant's phone to DC3/CFL for assistance in the extraction and analysis. Further, the military judge relied on Mr. TH's testimony that he "relocked" Appellant's cell phone in order for the program to work.

> If Mr. [TH] had not relocked Appellant's phone (putting it in the same locked status prior to the June *Mitchell* violation), the Cellebrite software would not have extracted the data from [Appellant's] phone. Therefore, the data that Mr. [TH] searched on [Appellant]'s phone was accessed independently from [Appellant]'s *Mitchell* violation.

The military judge found "it was reasonable to conclude that AFOSI would have obtained a valid authorization from the military magistrate had they known their actions were unlawful."

Finally, the military judge concluded that even if this court found her ruling in error, the good faith exception applied to the January 2018 search authorization, as there was no evidence that AFOSI agents "intentionally or recklessly made false statements or omissions in the supporting affidavit." Additionally, in conducting a Mil. R. Evid. 311(a)(3) balancing test, the military judge found exclusion of the evidence would "not result in an appreciable deterrence of future unlawful searches," and to exclude the evidence would deter law enforcement "to do just what they did – continually seek expanded search authorization from a new neutral and detached military magistrate when new crimes were discovered during their lawful searches."

b. Military Judge's supplemental ruling

On 17 June 2019, after considering additional evidence and argument from counsel, the military judge issued a supplemental ruling on the motion to suppress, with the primary focus on the searches conducted by Mr. TH.

On 28 March 2018, Mr. TH conducted his analysis under the 24 January 2018 search authorization. Despite being told about the 2 February 2018 search authorization for child pornography, Mr. TH received specific instructions that the 2 February 2018 search authorization was not relevant to his search. The military judge specifically found as fact that although Mr. TH re-

ceived the 2 February 2018 search authorization (on 11 April 2018), which authorized the search for child pornography and was based on SA MH's illegal search pursuant to the *Mitchell* violation, "[t]he only thing Mr. TH explicitly did under the 2 February 2018 search authorization was contact [the] National Center for Missing and Exploited Children (NCMEC) to determine if [Appellant's] cellular phone had any files containing known child victims" of which there were no known victims in the files related to Appellant. The military judge found Mr. TH credible during his in-court testimony.

Without reliance on the evidence from SA MH's 29 January 2018 search or the February 2018 search authorization, and under the doctrine of "plain view," Mr. TH found evidence of the communications leading to "Nerd," who informed Appellant she was 15 years old, Mr. TH saw that Appellant solicited "Nerd" for photographs and sent her a photograph of his penis via Whisper. Mr. TH then followed up with AFOSI agents and sought guidance which resulted in the Government seeking the fourth, 2 April 2018, search authorization. Mr. TH received a copy of the search authorization the next day, and that search authorization allowed him to search Appellant's cell phone for "text or social media communication with purported minors to include sexual communications via text or photographs." Therefore, when Mr. TH reviewed Appellant's search history to determine if Appellant used Kik or Facebook, he was operating under the April 2018 search authorization.

The military judge once again concluded that inevitable discovery applied to the evidence discovered by Mr. TH, which led to the April 2018 search authorization. The military judge also found the plain view exception applied, given that Mr. TH was relying on the January 2018 and April 2018 search authorizations. Finally, the military judge applied the Mil. R. Evid. 311(a)(3) balancing test and determined that exclusion of the evidence would not result in appreciable deterrence of future unlawful conduct. The military judge therefore denied the defense's motion to suppress in full.[22]

3. Law

a. Standard of Review

We review a military judge's ruling on a motion to suppress for an abuse of discretion, viewing the evidence in the light most favorable to the prevailing party. *United States v. Hoffman*, 75 M.J. 120, 124 (C.A.A.F. 2016) (citation omitted). A military judge abuses her discretion when: (1) her findings of fact are clearly erroneous; (2) she applies incorrect legal principles; or (3) her "application of the correct legal principles to the facts is clearly unreasonable."

[22] The military judge did not rule on whether SA MH could testify about what he saw during his 29 January 2018 search. SA MH did not testify during findings.

United States v. Ellis, 68 M.J. 341, 344 (C.A.A.F. 2010) (citing *United States v. Mackie*, 66 M.J. 198, 199 (C.A.A.F. 2008)). "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. Solomon*, 72 M.J. 176, 179 (C.A.A.F. 2013) (citation omitted).

"[O]n direct review, we apply the clear law at the time of appeal, not the time of trial." *United States v. Mullins*, 69 M.J. 113, 116 (C.A.A.F. 2010) (citing *United States v. Harcrow*, 66 M.J. 154, 159 (C.A.A.F. 2008)). Where an error is of constitutional dimensions, an appellate court must conclude the error was harmless beyond a reasonable doubt in order to affirm the result. *United States v. Condon*, 77 M.J. 244, 246 (C.A.A.F. 2018) (citing *United States v. Jerkins*, 77 M.J. 225, 228 (C.A.A.F. 2018)). An error is harmless beyond a reasonable doubt when it "did not contribute to the verdict." *Id*. (citing *United States v. Chisum*, 77 M.J. 176, 179 (C.A.A.F. 2018)).

b. Fifth Amendment

Servicemembers are generally entitled to the protections of the Fifth Amendment. *United States v. Tempia*, 37 C.M.R. 249, 254–55 (C.M.A. 1967). The Fifth Amendment provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself." U.S. CONST. amend. V. As "[t]he circumstances surrounding in-custody interrogation can operate very quickly to overbear the will of one merely made aware of his privilege by his interrogators[,] . . . the right to have counsel present at the interrogation is indispensable to the protection of the Fifth Amendment privilege." *Miranda,* 384 U.S. at 469. "Once a suspect in custody has 'expressed his desire to deal with the police only through counsel, [he] is not subject to further interrogation by the authorities until counsel has been made available to him, unless the accused himself initiates further communication.'" *Mitchell,* 76 M.J. at 417 (alteration in original) (quoting *Edwards,* 451 U.S. at 484–85); *see also* Mil. R. Evid. 305(e)(3).

Evidence derived from a custodial interrogation following the accused's invocation of his right to counsel and made outside the presence of counsel is generally inadmissible. Mil. R. Evid. 305(c)(2). However, evidence that would have been inevitably discovered without the illegally obtained information is an exception to this general rule. *See* Mil. R. Evid. 304(b)(3); *see also Mitchell*, 76 M.J. at 420.

For inevitable discovery to apply, the Government must "demonstrate 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 in a lawful manner." *Mitchell*, 76 M.J. at 420 (quoting *United States v. Wicks*, 73 M.J. 93, 103 (C.A.A.F.

2014)). "[M]ere speculation and conjecture" is not enough. *Wicks*, 73 M.J. at 103 (alteration in original) (quoting *United States v. Maxwell*, 45 M.J. 406, 422 (C.A.A.F. 1996)). "This exception is only applicable '[w]hen the routine procedures of a law enforcement agency would inevitably find the same evidence.'" *Id.* (alteration in original) (quoting *United States v. Owens*, 51 M.J. 204, 204 (C.A.A.F. 1999)).

c. Probable Cause and Search Authorizations

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, shall not be violated." U.S. CONST. amend. IV. It 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 Fourth Amendment requires that a search warrant describe the things to be seized with sufficient particularity to prevent a general exploratory rummaging in a person's belongings." *United States v. Richards*, 76 M.J. 365, 369 (C.A.A.F. 2017) (quoting *United States v. Carey*, 172 F.3d 1268, 1272 (10th Cir. 1999)). However, "the proper metric of sufficient specificity is whether it was reasonable to provide a more specific description of the items at that juncture of the investigation." *Id.* (quoting *United States v. Richards*, 659 F.3d 527, 541 (6th Cir. 2011)). "[I]t is folly for a search warrant to attempt to structure the mechanics of the search and a warrant imposing such limits would unduly restrict legitimate search objectives." *Id.* (alteration in original) (quoting *United States v. Burgess*, 576 F.3d 1078, 1094–95 (10th Cir. 2009)). The CAAF went on to state in *Richards*,

> In charting how to apply the Fourth Amendment to searches of electronic devices, we glean from our reading of the case law a zone in which such searches are 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.
>
> > On one hand, it is clear that because criminals can—and often do—hide, mislabel, or manipulate files to conceal criminal activity, a broad, expansive search of the hard drive may be required. . . . On the other hand, . . . granting the Government a *carte blanche* to search *every* file on the hard drive impermissibly transforms a "limited search into a general one."

Id. at 370 (omissions in original) (quoting *United States v. Stabile*, 633 F.3d 219, 237 (3d Cir. 2011)).

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) (citations omitted).

Under Mil. R. Evid. 315(f)(1), a military search authorization "must be based upon probable cause." Probable cause exists "when there is a reasonable belief that the person, property, or evidence sought is located in the place . . . to be searched." Mil. R. Evid. 315(f)(2). "Reasonable minds frequently may differ on the question whether a particular affidavit establishes probable cause, and we have thus concluded that the preference for warrants is most appropriately effectuated by according great deference to a magistrate's determination." *United States v. Leon*, 468 U.S. 897, 914 (1984) (internal quotation marks and citations omitted). "Close calls will be resolved in favor of sustaining the magistrate's decision." *United States v. Monroe*, 52 M.J. 326, 331 (C.A.A.F. 2000) (quoting *Maxwell*, 45 M.J. at 423).

A search authorization should not be found invalid by analyzing the underlying affidavit "in a hypertechnical, rather than a commonsense, manner." *United States v. Clayton*, 68 M.J. 419, 423 (C.A.A.F. 2010) (quoting *Illinois v. Gates*, 462 U.S. 213, 236 (1983)). "[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness.'" *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006) (citations omitted). In assessing the reasonableness of a search, we weigh the degree of the intrusion on the person's privacy against the degree to which the search promotes a legitimate governmental interest. *United States v. Gurczynski*, 76 M.J. 381, 386 (C.A.A.F. 2017) (citing *Riley v. California*, 573 U.S. 373, 385 (2014)).

When reviewing a search authorization, we "do not review a probable cause determination de novo;" rather we assess whether "the authorizing official had a 'substantial basis' for concluding that probable cause existed." *Hoffmann*, 75 M.J. at 125 (citation omitted). "A substantial basis exists '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.'" *United States v. Nieto*, 76 M.J. 101, 105 (C.A.A.F. 2017) (quoting *United States v. Rogers*, 67 M.J. 162, 165 (C.A.A.F. 2009)). The magistrate's probable cause determination is given "great deference" because of "the Fourth Amendment's strong preference for searches conducted pursuant to a warrant." *Id.* (quoting *Gates*, 462 U.S. at 236). Nonetheless, "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 *Leon*, 468 U.S. at 915). Probable cause requires the demonstration of "a sufficient nexus . . . between the alleged crime

and the specific item to be seized." *Id.* at 106. (citations omitted). In conducting this review, we look to the information that the authorizing official had at the time he made his decision. *United States v. Cowgill*, 68 M.J. 388, 391 (C.A.A.F. 2010) (citations omitted).

We ordinarily afford the magistrate's determination of probable cause great deference, but we recognize three exceptions to this general rule: (1) when the affidavit upon which the determination was based was prepared with knowing or reckless falsity; (2) when the magistrate is not neutral and detached or is serving as "a rubber stamp" for the police; or (3) when the affidavit fails to provide a substantial basis for a finding of probable cause or the determination is "a mere ratification of the bare conclusions of others." *United States v. Carter*, 54 M.J. 414, 419 (C.A.A.F. 2001) (quoting *Leon*, 468 U.S. at 914–15).

Searches conducted after obtaining a warrant or authorization based on probable cause are presumptively reasonable whereas warrantless searches are presumptively unreasonable unless they fall within "a few specifically established and well-delineated exceptions." *Hoffmann*, 75 M.J. at 123–24 (quoting *Wicks*, 73 M.J. at 99).

In regards to how to treat erroneous information in an affidavit, a court must sever "misstatements or improperly obtained information" from an affidavit and examine the remainder of the affidavit to determine if probable cause still exists. *United States v. Gallo*, 55 M.J. 418, 421 (C.A.A.F. 2001) (citation omitted).

In *United States v. Osorio*, this court addressed requirements regarding search warrants for computers—and by extension for stored electronic or digital media—when evidence of another crime is discovered, stating,

> [T]here must be specificity in the scope of the warrant which, in turn, mandates specificity in the process of conducting the search. Practitioners must generate specific warrants and search processes necessary to comply with that specificity and then, if they come across evidence of a different crime, stop their search and seek a new authorization.

66 M.J. 632, 637 (A.F. Ct. Crim. App. 2008).

d. Plain View

The plain view doctrine may "not be used to extend a general exploratory search from one object to another until something incriminating at last emerges." *Arizona v. Hicks*, 480 U.S. 321, 328 (1987) (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 466 (1971)). Under *Horton v. California*, 496 U.S. 128, 136–37 (1990), in 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.

e. Good Faith Exception and Exclusionary Rule

Evidence obtained as a result of an unlawful search is inadmissible against the accused if the accused: (1) makes a timely objection; (2) has an adequate interest, such as a reasonable expectation of privacy, in the person, place, or property searched; and (3) exclusion of such evidence "results in appreciable deterrence of future unlawful searches . . . and the benefits of such deterrence outweigh the costs to the justice system." Mil. R. Evid. 311(a)(3).

For the good faith exception to apply, the Government must establish that law enforcement's reliance on a defective authorization is "objectively reasonable." *Hoffmann*, 75 M.J. at 127 (citation omitted). The Government has the burden of establishing by a preponderance of the evidence the following: (1) the seizure resulted from a search and seizure authorization issued, in relevant part, by a magistrate; (2) the magistrate had a substantial basis for determining probable cause existed; and (3) law enforcement reasonably and in good faith relied on the authorization. Mil. R. Evid. 311(c)(3), (d)(5)(A); *see also Nieto*, 76 M.J. at 107 (citations omitted); *Carter*, 54 M.J. at 420 (citation omitted).

The second requirement is met if the person executing the search "had an objectively reasonable belief that the magistrate had a 'substantial basis' for determining the existence of probable cause." *United States v. Perkins*, 78 M.J. 381, 387 (quoting *Carter*, 54 M.J. at 422). The question 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) (quoting *Leon*, 468 U.S. at 922 n.23). We further "consider the objective reasonableness, not only of the officers who eventually executed a warrant, but also of the officers who originally obtained it or who provided information material to the probable-cause determination." *Leon*, 468 U.S. at 923 n.24.

The United States Supreme Court has identified four circumstances in which the "good faith exception" will not apply: (1) where the magistrate "was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth;" (2) where the magistrate "wholly abandoned his judicial role;" (3) where the warrant was based on an affidavit "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable;" and (4) where the warrant is so "facially deficient . . . in failing to particularize the place to be searched or the things to be seized . . . that the executing officers cannot reasonably presume it to be valid." *Id.* at 923 (citations omitted). The CAAF has harmonized

these four exceptions with the three requirements under Mil. R. Evid. 311(c)(3) by finding *Leon*'s first and third exceptions to be incorporated in Mil. R. Evid. 311(c)(3)'s second prong (magistrate having a substantial basis) and *Leon*'s second and fourth exceptions to be incorporated in Mil. R. Evid. 311(c)(3)'s third prong (good-faith reliance on the search authorization). *Carter*, 54 M.J. at 421.

The Supreme Court spoke in detail on application of the exclusionary rule in *Herring*. The Court stated,

> The fact that a Fourth Amendment violation occurred—*i.e.*, that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rule applies. Indeed, exclusion "has always been our last resort, not our first impulse," and our precedents establish important principles that constrain application of the exclusionary rule. . . . [T]he exclusionary rule is not an individual right and applies only where it "result[s] in appreciable deterrence." We have repeatedly rejected the argument that exclusion is a necessary consequence of a Fourth Amendment violation. Instead we have focused on the efficacy of the rule in deterring Fourth Amendment violations in the future.

555 U.S. at 140–41 (second alteration in original) (citations omitted).

Regarding the deterrence of future unlawful searches, the benefits "must outweigh the costs." *Id*. at 141. The Supreme Court has

> never suggested that the exclusionary rule must apply in every circumstance in which it might provide marginal deterrence. [T]o the extent that application of the exclusionary rule could provide some incremental deterrent, that possible benefit must be weighed against [its] substantial social costs. The principal cost of applying the rule is, of course, letting guilty and possibly dangerous defendants go free—something that offends basic concepts of the criminal justice system. [T]he rule's costly toll upon truth-seeking and law enforcement objectives presents a high obstacle for those urging [its] application.

Id. at 141–42 (alterations in original) (internal quotation marks and citations omitted).

4. Analysis

We find that the facts articulated in the military judge's ruling on the motion to suppress were not clearly erroneous, and we find that her conclusions of law are correct.

At the time of Appellant's interview with the AFOSI agents, the CAAF had not yet decided *Mitchell*. However, there is no debate on the illegality of AFOSI

agents asking Appellant to disable his passcode after he invoked his right to counsel. *See Mitchell*, 76 M.J. at 415. As such, the remaining issues are whether the military judge abused her discretion by finding the Government met its burden under the inevitable discovery doctrine, and if so, whether the good-faith exception would apply and whether the evidence should be excluded to deter future unlawful actions.

After the *Mitchell* violation, four searches of Appellant's phone occurred: in June 2017, when SA MH searched the contents after the first search authorization, and again in January 2018 after the second search authorization was granted; in March 2018, when Mr. TH searched the contents of Appellant's phone pursuant to the June 2017 and January 2018 search authorizations; and in April 2018, pursuant to all search authorizations. As this court recently noted in *United States v. Painter*, under the inevitable discovery doctrine we must view the situation as if SA MH had never asked Appellant to input his passcode, or that Mr. TH had never had the passcode to disable the security feature on his smartphone. No. ACM 39646, 2020 CCA LEXIS 474, at *34 (A.F. Ct. Crim. App. 23 Dec. 2020) (unpub. op.) (citing *United States v. Keller*, No. ACM 37729, 2013 CCA LEXIS 665, at *11 (A.F. Ct. Crim. App. 15 Jul. 2013) (unpub. op.) ("This requires a court to view the situation as it existed at the instant before the unlawful search and determine what would have happened had that unlawful search not occurred.")). With that factual landscape, we must determine whether the military judge abused her discretion when she concluded that "the inevitable discovery exception applie[d] in this case," as the "Government possessed, or w[as] actively pursuing evidence or leads that would have inevitably led to the discovery of the evidence in a lawful manner had not the illegality occurred."

a. June 2017 Search

At the time of the first search of Appellant's phone, AFOSI agents possessed a search authorization, the validity of which Appellant has never contested. SA CR had possession of Appellant's smartphone, informed Appellant of the authorization, and then asked Appellant to unlock his smartphone and disable the password.

We agree with the military judge that the military magistrate had a substantial basis for finding probable cause to seize Appellant's phone. Acting on information obtained from KL, AFOSI agents sought search authorization from a military magistrate to search "[Appellant]'s cell phone for text message conversations between [Appellant] and [KL] from 1 May 2017 to present." The military magistrate had a substantial basis to grant the request to search, as AFOSI agents outlined why the information AFOSI was looking for would be found at the location they identified. This was a fairly narrow request, based

on what KL disclosed to agents. The agents did not discover additional misconduct based on this search.

Appellant points out the AFOSI detachment lacked the capability to access locked phones, and at that time AFOSI did not communicate with DFC, Cellebrite, or DC3/CFL about whether those entities could access the phone in June 2017, and therefore, there was a possibility that a UFED extraction to recover the Snapchat messages would not have been successful. Yet, despite the lack of communications between those entities, the Government established it was ready and able to access Appellant's phone in June 2017. In her rulings on the June 2017 search of Appellant's phone, the military judge concluded "AFOSI possessed evidence of communications between [Appellant] and KL that AFOSI wanted to corroborate through evidence on [Appellant]'s phone." The investigation into KL's allegations was ongoing and developing, and given that AFOSI agents wanted to corroborate KL's messaging, SA CR's testimony that "he would have pursued every option to gain access" to Appellant's phone is credible. Finding a way to access Appellant's phone would have been a routine procedure for AFOSI agents, especially considering that the Government demonstrated that the phone could have been sent to CAS, which in June 2017 had the ability to unlock and access Appellant's phone. For inevitable discovery to apply, the Government must "demonstrate 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 in a lawful manner." *Mitchell*, 76 M.J. at 420 (quoting *Wicks*, 73 M.J. at 103). The Government met its burden of demonstrating by a preponderance of the evidence that the Government had the capability of unlocking Appellant's cell phone at the time the June 2017 illegality occurred.

b. 24 January 2018 Search Authorization and 29 January 2018 Search by Special Agent MH

The 24 January 2018 search authorization came about because trial counsel learned about KL and Appellant's social media communications. Trial counsel also learned that KL understood that Appellant had taken screenshots of his Snapchat messages to her because the messages he sent turned "gray." AFOSI agents were aware that KL and Appellant had communicated by Snapchat and Tinder, and therefore, when trial counsel sought this second search authorization, the agents were not presenting "new information" to the military magistrate.

Trial counsel recognized that the initial search authorization was too narrow and sought a broader authorization, to allow access to Appellant's social media applications and screenshots of communications. The search authorization was still fairly specific. It allowed the Government to search "[Appellant]'s

cell phone for any communications between [Appellant] and [KL] from 1 May 2017 to 16 June 2017, to include any data stored on the phone from social media messaging applications and/or screenshots of such communications." We find no abuse of discretion by the military judge in concluding that the military magistrate, Col JN, had probable cause to grant the 24 January 2018 search authorization and expand the search of Appellant's phone, and that the search authorization was reasonably "scoped" and lawful. We also agree with the military judge that once law enforcement found new evidence to support this new search authorization, agents were not precluded from modifying the initial June 2017 search authorization.

While SA MH's 29 January 2018 search was based on this valid search authorization, he conducted the search on a phone that was only unlocked and accessible to them because of the *Mitchell* violation. As the military judge rightfully recognized, unlike with the June 2017 search, where agents were actively pursuing leads and would have taken steps to access Appellant's phone, there was no evidence or testimony to suggest the agents were pursuing ways to access the phone without the passcode from Appellant. However, we agree with the military judge that the actions of SA MH did not impact Mr. TH's access to the phone. Despite SA MH's illegal search pursuant to the June 2017 *Mitchell* violation, Mr. TH would have still discovered the obscene anime material, as he was searching within the confines of the 24 January 2018 search authorization. In other words, as the military judge alluded, SA MH's illegal search had no impact on the legal search conducted by Mr. TH and his inevitable discovery of the evidence. We find no abuse of discretion on the part of the military judge regarding her rulings on this issue.

c. 28 March 2018 Search by Mr. TH

Based on the additional information provided by KL about her communications with Appellant, AFOSI agents sought an expanded search authorization to examine the social media accounts on Appellant's phone. However, the military judge found that the AFOSI agents did not have the capability to extract the information they were looking for in reliance on the 24 January 2018 search authorization. We agree with the military judge in her initial ruling that in an effort to actively pursue evidence against Appellant, AFOSI agents "needed to submit" Appellant's phone to DC3/CFL for assistance to conduct an "extraction and analysis relevant to the sexual assault allegation."

Once Mr. TH received the phone, he relocked it to conduct a brute force identification and extraction of the phone's data using DC3/CFL's Cellebrite software. The military judge made a notable conclusion based on Mr. TH's testimony: "[H]ad [Mr. TH] not relocked [Appellant]'s phone (putting it in the same locked status prior to the June *Mitchell* violation), the Cellebrite software would not have extracted the data" from the phone. This showed "the data that

Mr. [TH] searched on [Appellant]'s phone was accessed independently from [Appellant]'s *Mitchell* violation." Mr. TH's testimony that he was able to access Appellant's phone, with relative ease, supports the military judge's findings and conclusions on this issue.[23]

After Mr. TH accessed Appellant's phone, he conducted his search within the narrow parameters of the June 2017 and January 2018 search authorizations. When Mr. TH discovered Appellant's conversations with minors in plain view, he did exactly what the law would expect of an investigator: he stopped his search and relayed his discovery to AFOSI.

The military judge also found that even though Mr. TH was aware that there was suspected child pornography (based on the February 2018 search authorization), Mr. TH searched Appellant's phone within the confines of the lawful 24 January 2018 search authorization. The military judge's conclusion is supported by Mr. TH sending the AFOSI agents an email, asking for clarification on the parameters of his search.

As our colleagues on this court noted in *Painter,*

> In *Mitchell*, the CAAF concluded "the Government's eventual access to the phone's contents was not inevitable, but rather 'a matter of mere speculation and conjecture, in which [the Court] will not engage.'" Additionally, the majority in *Mitchell* specifically noted that the Government did not argue that a digital forensic examiner could have bypassed Mitchell's security. *Id*. at 420 n.8. That is not the case here—the Government clearly demonstrated that access to the pictures in the [ ] application was inevitable.

unpub. op. at *42 (first alteration in original) (citing *Mitchell*, 76 M.J. at 420) (quoting *Maxwell*, 45 M.J. at 422)). Much like *Painter*, the Government, through Mr. TH's convincing and credible testimony, clearly demonstrated that access to Appellant's social media accounts was inevitable. As such, we find the military judge did not abuse her discretion by finding the Government demonstrated by a preponderance of the evidence that Mr. TH would have inevitably discovered the contraband on Appellant's phone during the 28 March 2018 search.

---

[23] Mr. TH testified his confidence level in being able to "crack" a six-digit pin code was "[o]ne hundred percent." Had he been given Appellant's phone without the passcode on 16 June 2017 when it was seized, he was "still one hundred percent confident" he would have been able to unlock it.

d. 2 April 2018 Search Authorization and Subsequent Search by Mr. TH

Based on Mr. TH's 28 March 2018 discovery, the Government sought a fourth search authorization, and, on 2 April 2018, was given authorization to search "[Appellant]'s cell phone for text or social media communications with purported minors to include sexual communications via text or photographs."

Trial defense counsel objected to the 2 April 2018 search authorization on the basis the affidavit supporting the request contained information that had been suppressed as a result of SA MH's illegal search. Finding that the affidavit did have tainted information regarding the obscene anime material relied upon by the military magistrate, the military judge determined whether probable cause existed after severing that information from the affidavit. The military judge found that even without SA MH's observations, the military magistrate would still have had a substantial basis for determining probable cause existed based primarily on Mr. TH's observations and experience, and because Mr. TH had lawfully accessed Appellant's phone.

Operating under two lawful search authorizations—the January 2018 and April 2018 search authorizations—the military judge found inevitable discovery would apply to Mr. TH's search. We agree. Mr. TH saw obscene anime material, child pornography, and other obscene materials. Mr. TH notified the Government, who then sent him the 2 February 2018 search authorization. As the military judge found, "[e]ven if the initial *Mitchell* violations had not occurred and he was not made aware of the 2 February 2018 search authorization, Mr. [TH] would have discovered the evidence that led to the 2 April 2018 search authorization." Mr. TH's testimony clearly showed that it was not until he had already discovered this evidence, lawfully, that Mr. TH took any steps in reliance on the 2 February 2018 search authorization. We agree with the military judge that even if Mr. TH had known the 2 February search authorization was partially unlawful, it is reasonable to assume that Mr. TH would still have taken the same steps to receive clarification and/or additional search authorizations upon the discovery of new evidence.

e. Good Faith

The military judge found that even if the military magistrate's 2 April 2018 search authorization was not supported by probable cause due in part to the disclosure of the obscene anime material, the good faith exception would apply. The military judge concluded that (1) the search of Appellant's phone was conducted pursuant to a properly issued search authorization in June 2017; (2) the military magistrate had a substantial basis upon which to find probable cause; (3) the agents relied on good faith based on the verbal and written search authorizations in conducting their search of Appellant's phone; and (4) there

was no evidence that agents "intentionally or recklessly made false statements or omissions in the supporting affidavit." The evidence and testimony presented support the military judge's findings and conclusions on this issue, and this court specifically notes that every time additional evidence was discovered, AFOSI sought subsequent search authorizations. We also note the credible testimony from Mr. TH and the actions he took in executing the search authorizations. We find the military judge did not abuse her discretion in finding good faith would apply and that the requirements of Mil. R. Evid. 311(c)(3) were met.

f. Deterrence

Even if the above exceptions were not applicable in this case, applying the Mil. R. Evid. 311(a)(3) balancing test, we do not find the military judge abused her discretion in concluding that exclusion of the evidence obtained from Appellant's phone would not "result in an appreciable deterrence of future unlawful searches and seizures," and "the benefits of any such deterrence [did] not outweigh the costs to the justice system." Agents proactively sought search authorizations upon any indication that additional evidence against Appellant could be located, and Mr. TH's testimony shows that the evidence found on Appellant's phone would have been inevitably discovered even without Appellant's passcode. We have carefully considered the actions of the government agents with respect to searching Appellant's phone, and find their conduct does not warrant the severe reprimand of exclusion of evidence in this case. Having found a proper application of Mil. R. Evid. 311(c)(3), we find that the military judge did not abuse her discretion in denying Appellant's motion to suppress the contents of his phone.

B. Speedy Trial Pursuant to R.C.M. 707

1. Additional Facts

On 16 June 2017, AFOSI conducted its initial interview of Appellant. On 11 October 2017, a single charge was preferred for sexual assault of KL and on 5 January 2018, that charge was referred to general court-martial; however, upon the discovery of new evidence, on 26 April 2018, the convening authority withdrew and dismissed the charge and specification of sexual assault related to KL, "in order to provide an opportunity for revised charges to be preferred and considered for referral, if appropriate."

On 26 October 2018, three charges and seven specifications were preferred, including the initial charge related to KL. On 25 March 2019, two additional charges were preferred after the Article 32, UCMJ, preliminary hearing. On 8 April 2019, all charges and specifications were referred to general court-martial. Appellant was arraigned on 3 June 2019, and his trial began on 17 June 2019.

2. Law

"[W]hether an accused received a speedy trial is a legal question that is reviewed *de novo*." *United States v. Leahr*, 73 M.J. 364, 367 (C.A.A.F. 2014) (quoting *United States v. Cooper*, 58 M.J. 54, 58 (C.A.A.F. 2003)). A military accused may seek relief for alleged speedy trial violations under R.C.M. 707. *See United States v. Tippit*, 65 M.J. 69, 75 (C.A.A.F. 2007). "It is incumbent upon the government to arraign the accused within 120 days after the earlier of preferral of charges, the imposition of restraint, or entry on active duty. Where 'charges are dismissed . . . a new 120-day time period under this rule shall begin on the date of dismissal.' If charges are merely withdrawn and not subsequently dismissed, however, the R.C.M. 707 'speedy-trial clock continues to run.'" *Leahr*, 73 M.J. at 367 (omission in original) (citing *United States v. Britton*, 26 M.J. 24, 26 (C.M.A. 1988)).

3. Analysis

Appellant argues that he was not brought to trial within 120 days of preferral of charges, in violation of R.C.M. 707. A total of 221 days passed from when the charges were preferred on 26 October 2018 to 3 June 2019, when Appellant was arraigned. However, the convening authority excluded 118 days, upon request by both trial defense counsel due to their schedules.[24] Thus, taking into account the excluded time, only 103 days elapsed between preferral of charges and Appellant's arraignment, well within the 120-day period of the rule. Thus, we decline to grant relief on this issue.

C. Preemption and the Assimilated Article 134, UCMJ, Offense

1. Additional Facts

Additional Charge II and its specification alleged an assimilated offense under 18 U.S.C § 1466A, *Obscene visual representations of the sexual abuse of children*, in violation of Article 134, UCMJ. The specification alleged that Appellant

> did, within the Continental United States, on or about 16 June 2017, knowingly receive obscene visual depictions of a minor engaging in sexually explicit conduct, and such visual depictions were transported in interstate or foreign commerce by means of

[24] The convening authority excluded 13 November 2018 to 20 January 2019 (69 days), and from 21 January 2019 to 10 March 2019 (49 days) from the speedy-trial calculation.

> the internet, in violation of 18 U.S. Code 1466A, an offense not capital.[25]

This charge was based on a 23-page anime story, which contained graphic drawings depicting a father sexually assaulting his daughter. The story included words, conversations, and word bubbles directly incorporated within the novel. During his testimony, Mr. TH outlined how Appellant knowingly received these obscene visual representations on his cell phone.

2. Law

This court reviews questions of preemption de novo. *United States v. Benitez*, 65 M.J. 827, 828 (A.F. Ct. Crim. App. 2007) (citations omitted). "The preemption doctrine prohibits application of Article 134 to conduct covered by Articles 80 through 132." *Id.* (internal quotation marks and citation omitted); *see also United States v. Johnston*, No. ACM 39075, 2017 CCA LEXIS 715, at *4 (A.F. Ct. Crim. App. 16 Nov. 2017) (unpub. op.) (citing *Manual for Courts-Martial, United States* (2016 ed.), pt. IV, ¶ 60.c.(5)(a)).

In *United States v. Kick*, our superior court's predecessor, the United States Court of Military Appeals, defined the preemption doctrine as the

> legal concept that where Congress has occupied the field of a given type of misconduct by addressing it in one of the specific punitive articles of the code, another offense may not be created and punished under Article 134, UCMJ, by simply deleting a vital element. However, simply because the offense charged under Article 134, UCMJ, embraces all but one element of an offense under another article does not trigger operation of the preemption doctrine. In addition, it must be shown that Congress intended the other punitive article to cover a class of offenses in a complete way.

7 M.J. 82, 85 (C.M.A. 1979) (citations omitted); *see also United States v. Erickson*, 61 M.J. 230, 233 (C.A.A.F. 2005); *United States v. Hill*, No. ACM 38848, 2016 CCA LEXIS 291, at *2–3 (A.F. Ct. Crim. App. 9 May 2016) (unpub. op).

Accordingly, the preemption doctrine only precludes prosecution under Article 134, UCMJ, where two elements are met: "(1) 'Congress intended to limit prosecution for . . . a particular area' of misconduct 'to offenses defined in specific articles of the Code,' and (2) 'the offense charged is composed of a residuum of elements of a specific offense.'" *United States v. Curry*, 35 M.J. 359, 360–61 (C.M.A. 1992) (omission in original) (quoting *United States v. McGuinness*, 35

---

[25] Appellant visited the website associated with this charge the same day he was brought in by AFOSI for questioning and his cell phone seized, 16 June 2017.

M.J. 149, 151–52 (C.M.A. 1992)); *see also United States v. Wright*, 5 M.J. 106, 110–11 (C.M.A. 1978).

To be guilty of receipt of a child pornography offense under 18 U.S.C. § 1466A, Appellant must have knowingly received an obscene "visual depiction of any kind, including a drawing, cartoon, sculpture or painting, that depicts a minor engaging in sexually explicit conduct," provided the depiction had been mailed, shipped, or transported in interstate commerce by any means, including a computer. 18 U.S.C. §§ 1466A(a)(1), (d). The court notes that the enumerated offense under Article 134, UCMJ, for "receipt of child pornography" has a maximum punishment of 10 years of confinement, whereas the assimilated offense under 18 U.S.C § 1466A carries a maximum confinement period of 20 years.[26]

3. Analysis

Appellant argues that by assimilating 18 U.S.C § 1466A instead of charging Appellant under the enumerated Article 134, UCMJ, offense of receipt of child pornography, the Government "unlawfully and improperly subverted the intent of Congress and the President in creating the enumerated offense of 'receipt of child pornography' under Article 134, thereby preempting other charging assimilative methods." Appellant further argues that the Government's charging scheme "unlawfully exaggerate[d] the criminality of Appellant's misconduct through unreasonable multiplications of charges and multiplicious charging" and "unlawfully inflated Appellant's sentencing exposure."

In *Hill*, this court specifically addressed whether the preemption doctrine applied to the enumerated offense of child pornography under Article 134, UCMJ, and opined,

> [b]oth the *Manual* and *Kick* rely on an analysis of the power of the executive branch to act "where Congress has occupied the field." By contrast, the enumerated offense of child pornography was promulgated by the President. Accordingly, the preemption doctrine as described in the *Manual* and *Kick* does not apply.

Unpub. op. at *5. That is, the preemption doctrine does not prohibit the Government from charging a Clause 3, Article 134, UCMJ, offense for receipt of

---

[26] Violations under 18 U.S.C. § 1466A are subject to the penalties provided in 18 U.S.C. § 2252A(b)(2), which states that whoever violates that statute

> shall be fined under this title or imprisoned not more than 10 years, or both, but, if any image of child pornography involved in the offense involved a prepubescent minor or a minor who had not attained 12 years of age, such person shall be fined under this title and imprisoned for not more than 20 years . . . .

obscene visual representations of the sexual abuse of children through interstate commerce solely because the President has enumerated a different offense involving receipt of child pornography under Article 134, UCMJ. Even if we found the preemption doctrine applied to enumerated offenses under Article 134, UCMJ, we would still conclude that Additional Charge II and its specification is not a residuum of the enumerated offense of receipt of child pornography.

III. CONCLUSION

The findings and sentence entered are correct in law and fact, and no error materially prejudicial to the substantial rights of Appellant occurred. Articles 59(a) and 66(d), UCMJ, 10 U.S.C. §§ 859(a), 866(d). Accordingly, the findings and the sentence are **AFFIRMED**.

FOR THE COURT

Carol K. Joyce

CAROL K. JOYCE
Clerk of the Court