UNITED STATES ARMY COURT OF CRIMINAL APPEALS

Before the Court Sitting *En Banc*[1]

UNITED STATES, Appellee
v.
Staff Sergeant LADONIES P. STRONG
United States Army, Appellant

ARMY 20200391

Headquarters, Fort Stewart
G. Bret Batdorff, Military Judge
Colonel Joseph M. Fairfield, Staff Judge Advocate

For Appellant: Major Brian A. Osterhage, JA (argued); Colonel Michael C. Friess, JA; Jonathan F. Potter, Esquire; Captain Joseph A. Seaton, Jr., JA (on brief and reply brief); Major Joyce C. Liu, JA (on reply brief).

For Appellee: Captain Timothy R. Emmons, JA (argued); Colonel Christopher B. Burgess, JA; Lieutenant Colonel Craig J. Schapira, JA; Major Mark T. Robinson, JA; Captain Timothy R. Emmons, JA (on brief).

6 January 2023

OPINION OF THE COURT

BROOKHART, Senior Judge:

At a general court-martial, a panel of officers and enlisted members found appellant guilty of one specification of prevention of authorized seizure of property and one specification of negligent homicide in violation of Articles 131e and 134, Uniform Code of Military Justice, 10 U.S.C. §§ 931e and 934 (2019) [UCMJ], respectively. Appellant was sentenced to a bad-conduct discharge, confinement for three years, and reduction to the grade of E-1. The convening authority approved the findings and sentence.

Appellant's lone assignment of error is that all of her convictions are both legally and factually insufficient. We find appellant's conviction for the negligent homicide specification is both legally and factually sufficient and requires no further discussion. Appellant's conviction on the lone specification alleging prevention of

---

[1] Judge ARGUELLES decided this case while on active duty.

an authorized seizure bears further examination due to the unique nature of the property subject to that seizure, but ultimately warrants no relief.[2]

BACKGROUND

Appellant was a motor transport operator assigned to a transportation unit at Fort Stewart, Georgia. In the summer of 2019, appellant and members of her company were on temporary duty to the United States Military Academy at West Point, New York. Their mission was to support cadets who were performing a number of year-end training events in a mountainous training area near the Academy.

On 6 June 2019, appellant was part of a group tasked with transporting several dozen cadets in M1085 medium tactical vehicles to a land navigation course in the mountainous training area. The route selected for the mission was an unpaved single switchback road known as Firebreak 20. The firebreak cut through the downward slope of the mountain so that as one traveled towards the top of the mountain, the terrain on the left, or driver's side, sloped upward going away from the road. In turn, the terrain on the right, or passengers' side, sloped downward and dropped off steeply at various points. Trees and loose rocks, interspersed by gaps, lined both sides of the road. Since the route was not wide enough to accommodate two-way traffic, in the event drivers encountered oncoming traffic they were instructed to pull over to the "high side," meaning the upward sloping side, rather than towards the downward sloping side with frequent drop-offs, to allow the other vehicle to pass. While it was not ideal, appellant's command reconnoitered the route and determined it to be the best option available to accomplish the mission.

That morning, eight M1085s formed a convoy and departed the Academy grounds for the training exercise. Appellant's vehicle was last in the convoy and carried approximately twenty personnel. The vehicle immediately in front of appellant's had its rear flap open so that the cadets sitting in the back could see appellant's vehicle following behind them. At one point, the cadets in the vehicle ahead of appellant saw her vehicle strike a tree along the side of the road. At around that same time, some cadets in appellant's vehicle reported being jostled. Later, a cadet in the vehicle in front of appellant's vehicle grew concerned when he saw her vehicle drift toward the right, or drop-off side of Firebreak 20 before correcting back toward the middle of the road.

Shortly thereafter, the cadets in the preceding vehicle again saw appellant's vehicle veer toward the drop-off. This time, appellant was unable to correct course

[2] We have also given full and fair consideration to the matters submitted personally by appellant pursuant to *United States v. Grostefon*, 12 M.J. 431 (C.M.A. 1982), and find they lack merit and warrant neither discussion nor relief.

and her vehicle slowly slid sideways down the embankment before rolling over onto its top. The rollover injured a number of cadets in the back of appellant's vehicle. It also killed one cadet who was trapped between the bed of the truck and a boulder that protruded through the canvas top.

A relatively junior and inexperienced Private First Class served as the truck commander in appellant's vehicle. That particular duty required him to sit in the passenger seat and serve as an observer for the driver, warning her of any hazards she might not be able to see. Not seriously injured in the rollover, the truck commander was able to get out of the cab relatively quickly. However, other witnesses described him as somewhat hysterical due to the shocking experience. Nonetheless, the truck commander almost immediately reported that appellant had been on her phone at the time the vehicle rolled over. He later clarified that rather than using her phone, she was manipulating a smart watch on her wrist at the time of the accident. Smart watches typically display data relayed from the wearer's cellular phone.

Due to the loss of life, Criminal Investigation Command (CID) handled the investigation with assistance from the New York State police. Based on the truck commander's statements, CID agents obtained a warrant to seize appellant's Apple brand cell phone and smart watch for the purpose of extracting data. Later that evening, the CID Acting Senior Agent in Charge ("Agent") executed the warrant at appellant's billeting area on the Military Academy grounds.

The Agent, accompanied by a Noncommissioned Officer ("NCO") from appellant's unit, located appellant in her sleeping area, at which time the Agent identified herself to appellant as a CID agent. She further told appellant she had a warrant to seize appellant's cellular phone and smart watch. The Agent briefly left appellant alone with the NCO while appellant was getting dressed, instructing the NCO not to let appellant use her phone or watch. After the Agent heard the NCO say "you're not allowed to be on the phone" several times, she entered the room and saw appellant attempting to use her phone. Indeed, even after the Agent seized the phone, appellant tried multiple times to physically snatch the phone back out of the Agent's hands. Specifically, the Agent testified that appellant was "belligerent" in trying to take back her phone, such that the Agent finally had to tell her "at ease, Sergeant." The Agent also described how that was the only time in her career that she had to give such an admonishment to the subject of a seizure warrant.

After obtaining appellant's phone and watch, the Agent attempted to prevent any subsequent wireless signal alteration of the phone by placing it in airplane mode. Unable to get the phone in airplane mode, she instead placed it in what she believed was a "Faraday Bag," which was described as a container made of material designed to block incoming and outgoing electronic signals. The Agent then

transported the phone and watch to the nearest CID office with the personnel and equipment necessary to exploit any relevant digital media from electronic devices.

The evidence at trial demonstrated that a common feature of appellant's Apple iPhone and Apple account allowed her to remotely reset the phone to its original factory settings, effectively erasing all of the data stored on the phone. When the forensic analysts at the CID office began the process of extracting data from appellant's phone, they discovered that it had been remotely reset to factory conditions, and that all of the data on the phone had been erased. Upon further examination, the CID agents discovered that the Faraday Bag thought to have secured the phone was mislabeled by the manufacturer and did not actually have any capacity to block electronic signals. With respect to her Apple watch, the agents were unable to penetrate the device's security in order to search it.

After discovering that the phone was "wiped," CID agents obtained subsequent search warrants and served them on Apple and Verizon, which was appellant's cell phone carrier, in an effort to obtain appellant's account data. They also obtained a warrant for any other electronic devices appellant owned. The latter yielded an Apple iPad tablet and another Apple iPhone. A forensic analysis of the account data provided by Apple and the digital content of the newly seized devices revealed that shortly after her original cell phone was seized, appellant used her MacBook from a location near West Point to access her Apple account and initiate the remote factory reset. The factory reset process required knowledge of appellant's account credentials to include her password. At trial, the government's forensic expert explained that appellant was able to use the "Find My iPhone" application on her MacBook to access the backup data on the iCloud and remotely wipe her phone. Although not entirely clear, the forensic expert's testimony at trial appeared to confirm that appellant only had the ability to remotely wipe her entire phone, as opposed to manipulating specific pieces of data on the phone.

The investigation also discovered several internet searches initiated from appellant's internet protocol (ip) address for information on how to reset an Apple iPhone remotely. Finally, the forensic expert also testified that roughly 90 percent of the data he needed in order to determine whether appellant was on her watch or phone at the time of the fatal rollover would have been contained on her cell phone. Accordingly, appellant was charged with prevention of an authorized seizure under Article 131e, UCMJ.

On appeal, appellant avers that her cell phone was already seized at the time she remotely disposed of the data stored thereon, placing her conduct beyond the reach of the statute. We disagree.[3]

LAW AND DISCUSSION

A. Law

This court reviews questions of legal and factual sufficiency de novo. *United States v. Washington,* 57 M.J. 394, 399 (C.A.A.F. 2002). The test for factual sufficiency is "whether, after weighing the evidence in the record of trial and making allowances for not having personally observed the witnesses, *the members of the service court are themselves convinced of appellant's guilt beyond a reasonable*

---

[3] We are unpersuaded by the dissenter's argument that appellant's conviction under Article 131e is factually insufficient because the government did not admit the warrant or evidence of its specific contents, thereby creating reasonable doubt as to whether the cell phone data or just the cell phone was the authorized target of the seizure. As the dissent aptly notes, neither the warrant nor its contents are required elements of the offense as defined by the statute. Nor does the model specification in the Manual for Courts-Martial require any reference to a warrant or its contents. Instead, the statute requires only that appellant know that a person authorized to make seizures is seizing, about to seize, or endeavoring to seize certain property. The discussion to Article 131(e) refers to Military Rule of Evidence [Mil. R. Evid.] 316(d) for a list of persons authorized to conduct seizures. That list includes criminal investigators. *See Manual for Courts-Martial, United States* [MCM], pt. IV, ¶ 86; Mil. R. Evid. 316(d). In this case, the agent conducting the seizure testified that she identified herself to appellant as a CID agent who was there to seize her cell phone and smart watch as part of the fatal rollover investigation. Although the Agent did not specifically reference cell phone data, the record is replete with evidence that the Agent was endeavoring to seize appellant's cell phone data, rather than just the husk of the cell phone as the dissenters would have it. Most importantly to the government's burden, the evidence makes it quite clear appellant *knew* the data was the "certain property" targeted by the seizure because it was the data, rather than the cell phone, she undertook to dispose of using the remote reset feature. *See United States v. Braddock*, No. ACM 39465, 2019 CCA LEXIS 441, at *13 (A.F. Ct. Crim. App. Oct. 29, 2019) (*citing State v. Casady*, 491 N.W.2d 782, 787 (Iowa 1992)) (state of mind can be established by inferences reasonably drawn from the conduct of the accused); Dep't of Army Pam. 27-9, Legal Services: Military Judges' Benchbook, para 7-3 (10 September 2014) (knowledge and intent can be proven by circumstantial evidence). Finally, it is worth noting that discussion to Article 131(e) also states that it is not a defense to violation of the statute that a search or seizure was defective, further belying the necessity of a warrant to prove the charge.

doubt." *United States v. Rosario,* 76 M.J. 114, 117 (C.A.A.F. 2017) (citations and internal quotation marks omitted) (emphasis in original). This court applies "neither a presumption of innocence nor a presumption of guilt" but "must make its own independent determination as to whether the evidence constitutes proof of each required element beyond a reasonable doubt." *Washington,* 57 M.J. at 399. In reviewing for factual sufficiency, we are limited to the facts introduced at trial and considered by the court-martial. *United States v. Beatty*, 64 M.J. 456, 458 (C.A.A.F. 2007).

"'The test for legal sufficiency is whether, after viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt.'" *Rosario*, 76 M.J.at 117 (quoting *United States v. Gutierrez*, 73 M.J. 172, 175 (C.A.A.F. 2014)).

The elements of Article 131e, UCMJ, are:

> 1. That one or more persons authorized to make searches and seizures were seizing, about to seize, or endeavoring to seize certain property;
>
> 2. That the accused destroyed, removed, or otherwise disposed of that property with intent to prevent the seizure thereof; and
>
> 3. That the accused then knew that person(s) authorized to make searches were seizing, about to seize, or endeavoring to seize the property.

MCM, pt. IV, ¶86.b.

The statute criminalizes actions taken by an accused to prevent the seizure of property by authorized personnel. "Prevent" means to keep something from happening or existing.[4] Therefore, by definition, any action to "prevent" a seizure of property must occur before the seizure of the property. As such, the statutory phrase, "are seizing, are about to seize, or are endeavoring to seize" contemplates the destruction, removal, or disposal of the targeted property either before the seizure or while the seizure is ongoing. As appellant observes, it is not designed to cover conduct occurring after the property is seized. *See United States v. Hamilton*, 82 M.J. 530, 531 (Army Ct. Crim. App. 2022) ("[R]espect for Congress's prerogatives as policymaker means carefully attending to the words it chose rather

[4] Merriam-Webster Online Dictionary, https://merriam-webster.com/dictionary/prevent (last visited 3 Nov 2022).

than replacing them with others of our own. In short, words have meaning.") (internal citation omitted) (alteration in original).[5]

B. Factual Sufficiency Based on Missing Evidence at Trial

For her actions related to the phone and watch, the panel returned a guilty verdict on The Specification of Charge III, a violation of Article 131e, UCMJ.[6] Specifically, the Charge Sheet alleged that:

> [Appellant], U.S. Army, did, at or near West Point, New York, on or about 7 June 2019, with intent to prevent its seizure, obstruct, obscure, and dispose of the digital content of her cell phone, property [appellant] then knew a person authorized to make searches and seizures was endeavoring to seize. [7]

Neither the text of Article 131e, UCMJ, nor the explanation in Part IV of the *MCM*, define when a seizure is complete for purposes of the statute. However, in a different factual context, the Court of Appeals for the Armed Forces (CAAF) held that property is seized when there is "meaningful interference with an individual's possessory interest in that property." *United States v. Hahn*, 44 M.J. 360, 362 (C.A.A.F. 1996) (citing *United States v. Jacobsen*, 466 U.S. 109, 113 (1984)). In *Hahn*, agents found property in a third-party sailor's house that they suspected appellant had stolen. *Hahn, 44 M.J.* at 361. In order to confirm their suspicions, the agents directed the third-party to call appellant and tell him that agents were going to search his house that night and, therefore, appellant should come right away and

---

[5] In contrast, the federal civilian corollary to Article 131e, UCMJ, criminalizes similar conduct which occurs "before, during, or *after* any search for or seizure of property . . . ." 18 U.S.C. § 2232(a) (emphasis added).

[6] Prevention of Authorized Seizure of Property became an enumerated article with the passage of the Military Justice Act of 2016 on 1 January 2019. *See* National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, § 5448, 130 Stat. 2957. Previously, a nearly identical offense was among those listed in the general article.

[7] With respect to the second element of the offense: (1) the Charge Sheet uses the words "obstruct" and "obscure," in addition to "dispose of" to define appellant's conduct even though the former two words are not specifically set forth as means of violating Article 131e, UCMJ; and (2) the military judge likewise included these two terms, along with definitions, in his panel instructions. Nonetheless, given that a statutory means of violation was charged and instructed upon, the alternate terms are similar in meaning to those enumerated, and neither side objected to the Charge Sheet or the instructions, we find no error in the inclusion of these alternate terms.

retrieve his stolen property. *Id.* When appellant arrived shortly thereafter and took the property to his car, the surveilling agents quickly arrested him. *Id.*

On appeal, appellant argued that the agents constructively took possession of the property by identifying it as stolen and setting up the sting, and therefore the seizure was complete before he arrived to retrieve the property. *Id.* at 362. The CAAF disagreed, finding that the ease with which appellant was able to gather up the property and move it to his car negated any claim that there was a meaningful interference with his possessory interest. *Id.* The CAAF explained that "[t]he record does not reflect that these agents seized or even touched the property in question," and that appellant's theory "would require a holding that whenever a law enforcement agent observes stolen or contraband property and has the opportunity to wrest exclusive physical custody of it, as a matter of law the agent thereby has seized it at that moment." *Id.*

The reasoning in *Hahn* is ultimately applicable to this case even though here we confront digital data, which can be moved, stored, and disposed of in ways unique to its non-physical nature. Indeed, we recognize that incredible amounts of personal data are routinely stored on or accessed through modern smart phones. *Riley*, 573 U.S. at 393–94 (citing Kerr, Foreword: Accounting for Technological Change, 36 Harv. J. L. & Pub. Pol'y 403, 404–405 (2013); *United States v Flores-Lopez*, 670 F.3d.803, 806 (7th Cir. 2012)). In order to protect that data, a common feature of many cell phones, including appellant's Apple iPhone, allows users with internet access to remotely reset the phone to its original factory settings even if the phone is not in their possession. Resetting the phone effectively wipes all of the data stored on the phone at the time of the reset. *See e.g. Flores-Lopez*, 670 F.3d at 808 (stating remote wiping is available on all major platforms or can be bought separately). Testimony at trial also indicated that many cell phones, including appellant's, have the capacity, through a wireless connection, to automatically back-up data from the phone to a storage location separate from the phone itself, such as the iCloud. This wireless back-up function can be programmed to happen automatically at predetermined intervals, or when certain commands are entered by a user in possession of the phone. Like the factory reset, this back-up function protects user data by storing copies of data in the event the phone is lost, stolen, or simply stops functioning. Finally, although not at issue in this case, some cell phones can be enabled to automatically encrypt all the stored data on the phone if certain conditions are met, such as too many attempts to guess a phone's password. This feature also protects data on a lost or stolen phone. *See Riley*, 573 U.S. at 389.

Unfortunately, these practical privacy enhancements are equally useful to someone seeking to destroy incriminating data on a cell phone or remove it beyond the reach of law enforcement, even when they do not have physical possession of the phone. Given the capacity of these common features to impact potential evidence, it is no longer enough for law enforcement officials executing a warrant for digital

media to simply take possession of the physical device containing the media. To ensure the digital media is not remotely altered, destroyed, or rendered inaccessible after the physical device containing the data is lawfully seized, those executing seizures must take additional protective measures. *See* Dept. of Commerce, National Institute of Standards and Technology, R. Ayers, S. Brothers, & W. Jansen, Guidelines on Mobile Device Forensics 29 (SP 800-101 Rev. 1 May 2014); Interpol, Guidelines for Digital Forensics First Responders, Best Practices for Search and Seizure of Electronic and Digital Devices, (2021).

As described at trial, the protocols for seizing cell phones include placing the device in airplane mode and/or placing the seized device in a specialized container, such as a Faraday bag, designed to block incoming and outgoing wireless signals. These measures allow the seized device to be securely transported to a location where the digital media identified in the warrant can be securely extracted or copied. However, the testimony at trial revealed that these protocols are not foolproof. Faraday bags do not always block all incoming and outgoing signals. *See* Ashleigh Lennox-Steele & Alastair Nisbet, A Forensic Examination of Several Mobile Device Faraday Bags and Materials to Test Their Effectiveness (2016) (on file with Edith Cowan University Research Online); Eric Katz, A Field Test of Mobile Shielding Devices (Dec. 10 2010) (unpublished Purdue University College of Technology Masters Theses) (on file with Purdue University). Moreover, as the forensic examiner testified at trial, functions such as airplane mode can be password protected to prevent anyone other than the user from isolating the device from wireless signals. Accordingly, even when the physical device containing the data is in the hands of those authorized to seize it, the targeted data will often remain subject to active and passive alteration up until the time it is copied or extracted.

Based upon the foregoing, we find that the routine efforts of law enforcement to protect digital media on a seized physical device are part and parcel of the seizure of digital media. Under this analysis, a seizure is ongoing while those authorized to seize the property execute the protocols necessary to isolate and preserve the digital media. For purposes of Art. 131e, UCMJ, we further find that digital media is "seized," and beyond the reach of the statute, when the device containing it is secure from passive or active manipulation, even if that does not occur until the targeted data is copied or otherwise transferred from the seized device at some other location.

This framework is necessary to address both evolving technology and the ethereal nature of digital evidence. Moreover, it is consistent with the holding in *United States v. Hahn*, 44 M.J. 360 (C.A.A.F. 1996), because the only "possessory interest" of any relevance to Article 131e, UCMJ, is the capacity to destroy, remove, or otherwise dispose of the putative evidence. The law is unconcerned with whether Hahn still had sufficient possessory interest in stolen stereo equipment to listen to music on it, or whether appellant might be able to complete the day's Wordle on her cell phone. Rather, the only question for purposes of Article 131e, UCMJ, is

whether appellant maintained sufficient possessory interest in the item seized to destroy its evidentiary value; the very harm the statute is designed to prevent. In *Hahn*, the court found that the agents had not meaningfully interfered with Hahn's possessory interest in the stolen property precisely because he was still able to "remove" it, something also prohibited by the statute. *Id.* at 362.[8] Likewise, a suspect may maintain the capacity to effectively "gather up...and move" digital evidence even when the physical device containing it is in police hands. *Id.*

This framework is also consistent with the language of the statute which we are bound to honor. *Hamilton*, 82 M.J. at 531. Seize is a verb meaning to "take possession of by legal process."[9] "Endeavor," when used as a verb means to "attempt . . . by exertion of effort."[10] Both "seizing" and "endeavoring" are present participles, which are verbs that form a continuous tense. Present participles describe actions that are ongoing, such as running, lifting, or writing.[11] As such, "endeavoring to seize" describes someone exerting effort to seize an item.

It is a basic tenet of statutory construction that the language of the statute must be interpreted such that each clause has independent meaning. *See* Antonin Scalia & Bryan A. Garner, Reading Law: The Interpretation of Legal Texts, 174 (2012) (defining the "Surplusage Canon" as the requirement that "[i]f possible, every word and every provision is to be given effect," and "[n]one should be ignored"). Accordingly, "seizing," "about to seize," and "endeavoring to seize" must be read to have independent meanings and operate to criminalize distinct conduct. To that end, we believe Congress intended "seizing" to criminalize intentional efforts to destroy, remove, or otherwise dispose of property at the time when authorized officials are in the act of physically taking control of the evidence, such as when a suspect swallows evidence or flushes it down a toilet as agents attempt to take it from his person. We further find "endeavoring to seize" addresses situations where the seizure has progressed to the point where the authorized persons have some degree of physical control over the seized evidence but are still actively securing it in accordance with their applicable procedures. An example of

---

[8] Presumably, had Hahn destroyed the evidence in the apartment's living room while the NIS agents waited outside, he would have been equally guilty of violating the former Article 131e.

[9] Merriam-Webster Online Dictionary, https://merriam-webster.com/dictionary/seize (last visited 29 Sep 2022).

[10] Merriam-Webster Online Dictionary, https://merriam-webster.com/dictionary/endeavor (last visited 29 Sep 2022).

[11] Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/present%20participle (last visited 29 Sep 2022)

endeavoring to seize physical evidence would be when agents are preserving, marking, and packaging evidence for removal from the scene of the seizure and transportation to the facility where it will be stored or analyzed.[12]

In this case, persons authorized to seize appellant's phone and the digital media contained therein physically seized the phone and according to their protocol for such evidence, attempted to turn-off the phone's wireless communications function. When that effort failed, the agent further endeavored to secure the seized data by placing the phone in a container designed to block wireless signals. [13] The fact that the container was mislabeled and had no capacity to block wireless signal does not relieve appellant of her criminal liability because even a properly marked and functioning Faraday container is not foolproof. Therefore, even though the physical device was in law enforcement custody, the seizure was ongoing because like Hahn, appellant still had sufficient access to the data on the phone, whether "authorized"[14] or not, to dispose of it in precisely the manner the seizing authority sought to prevent. As the Court in *Hahn* might say, "witness the ease with which

---

[12] Although not at issue in this case, we believe "about to seize" encompasses scenarios where the subject is aware that authorized persons intend to seize the property but have not yet arrived at the location of the property or otherwise began their efforts. The scenario in *Hahn*, where Hahn sought to remove the evidence when he learned law enforcement would soon be coming, is such an example.

[13] The unique nature of digital media often defies hypotheticals premised on physical property. *United States v Wicks*, 73 MJ 93, 102 (C.A.A.F. 2014) ("not good enough" to analogize a cell phone to a container for 4th Amendment purposes). Nonetheless, we agree that the dissent's example describes the facts of this case, although here appellant did not need to physically remove the cell phone from the trunk of the law enforcement vehicle in order to dispose of its contents because through an inherent feature of her cell phone, she maintained sufficient possessory interest in the data to access it remotely. Accordingly, we are unmoved.

[14] The dissent concludes that once the physical device was in the Faraday bag, the seizure was complete because appellant no longer had "authorization" to access it. However, we find the concept of "authorization" is ultimately at odds with a statute criminalizing the destruction of evidence even before its seizure. Hahn did not have authorization to remove the stolen property from his associate's apartment as evidenced by his arrest as soon as he did so. Nonetheless, our superior court upheld his guilty plea for violating the predecessor to Art. 131e, UCMJ. Conversely, during the timeframe that investigators were "about to seize" appellant's phone, she seemingly had authorization to possess both it and the data on it, however, it would have still been a violation of Art. 131e for her to destroy either. Accordingly, the question is not whether appellant had "authorization" to access the phone or the data, but whether agents were still endeavoring to seize it when she did.

appellant was able to delete the digital media." Accordingly, we find the evidence demonstrated appellant intentionally destroyed the data on her phone while law enforcement agents were still "endeavoring to seize" it by transporting it to a location where the data could be securely extracted or copied. Appellant's conviction is both legally and factually sufficient.[15]

CONCLUSION

The findings of guilty and sentence are AFFIRMED.

Senior Judge WALKER, Senior Judge FLEMING, Judge HAYES, Judge MORRIS, and Judge PARKER concur;

ARGUELLES, Judge, joined by SMAWLEY, Chief Judge, and PENLAND, Judge dissenting;

I concur with the majority's ruling as to the negligent homicide specification. For three reasons, however, I respectfully disagree with my colleagues' determination that Appellant's conviction on The Specification of Charge III was legally and factually sufficient. First, there was insufficient evidence as to what the

[15] In addition to finding the Article 131e conviction legally and factually insufficient, the dissent would exercise our statutory "should be approved" power to set aside that conviction due to a waived instructional error. *Contra United States v Nalezynski,* ARMY 20200038, 2021 CCA LEXIS 509 at *9 (Army Ct. Crim. App. 30 Sep. 2021) (mem. op.). However, where the military judge otherwise correctly defined the elements, we find no error in his use of the colloquial "cell phone" rather than the expansive "digital content of her cell phone" in his charge to the panel. While careful distinction between the two might be necessary in the Fourth Amendment context, "syntactical nicety is not the standard for instructional adequacy." *United States v Alford*, 31 M.J. 814, 819 (A.F.C.M.R. 1990) (citing *United States v. Truman*, 19 U.S.C.M.A. 504, 507, 42 C.M.R. 106, 109 (1970)). Accordingly, we are confident that the instructions as a whole were legally correct and did not mislead the panel. *Alford*, 31 M.J. at 819. *See also United States v. Prather*, 69 M.J. 338, 344 (C.A.A.F. 2011) (quoting *Humanik v. Beyer*, 871 F.2d 432, 441 (3d Cir. 1989)) (instructions are reviewed in the "context of the overall message conveyed to the [panel]."). Further, irrespective of waiver, we find no reasonable possibility that the findings or sentence would be any different had the instructions included the words "digital content of her cell phone" as the dissenters believe was required. *United States v Wolford*, 62 MJ 418, 420 (C.A.A.F. 2006). In the absence of error or any arguable prejudice there are no permissible grounds to exercise our twilighting "should be approved" authority under Article 66. See National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 542(b), 134 Stat. 3611.

Agent was "authorized" to search for, and in any event, appellant's destruction of the cell phone data did not occur as agents were "about to seize" the data. Alternatively, because the military judge's instructional errors on this specification were not harmless beyond a reasonable doubt, the Article 131e specification must be set aside.

LAW AND DISCUSSION

A. Law

This court reviews questions of legal and factual sufficiency de novo. *United States v. Washington,* 57 M.J. 394, 399 (C.A.A.F. 2002). The test for factual sufficiency is "whether, after weighing the evidence in the record of trial and making allowances for not having personally observed the witnesses, *the members of the service court are themselves convinced of appellant's guilt beyond a reasonable doubt.*" *United States v. Rosario,* 76 M.J. 114, 117 (C.A.A.F. 2017) (citations and internal quotation marks omitted) (emphasis in original). This court applies "neither a presumption of innocence nor a presumption of guilt" but "must make its own independent determination as to whether the evidence constitutes proof of each required element beyond a reasonable doubt." *Washington,* 57 M.J. at 399. In reviewing for factual sufficiency, we are limited to the facts introduced at trial and considered by the court-martial. *United States v. Beatty*, 64 M.J. 456, 458 (C.A.A.F. 2007).

"The test for legal sufficiency is whether, after viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *Rosario*, 76 M.J.at 117 (quoting *United States v. Gutierrez*, 73 M.J. 172, 175 (C.A.A.F. 2014)).

The elements of Article 131e, UCMJ, are:

> 1. That one or more persons authorized to make searches and seizures were seizing, about to seize, or endeavoring to seize certain property;
>
> 2. That the accused destroyed, removed, or otherwise disposed of that property with intent to prevent the seizure thereof; and
>
> 3. That the accused then knew that person(s) authorized to make searches were seizing, about to seize, or endeavoring to seize the property.

Manual for Courts-Martial, United States (*MCM*), pt. IV, ¶86.b.

The statute criminalizes actions taken by an accused to prevent the authorized seizure of property. "Prevent" means to keep something from happening or arising. Therefore, by definition, any action to "prevent" a seizure must occur before the seizure of the property. As such, the statutory phrase, "seizing, are about to seize, or are endeavoring to seize" contemplates the destruction, removal, or disposal of the targeted property either before the seizure or while the seizure is ongoing.

B. Factual Sufficiency Based on Missing Evidence at Trial

For appellant's actions related to the phone and watch, the panel returned a guilty verdict on The Specification of Charge III, a violation of Article 131e, UCMJ. As noted above, the Charge Sheet alleged that:

> [Appellant], U.S. Army, did, at or near West Point, New York, on or about 7 June 2019, with intent to prevent its seizure, obstruct, obscure, and dispose of the digital content of her cell phone, property [appellant] then knew a person authorized to make searches and seizures was endeavoring to seize.

Although the specification alleged that appellant acted with the intent to prevent the seizure of "the digital content of her cell phone," the actual warrant authorizing such a seizure was *not* introduced into evidence, nor is it anywhere in the Record of Trial. To the contrary, the only evidence introduced at trial pertaining to the scope of the warrant was the Agent's testimony that "[w]e applied for a search authorization – a search warrant to seize" appellant's watch and phone. On cross-examination, the Agent also explained why it was important to preserve digital evidence when seizing a cell phone, to include placing the phone into airplane mode and properly securing it in a Faraday Bag. The Agent did *not*, however, provide any further testimony about whether the warrant in this case authorized the seizure of: (1) the "cell phone" itself; (2) the cell phone and its digital content (as charged by the Government); or (3) the cell phone, its data, and any data simultaneously stored in the iCloud.

Likewise, trial counsel told the panel in his opening statement that the Agent executed "a search warrant to seize the phone from" appellant, and argued in his closing that the Agent "seized that watch, seized the cell phone." Conversely, there was *no* evidence introduced at trial that the applicable warrant in any way authorized the seizure of the data on appellant's phone, much less any of her backup data that might be stored or accessible in the iCloud.

While the government could have charged appellant with interfering with the physical seizure of the phone based on her interaction with the Agent at the barracks, it instead elected to allege that she interfered with the seizure of "the digital content of her cell phone" in order to capture her subsequent conduct in digitally "wiping" her phone after it was taken. This is a significant point of

departure from the majority's reasoning: the phone's digital content is different from the phone itself. As such, the government was bound by its charging decision to prove that there was in fact authorization for the seizure of the digital content of appellant's phone. *United States v. English*, 79 M.J. 116, 120 (C.A.A.F. 2019) (holding that government is bound to prove the facts as alleged).

With respect to the basis for such a lawful seizure, there is no dispute that in the military context there are multiple sources of "authorization" for such a seizure, to include a search warrant, lawful inspections and inventories, exigent circumstances, and/or searches and seizures conducted upon entry to an installation. In the instant analysis, however, we are not suggesting that Article 131e contains an additional search warrant or probable cause element, but rather take issue with any argument that the first element of that statute requires only a "general" or free-floating authorization to conduct seizures, untethered to any specific lawful basis for such a seizure.

Put another way, because the "authorization of the person" to seize the item at issue is a mandatory condition precedent to examining the accused's knowledge and intent, absent evidence that there was some specific lawful basis for the seizure, be it via search warrant, inspection, or otherwise, there is simply no basis to establish the first element of Article 131e. To interpret the first element of the statute as requiring only a "general" authorization would mean that an accused could be found guilty for resisting a CID agent who simply walked up to her on the street and attempted to seize her phone without any lawful authorization. As such a result would defy both logic and common sense, we cannot accept such an interpretation of Article 131e. *Cf. United States v. Cote*, 72 M.J. 41, 42 (C.A.A.F. 2013) (holding that in general "the search and seizure conducted under the warrant must conform to the warrant or some well-recognized exception") (citations omitted); Dep't of Army Pam. 27-9, Legal Services: Military Judges' Benchbook, para. 3-96-1 (10 Sep. 2014) (in the context of obstruction of justice, "'criminal proceedings' includes *lawful* searches") (emphasis added). Finally, for the same reasons, it follows that in the absence of evidence of the source for a lawful seizure, any "good faith" on the part of the Agent is entirely irrelevant.[16]

---

[16] Military Rule of Evidence [Mil.R.Evid.] 316 does not provide the "free-floating" source of authorization for the first element of Article 131e. To the contrary, this evidentiary rule pertains only to the "admissibility" of seized evidence, providing that even absent a warrant or other lawful authorization, evidence of a crime seized by a CID agent acting in good faith may still be *admissible* at trial. Mil.R.Evid. 316(c)(1), (d). But interpreting such an evidentiary rule regarding the *admissibility* of seized property as definitively settling the question of what authority is required for a seizure under Article 131e is a *non sequitur*. Indeed, given that Mil.R.Evid.

(continued . . .)

We further recognize that when viewing the evidence in the light most favorable to the government, an argument can be made that the panel may have reasonably inferred that the warrant also authorized the seizure of the "digital content" of appellant's phone. Indeed, although the government elected to charge the object of the offense as "the digital content of her cell phone" and conceded at oral argument that there is a distinction between a cell phone and its digital contents, counsel also argued that we can infer from the Agent's testimony that the missing warrant must have authorized seizure of the phone's digital content. First, to the extent the government is asking us to draw such inferences from the evidence, that is relevant only to our *legal* sufficiency review. *See Rosario*, 76 M.J.at 117 (holding that the test for legal sufficiency is whether, after viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt."). In making our *factual* sufficiency determination, we apply no presumptions as to guilt or innocence, but are instead required to make our own "independent determination as to whether the evidence constitutes proof of each required element beyond a reasonable doubt." *Washington,* 57 M.J. at 399.

As such, the fact that the Agent apparently recognized the need to preserve digital content when seizing cell phones, and/or may have had a "good faith" belief that she was authorized to seize the data, does not answer the question of what the scope of the warrant was in this case, nor is it enough to conclusively establish that the warrant expressly authorized the seizure of "the digital content of [appellant's] cell phone." Indeed, numerous federal courts have recognized that there is a distinction between a warrant authorizing seizure of a phone, and a warrant authorizing seizure of its digital contents. *See e.g. United States v. Wecht*, 619 F.Supp.2d 213, 247 (W.D. Pa. 2009) ("[T]he law recognizes a distinction between the seizure of computer equipment on one hand and, on the other hand, the seizure of information stored *within* the computer equipment . . . . when the government seeks to seize the information stored on a computer, as opposed to the computer itself, that underlying information must be identified with particularity") (emphasis in original) (citation omitted); *Cf. Riley v. California,* 573 U.S. 373, 401 (2014) ("Our holding, of course, is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell

---

(. . . continued)
316(d) expressly limits its application to property seized "pursuant to this rule", any assertion that the definitions in Mil.R.Evid. 316 govern the "authorization" requirement of Article 131e is ambiguous at best, and would violate the rule of lenity. *See United States v. Davis*, 139 S.Ct. 2319, 2333 (2019) (the rule of lenity requires that ambiguities concerning the breadth of a criminal statute be resolved in the defendant's favor); *United States v. Thomas*, 65 M.J. 132, 135 n.2 (C.A.A.F. 2007) ("We have long adhered to the principle that criminal statutes are to be strictly construed, and any ambiguity resolved in favor of the accused.").

phone is seized incident to arrest."); *United States v. Wicks*, 73 M.J. 93, 102 (C.A.A.F. 2014) ("Because of the vast amount of data that can be stored and accessed, as well as the myriad ways they can be sorted, filed, and protected, it is not good enough to simply analogize a cell phone to a container").

Finally, accepting the government's invitation to find factual sufficiency on the grounds that there is no real difference between the term "cell phone" and its digital content would require us to except the words "digital content" out of the specification, an action we are precluded from taking under prior CAAF precedent. *See English*, 79 M.J. at 121 (holding that "there is no authority, statutory or otherwise, that permits the ACCA to except language from a specification in such a way that creates a broader or different offense than the offense charged at trial.").

In short, given the context of this case, we cannot make a factual sufficiency determination without knowing the specific wording of the warrant authorizing the seizure. If, as described by the Agent at trial, the warrant authorized the seizures of only the watch and the phone, appellant cannot be guilty of interfering with those seizures by wiping the phone of its digital content after it was no longer in her possession. On the other hand, if the warrant more broadly authorized the seizure of the phone, the data contained on the phone, and any of the phone's backup data in the iCloud, there would likely be no factual sufficiency issue. And, if as expected, the actual authorization of the language of the missing warrant was somewhere in between these two extremes, our factual sufficiency determination would necessarily turn on the exact words used. *See Cote*, 72 M.J. at 42 (holding that in general "the search and seizure conducted under the warrant must conform to the warrant").

In sum, since the only evidence pertaining to the actual scope of the warrant's seizure authorization was the Agent's testimony that she "applied for a search authorization – a search warrant to seize" appellant's watch and phone, combined with the fact that the government's opening statement/closing argument focused the panel members on the phone itself, and not its digital content, the government failed to meet its burden of proof as to the "condition precedent" for the first element of Article 131e. In other words, the government failed to prove beyond a reasonable doubt that the Agent was in fact authorized "to seize certain property." Indeed, because we can only speculate about the extent of the authorized seizure and what "certain" property was at issue, we are not convinced that the evidence at trial "constitutes proof of each required element beyond a reasonable doubt." Accordingly, the guilty finding on The Specification of Charge III is factually insufficient. *See United States v. Christensen*, ARMY 20190197, 2021 CCA LEXIS 159 at *4-5 (Army Ct. Crim. App. 29 Mar. 2021) (mem op.) (holding that a lack of evidence supporting the panel's finding renders appellant's conviction factually insufficient); *United States v. Brown*, ARMY 20180176, 2019 CCA LEXIS 313 at *4-5 (Army Ct. Crim. App. 31 Jul. 2019) (mem op.) (same).

C. Remote Deletion of Data on Phone

Alternatively, and even setting aside the evidentiary issue discussed above, because appellant's destruction of the cell phone data did not occur as agents were "about to seize" the data, the evidence is still factually insufficient to support the guilty verdict for the Article 131e specification.

Neither the text of Article 131e, UCMJ, nor the explanation in Part IV of the *MCM*, define when a seizure is complete. However, in a different factual context, the Court of Appeals for the Armed Forces (CAAF) held that property is seized for purposes of the statute in question when there is "meaningful interference with an individual's possessory interest in that property." *United States v. Hahn*, 44 M.J. 360, 362 (C.A.A.F. 1996) (citing *United States v. Jacobsen*, 466 U.S. 109, 113 (1984)). In *Hahn*, agents found in a third-party sailor's house property that they suspected appellant had stolen. *Hahn, 44 M.J.* at 361. In order to confirm their suspicions, the agents directed the third-party to call appellant and tell him that, since agents were going to search his house that night, appellant should come right away and retrieve his stolen property. *Id.* When appellant arrived shortly thereafter and took the property to his car, the surveilling agents quickly arrested him. *Id.*

On appeal, Hahn argued that the agents constructively took possession of the property by identifying it as stolen and setting up the sting, and that the seizure was complete before he arrived to retrieve it. *Id.* at 362. The CAAF disagreed, finding that the ease with which appellant was able to gather up the property and move it to his car negated any claim that there was a meaningful interference with his possessory interest. *Id.* The CAAF explained that "[t]he record does not reflect that these agents seized or even touched the property in question," and that appellant's theory "would require a holding that whenever a law enforcement agent observes stolen or contraband property and has the opportunity to wrest exclusive physical custody of it, as a matter of law the agent thereby has seized it at that moment." *Id.*

This case is distinguishable from *Hahn* on multiple levels, including the fact that we are dealing here with "data" potentially stored on the phone and elsewhere. Indeed, we recognize that incredible amounts of personal data are routinely stored on or accessed through modern smart phones. *Riley*, 573 U.S. at 393–94 (citing Kerr, Foreword: Accounting for Technological Change, 36 Harv. J. L. & Pub. Pol'y 403, 404–405 (2013); *United States v Flores-Lopez*, 670 F.3d.803, 806 (7th Cir. 2012)). In this case, the evidence at trial revealed that appellant's Apple iPhone and accompanying Apple account had a commonly available feature that allowed an owner not in possession of the phone to access the account through another device and remotely delete all of the data, or digital media, by restoring factory settings. *See e.g. Flores-Lopez*, 670 F.3d at 808 (stating remote wiping is available on all major platforms or can be bought separately). The obvious benefit of this feature is

that if the phone is lost or stolen, the owner can prevent exposure of any personal data on it.

Given this common feature on cellular phones, law enforcement officials executing a warrant for digital media stored on an electronic device generally take measures to prevent the alteration or destruction of the digital media after the device is lawfully seized. *See, e.g.,* Dept. of Commerce, National Institute of Standards and Technology, R. Ayers, S. Brothers, & W. Jansen, Guidelines on Mobile Device Forensics 29 (SP 800-101 Rev. 1 May 2014); Interpol, Guidelines for Digital Forensics First Responders, Best Practices for Search and Seizure of Electronic and Digital Devices, (2021). As noted above, testimony at trial revealed that Army law enforcement agents generally follow several protocols to protect digital media from active or passive manipulation after seizure of the physical device. For cellular phones, one step involves placing the device in airplane mode, which effectively prevents the device's communication with wireless data streams. Additionally, CID agents will often place seized devices in Faraday bags, or similar containers, to block wireless signals from accessing or leaving the devices. These preventative measures generally allow for secure transportation of a device to an appropriate location for *search* and extraction of relevant digital media.

Finally, in *Jacobsen*, the case cited in *Hahn*, the Supreme Court held that "the agents' assertion of dominion and control over the package and its contents" constituted a seizure. 466 U.S. at 120. Likewise, in *United States v. Eugene*, ARMY 20160438, 2018 CCA LEXIS 106, at *7 (Army Ct. Crim. App. 28 Feb. 2018) (mem. op.), we reiterated that with respect to a seizure, there is a meaningful interference with an individual's possessory interest when "law enforcement [] exercise[s] a fair degree of dominion and control over the property." As such, we held that because "meaningful interference" occurred when appellant's wife consented to the seizure of the cell phone and provided it to CID, the "seizure was therefore complete." *Id.*; *Cf. Cote*, 72 M.J. at 45 (seizure of appellant's electronics interfered with his possessory interest in the noncriminal matters that were part of the digital content); *Fox v. Van Oosterum*, 176 F.3d 342, 351 (6th Cir. 1999) ("[T]he Fourth Amendment protects an individual's interest in *retaining* possession of property . . . . Once that act of taking the property is complete, the seizure has ended and the Fourth Amendment no longer applies.") (emphasis added); *Texas v. Brown*, 460 U.S. 730, 747 (1983) (stating a seizure threatens a citizen's interest in "*retaining* possession of property") (Stevens, J., concurring) (emphasis added).

Appellant now contends that her conviction under Article 131e, UCMJ, is legally and factually insufficient because CID agents had already seized her phone and its digital content by the time she remotely destroyed the data. We agree.

Simply put, and notwithstanding her testimony that Faraday Bags are "not completely" foolproof, once the Agent put appellant's phone into the Faraday Bag,

the seizure was for all intents and purposes complete, because appellant no longer had authorization to possess either the phone or its digital contents. While the defective Faraday Bag may have provided appellant with the opportunity to destroy the data remotely, the Agent's negligence is simply not the legal equivalent of providing appellant with meaningful access to her phone and its data. To the contrary, in order to uphold appellant's Article 131e, UCMJ, conviction based on her conduct in deleting the data after the Agent took her phone, we would have to conclude that the Agent's negligence in failing to properly secure the phone necessitated a finding that the government was still somehow *unknowingly and inadvertently* "endeavoring" to seize the phone and its data, up until the point when the agents finally got around to attempting to extract the data. That is a leap of logic we are not willing to make, as we decline to read *Hahn* as standing for the proposition that, for a seizure to be complete, law enforcement agents must eliminate any and all possible access to the seized item or items. Rather, once the Agent put the phone in the Faraday Bag and secured it, law enforcement asserted a "fair degree" of dominion and control over both the phone and its data, such that the seizure was complete. *Jacobsen*, 466 U.S. at 120; *Eugene*, 2018 CCA LEXIS 106, at *7.

To the extent the government argues that as a result of the Agent's negligence, and/or because Faraday Bags are not completely foolproof, there was no "meaningful interference" with appellant's "possessory interest" as *Hahn* defined that term, we disagree. First, in *Hahn* the appellant was able to physically pick up and move the property into his car before the agents took physical possession of it, and the CAAF specifically noted "[t]he record does not reflect that these agents seized or even touched the property in question [before appellant moved it]." 44 M.J. at 362. Moreover, the core holding in *Hahn* was that a law enforcement agent did not as a matter of law seize property the moment he observed it. *Id.* Unlike in *Hahn*, in this case there is no dispute that the Agent "seized or even touched" the phone. Nor is there any claim the Agent "seized" appellant's phone before taking physical custody of it. Likewise, because *Hahn* is silent on the issue of what happens when law enforcement physically takes an item but negligently fails to secure it, that case is inapposite.

A hypothetical example is illustrative. First, assume that appellant in this case was not present when the search occurred, and that after finding the phone, the agents put it in their trunk, failed to close the trunk, and then went back into barracks to search for more electronic devices. Then assume that upon her return while the agents were still executing the warrant, appellant saw the agents heading back into the barracks, and reached into the open trunk to take back her phone. In such a case, we would give short shrift to any claim that the agents' negligence in failing to shut the trunk meant that they were still somehow "endeavoring" to seize the phone and/or that the government failed to assert a "fair degree" of dominion

and control over the phone and its data. There is no meaningful difference between the hypothetical and the facts of this case.[17]

In sum, because appellant's phone and its data were already seized when she remotely "wiped" the phone, her conduct cannot legally or factually support the panel's finding of guilty on The Specification of Charge III. While such a conclusion may appear to give appellant a windfall, it was the Government who decided to "push the envelope" by grounding their Article 131e, UCMJ, charge on the tenuous theory that the agents were still "endeavoring" to seize the phone, even after it was in the Government's physical possession.[18]

D. Instructional Error

In *United States v. Wolford*, the CAAF reiterated that the military judge's obligation to assure the accused receives a fair trial includes the duty to "provide appropriate legal guidelines to assist the jury in its deliberations." 62 M.J. 418, 419 (C.A.A.F. 2006) (citing *United States v. Graves*, 1 M.J. 50, 53 (C.M.A. 1975); *United States v. McGee*, 1 M.J. 193, 195(C.M.A. 1975)). As such, the failure to provide correct and complete instructions to the panel before deliberations begin may amount to a denial of due process. *Wolford,* 62 M.J. at 419, citing *United States v. Jackson*, 6 M.J. 116, 117 (C.M.A. 1979).

Although the charge sheet alleged that appellant obstructed, obscured, and disposed of the "digital content of her cell phone," when instructing on the Article 131e specification the military judge only used the term "cell phone," and made no mention of the charged term "digital content:"

> In order to find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt:

---

[17] It is also worth contrasting the first warrant (at issue) in this case with the warrants subsequently served on Apple. With respect to the warrants served on Apple, if appellant had been able to delete her data remotely while the agents were still waiting for Apple to respond, such conduct would fit the Article 131e, UCMJ, definition of "endeavoring" to seize because the data was not yet in the agent's possession. That, however, is not our case.

[18] Along the same lines, it is worth noting that this undertaking is so many angels on the head of a pin given the availability of another punitive article, Article 131b, UCMJ, Obstruction of Justice, which would unambiguously cover appellant's conduct with respect to her cell phone data should a similar scenario arise in the future.

> One, that persons authorized to make searches and seizures were endeavoring to seize certain property, to wit: the accused's *cell phone*;
>
> Two, that at or near West Point, New York, on or about 7 June 2019, the accused obstructed, obscured, and disposed of her *cell phone* with the intent to prevent its seizure;
>
> Three, that the accused then knew that persons authorized to make searches and seizures were endeavoring to seize her *cell phone.*

(emphasis added). As noted above, however, in the context of search and seizure, there is a clear distinction between a "cell phone" and its digital contents. *See Wicks*, 73 M.J.at 102 ("Because of the vast amount of data that can be stored and accessed, as well as the myriad ways they can be sorted, filed, and protected, it is not good enough to simply analogize a cell phone to a container"); *Wecht*, 619 F.Supp.2d at 247 ("[T]he law recognizes a distinction between the seizure of computer equipment on one hand and, on the other hand, the seizure of information stored *within* the computer equipment."); *Riley,* 573 U.S. at 401.

In this case, given defense counsel's acquiescence at trial to this discrepancy between the charge sheet and the instructions, any challenge to the military judge's instructional error is waived and must be considered "correct in law" under the applicable version of Article 66, UCMJ. *See United States v. Davis*, 79 M.J. 329, 331 (C.A.A.F. 2020) (holding that by "'expressly and unequivocally acquiescing' to the military judge's instructions, [a]ppellant waived all objections to the instructions"); *United States v. Conley*, 78 M.J. 747, 749 (Army Ct. Crim. App. 2019) (a waived claim is "correct in law" for purposes of our Article 66 review when a valid waiver applies to what would otherwise be prejudicial error).

In *Conley*, however, we held that even where an issue is both correct in fact and correct in law, the third "should be approved" prong of Article 66, UCMJ "allows us to, in our discretion, treat a waived or forfeited claim as if it had been preserved at trial." *Id.* at 750-51, citing *United States v. Britton*, 26 M.J. 24, 27 (C.M.A. 1988).[19] We further explained that while this "safety valve" of last resort was in "no way limited to certain issues," on a practical level the exercise of this unique power "is more likely to be found in certain military circumstances." *Conley,* 78 M.J. at 752. *See also United States v. Nalezynski*, ARMY 20200038, 2021 CCA LEXIS 509 at * 9 (Army. Ct. Crim. App. 30 Sep. 2021) (mem. op.) (holding that "a dispute about findings instructions is not the type of issue 'born

[19] We are cognizant that under the current version of Article 66, effective 1 January 2021, we no longer retain the "should be approved" discretion to reach waived claims. This case, however, is governed by the prior version of Article 66 in effect at the time of referral.

from uniquely military origins'" warranting Article 66 relief). Nevertheless, given the unique circumstances before us, to include the interplay between the lack of any evidence authorizing the seizure the digital contents of the phone and the military judge's erroneous instructions, we find that this is the rare case that warrants exercise of our Article 66 "should be approved" authority to reach the waived instructional error.

With respect to the standard of review, as noted above in *Conley* we held that the "should be approved" prong of Article 66, UCMJ, allows us to treat a waived claims "as if it had been preserved at trial." 78 M.J. at 751-52. On the other hand, in the context of forfeited, but not waived, instructional errors, the CAAF has applied a plain error standard of review. *United States v. Davis*, 76 M.J. 224, 229 (C.A.A.F. 2017). In order to prevail under a plain error analysis, an appellant must show that (1) there is error; (2) the error is plain or obvious; and (3) the error results in material prejudice to a substantial right of the accused. *United States v. Harcrow*, 66 M.J. 154, 158 (C.A.A.F. 2008) (citations omitted). In *Wolford*, 62 M.J. at 420, the CAAF held that under the plain error standard, claimed instructional errors "must be tested for prejudice under the standard of harmless beyond a reasonable doubt," and that such inquiry is "whether, beyond a reasonable doubt, the error did not contribute to the defendant's conviction or sentence." (citations omitted); *see also United States v. Tovarchavez*, 78 M.J. 458, 460 (C.A.A.F. 2019) (holding the plain error harmless beyond a reasonable doubt prejudice standard "is met where a court is confident that there was no reasonable possibility that the error might have contributed to the conviction") (citing *Chapman v. California*, 386 U.S. 18, 24 (1967)).

Regardless of whether we treat the instructional error in this case as preserved at trial under our Article 66, UCMJ "should be approved" authority, or under the more rigorous plain error standard applicable to forfeited claims, the results are the same. In short, based on this inconsistency between the charge sheet and the instructions, there are at least three separate theories under which the panel could have returned their guilty verdict. First, if the panel followed the instructions as written, as they were required to and we presume they did, they could not have found appellant guilty based on her subsequent remote wiping since at that point the Agent had already taken possession of the "cell phone." Second, it is possible that, notwithstanding the lack of any argument on this theory, the panel followed the instructions and found appellant guilty based on her conduct at the barracks, when she physically resisted the Agent as she tried to seize the phone. Third, it is conceivable that the panel went beyond the language of the instructions by interpreting the word "cell phone" to include digital content, and convicted appellant based on the government's theory at trial.

At this point, however, it is impossible for us to determine which, if any, of these theories formed the basis for appellant's conviction. Indeed, because at least

one of these theories has no factual or legal basis, we cannot be confident that there was no reasonable possibility that the error might have contributed to the conviction, nor are we convinced beyond a reasonable doubt that the instructional error did not contribute to the appellant's conviction. This is especially true given that trial counsel compounded the instructional error by only telling the panel in his opening statement that the Agent executed "a search warrant to seize *the phone* from" appellant, and arguing in his closing that the Agent "seized that watch, seized *the cell phone*." As such, the Article 131e specification must be set aside. *See United States v. Harville*, 14 M.J. 270, 270 (C.M.A. 1982) (holding that where evidence and testimony at trial fails to exclude any fair and reasonable doubt except that of guilt, guilty finding must be reversed); *Cf. United States v. Upshaw*, 81 M.J. 71, 76 (C.A.A.F. 2021) (holding that where trial counsel "exploited" the confusion created by the erroneous instructions and it is not certain if the instructional error affected the members' ultimate determination of guilt, "we cannot conclude that the military judge's error was harmless beyond a reasonable doubt"); *United States v. Cherry*, 14 M.J. 251, 252 (C.M.A. 1982) (finding error where "correct instruction *could* have led to a different verdict")(emphasis in original); *United States v. Livingston*, No. ARMY 20190587, 2022 CCA LEXIS 145 at *15 (Army Ct. Crim. App. 8 Mar. 2022)(finding error where "we cannot say with confidence that the instructional error did not contribute to appellant's conviction for the offense in question"); *People v. Hendrix*, 515 P.3d 22, 34 (2022) ("Because there is at least a reasonable probability a jury making that assessment would have given a different answer had it received correct instructions in this case, we conclude the instructional error was prejudicial and requires reversal.").

CONCLUSION

For the reasons set forth above, I respectfully disagree with my colleagues in the majority and would set aside the finding of guilty of The Specification of Charge III.

SMAWLEY, Chief Judge, joined by PENLAND, Judge, and ARGUELLES, Judge Dissenting:

I join my colleagues in the Dissent. I write separately to emphasize the vital importance of specificity in charging language related to searches and seizures in the context of digital evidence. I would set aside the finding of guilty of The Specification of Charge III based on a factual landscape entirely of the government's own creation.

The majority maintains the legal and factual sufficiency analysis for offenses under Article 131e, UCMJ, does not require proof of either the warrant or evidence of its specific contents. I disagree. The antecedent authority for a person conducting a seizure of individual property in this case is a duly issued search

authorization, which trial testimony acknowledged. The majority concludes that the authorization of a Criminal Investigation Command (CID) agent to conduct searches and seizures in the general sense is sufficient to satisfy the element of the offense; it is not. Article 131e, UCMJ requires proof "[t]hat one or more persons authorized to make searches and seizures were seizing, about to seize, or endeavoring to seize certain property." *Manual for Courts-Martial, United States* (*MCM*), pt. IV, ¶86.b. That a CID agent is among the persons generally authorized by Military Rule of Evidence 316(d) to seize property does not constitute authority to seize *certain property*. The "authority to conduct a seizure" of property under the facts of the case presupposes the legality of the seizure itself. The seizure, to be lawful, must cross the basic threshold of actually identifying the specific items authorized to be seized. The issue therefore remains the scope of the authorization, which in the instant case was never offered into evidence.

While seizing a cell phone necessarily involves the incidental seizure of any digital content stored within, a cell phone and its digital data are *not* synonymous for purposes of seeking and obtaining search and seizure authorizations. *See Riley v. California*, 573 U.S. 373, 401 (2014). The government must be precise regarding the language in the authorization during the course of an operation to search and seize a cell phone *and* its digital contents. A cell phone differs from many other physical objects in that the physical device itself is often of little to no import when compared to the digital content stored within. *See Id.* at 393-94.

As mentioned by my colleague *supra*, the government is bound in this case by its own charging decision to prove that appellant acted to prevent the seizure of "the digital content of her cell phone." *See United States v. English*, 79 M.J. 116, 120 (C.A.A.F. 2019). Compounding the issue regarding the specificity of language in the context of digital evidence in this case is the government's failure to introduce or admit into evidence at trial the authorization for the seizure in question. The absence of the authorization leaves this court guessing as to the specific property authorized for seizure. In place of the authorization, we have instead the testimony of the Agent regarding her application for authorization to seize appellant's Apple Watch and iPhone to convince us of the sufficiency of appellant's conviction beyond a reasonable doubt. While the majority, and the military judge's instruction at trial, use the terms "cell phone" and "cell phone data" as though the former implies with it the latter, this is inconsistent with the holding from *Riley*. 573 U.S. at 401. We cannot infer that authorization to seize a phone automatically included authorization to seize the digital contents of that phone.

As it stands, the record is devoid of sufficient evidence to support a conclusion that persons authorized to make searches and seizures were seizing, about to seize, or endeavoring to seize the digital content of appellant's cell phone. The majority turns to Mil. R. Evid. 316(d) as proof of the requisite authorization, however a Military Rule of Evidence is not synonymous with an authorization to

conduct a search. A rule of evidence and a search authorization are two distinct concepts, each with distinct constitutional underpinnings. Put simply, a rule of evidence discussing authorized seizures and the admissibility of evidence is not a substitute for the actual authorization to conduct a specific search.

Left only with the Agent's testimony that the search authorization at issue gave agents authority to seize appellant's Apple Watch and iPhone and with no mention of the digital contents of either device, the analysis turns to whether authorized persons were still seizing, about to seize, or endeavoring to seize the iPhone at the time of appellant's misconduct. They were not. Every seizure must logically have a start and end point, and even in the context of the digital contents of a phone, this principle is no different. Seizure of a cell phone is legally complete when there is "meaningful interference with an individual's possessory interest in that property." *United States v. Hahn*, 44 M.J. 360, 362 (C.A.A.F. 1996) (citing *United States v. Jacobsen*, 466 U.S. 109, 113 (1984)). In the instant case, the seizure of appellant's iPhone was complete as soon as the Agent departed the encounter with iPhone in hand. When appellant remotely wiped the data on her iPhone some twelve hours later, no persons authorized to make searches and seizures were seizing, about to seize, or endeavoring to seize the *cell phone*, rendering her conviction for The Specification of Charge III factually insufficient. *See United States v. Christensen*, ARMY 20190197, 2021 CCA LEXIS 159 at *4-5 (Army Ct. Crim. App. 29 Mar. 2021) (mem op.).

FOR THE COURT:

JAMES W. HERRING, JR.
Clerk of Court