No. 24-566

In the Supreme Court of the United States

LADONIES P. STRONG,

Petitioner

v.

UNITED STATES OF AMERICA,

Respondent

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES

PETITION FOR A WRIT OF CERTIORARI

SEAN PATRICK FLYNN
Counsel of Record
PHILIP M. STATEN
AUTUMN R. PORTER
JONATHAN F. POTTER
U.S. Army
Defense Appellate Division
9275 Gunston Road
Fort Belvoir, VA 22060
(703) 693-1238
sean.p.flynn40.mil@army.mil

JEFFREY T. GREEN
Green Law Chartered LLC
5203 Wyoming Road
Bethesda, MD 20816
jeff@greenlawchartered.com

Counsel for Petitioner

QUESTION PRESENTED

In *United States v. Jacobsen*, 466 U.S. 109, 113 (1984), this Court held that "[a] 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." The Court of Appeals for the Armed Forces, however, held—regarding the seizure of data under Article 131e, Uniform Code of Military Justice, 10 U.S.C. § 931e (2016)—that a seizure is complete when the authority seizing the property "has possession of the property and exercises dominion over it to the exclusion of all others."

The question presented is whether, regarding the seizure of data contained on a device, a different test is required than the one laid out by this Court in *Jacobsen*.

PARTIES TO THE PROCEEDINGS

Petitioner is Staff Sergeant Ladonies P. Strong.

Respondent is the United States of America.

RELATED PROCEEDINGS

Other than the direct appeals that form the basis for this petition, there are no related proceedings for purposes of S. Ct. R. 14.1(b)(iii).

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases: Page

Statutes:

Other Authorities

Constitutional Provision:

In the Supreme Court of the United States

No. 24-566

LADONIES P. STRONG,
Petitioner

v.

UNITED STATES OF AMERICA,
Respondent

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES

PETITION FOR A WRIT OF CERTIORARI

The petitioner, Staff Sergeant Ladonies P. Strong, respectfully petitions this Court for a writ of certiorari to review the final judgment of the Court of Appeals for the Armed Forces.

OPINIONS BELOW

The opinion of the Court of Appeals for the Armed Forces (App., *infra*, 1a–29a) is not yet reported, but can be found at 2024 CAAF LEXIS 478 (C.A.A.F. 2024). The opinion of the Army Court of Criminal Appeals (App., *infra*, 30a–75a) is reported at 83 M.J. 509 (A. Ct. Crim. App. 2023).

JURISDICTION

The Court of Appeals for the Armed Forces issued its opinion denying relief and its judgment on August 22, 2024. App., *infra*, 1a. The order of the Court of Appeals for the Armed Forces that denied the petition for reconsideration was entered on September 20, 2024. App., *infra*, 76a. On December 12, 2024, Chief Justice Roberts extended the time for petitioner to file a petition for a writ of certiorari to and including February 17, 2025. This Court has jurisdiction over the timely filed petition under 28 U.S.C. § 1259(3).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The Fourth Amendment to the United States Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Article 131e, Uniform Code of Military Justice, 10 U.S.C. § 931e provides:

> Any person subject to this chapter . . . who, knowing that one or more persons authorized to make searches and seizures are seizing, are about to seize, or are endeavoring to seize property, destroys, removes, or otherwise disposes of the property with intent to prevent the seizure thereof shall be punished as a court-martial may direct.

INTRODUCTION

What constitutes a seizure of data "is tremendously important, as it determines the legal framework that governs almost every digital evidence investigation." Orin Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J. 700, 702 (2010). In this case, Staff Sergeant Strong's conviction hinges on whether the data on her phone was seized when the phone itself was seized. This Court's answer to the question of when data is seized will impact how federal and state courts interpret and apply statutes and regulations involving the seizure of property and the Fourth Amendment.

In *United States v. Jacobsen*, 466 U.S. 109, 113 (1984), this Court held that a seizure occurs when there has been "some meaningful interference with an individual's possessory interests in that property." The Court of Appeals for the Armed Forces (CAAF) in *United States v. Hahn*, 44 M.J. 360, 362 (C.A.A.F. 1996), embraced this test for the presidentially promulgated precursor to Article 131e, Uniform Code of Military Justice (UCMJ). 10 U.S.C. § 931e. Two decades later, when confronting a suppression issue under the Fourth Amendment, the CAAF reiterated that the test from *Jacobsen* controlled when a seizure occurred. *United States v. Hoffmann*, 75 M.J. 120, 124 (C.A.A.F. 2016).

Here, however, the CAAF crafted a novel test that—in addition to effectively overruling *Hahn* and *Hoffmann*—held a seizure does not occur until the "digital content is in the exclusive control of authorized personnel, secure from unauthorized manipulation or destruction." App., *infra*, 2a. The

CAAF, while it cited this Court's—and its own—precedent, did not explain why that precedent was inadequate. In his dissent, Judge Gregory Maggs—noting this Court's decision in *Jacobsen*—engaged with it, and the prior decisions of the CAAF, and "conclude[d] that the Government agents 'seized' [Petitioner's] cell phone and its digital content when they took the physical cell phone from her possession . . . ." *Id.* at 25a. He noted the CAAF's new test "fundamentally transformed the definition of what constitutes a 'seizure'" and "turns on its head the test of when a seizure occurs." *Id.* at 22a, 26a. This Court should grant review to determine whether the seizure of a device containing data constitutes the seizure of that data.

STATEMENT OF THE CASE

A. Factual Background

Petitioner, during the summer of 2019, was responsible for driving West Point cadets to various locations to conduct their summer training. App., *infra*, 6a. Enroute to a training site, the truck she was driving—with several cadets aboard—rolled over. *Id.* One cadet was tragically killed. *Id.* Suspecting petitioner may have been using her phone while driving the truck, law enforcement obtained a search authorization for—and seized—her phone. *Id.* at 6a–7a.

To protect the phone from electronic transmissions, law enforcement sealed the phone in what they thought was a functional "Faraday bag" and returned to their headquarters. *Id.* at 7a–8a; *cf. Riley v. California*, 573 U.S. 373, 391 (2012).

Approximately an hour after the seizure of the phone, the data on petitioner's phone was wiped by a remote reset. App., *infra*, 8a–9a. Law enforcement later learned that the "Faraday bag" was defective. *Id.*

In addition to charging petitioner with the death of the cadet, the government charged petitioner with violating Article 131e, UCMJ for preventing an authorized seizure. App., *infra*, 31a. It alleged the following:

> [Petitioner], 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 cellphone, property [Petitioner] then knew a person authorized to make searches and seizures was endeavoring to seize.

Id. at 40a.

At trial, the government only introduced evidence that petitioner had the ability to remotely wipe her phone. *Id.* at 26a, 36a. The government did not introduce evidence that she, or anyone else, had any ability to access, view, organize, use, or manipulate any of the data in the phone. The court-martial found petitioner guilty of this charge, as well as negligent homicide under Article 134, UCMJ, 10 U.S.C. § 934, and sentenced her to three years confinement and a bad-conduct discharge. *Id.* at 31a. Petitioner's conviction for negligent homicide is not at issue in this appeal.

B. Procedural Background

1. The Army Court reviewed petitioner's case under Article 66(b)(3), UCMJ. 10 U.S.C. § 866(b)(3). Before the Army Court, petitioner argued that her conduct in wiping the phone was beyond the reach of Article 131e, UCMJ. App., *infra*, 37a. Specifically, she argued that by the time of the remote wipe, law enforcement had already seized the phone and its digital contents. *Id.* On January 6, 2023, the Army Court affirmed petitioner's findings and sentence. *Id.* at 31a. It determined that due to the "ethereal nature of digital evidence" a seizure is not complete until "those authorized to seize the property execute the protocols necessary to isolate and preserve the digital media" which may include copying the data on the device. *Id.* at 44a–45a. Three judges dissented from this opinion, because—in part—they concluded that when law enforcement took the phone and put it in the Faraday bag law enforcement "asserted a 'fair degree' of dominion and control over both the phone and its data." *Id.* at 64a (citing *Jacobsen*, 466 U.S. at 120).

2. The CAAF granted petitioner's request for review and affirmed the lower court in a divided opinion on August 22, 2024. App., *infra*, 2a. The majority concluded that a seizure is not complete until "a person authorized to seize certain property has possession of the property and exercises dominion over it to the exclusion of all others." *Id.* at 14a. It reasoned that, although petitioner's cell phone had been seized, petitioner's ability to remotely delete the digital contents of the cell phone demonstrated that law enforcement did not have exclusive control of the data. *Id.* at 15a.

Judge Maggs dissented. *Id.* at 22a. He noted the majority's holding was "contrary to long-standing precedent establishing that a seizure occurs 'when there is some meaningful interference with an individual's possessory interests in that property.' *United States v. Hahn*, 44 M.J. 360, 362 (C.A.A.F. 1996) (quoting *United States v. Jacobsen*, 466 U.S. 109, 113 (1984))." *Id.* at 22a. He was concerned the CAAF "create[d] an unobtainable seizure standard because the government does not acquire the same property interest as the property owner when it takes possession of property for law enforcement purposes." *Id.* at 26a. Judge Maggs instead would find the seizure of the phone and its data was complete prior to the phone being remotely wiped. *Id.* at 28a. Additionally, while he believed his interpretation was unambiguously correct, should the question even be close, he believed that the rule of lenity required ruling in petitioner's favor. *Id.* at 29a.

The CAAF denied a request for reconsideration on September 20, 2024. *Id.* at 76a.

REASONS FOR GRANTING THE PETITION

This Court's resolution to the question of when data is seized is an issue of increasing importance. What constitutes the seizure of data will govern the legal framework of almost every digital evidence investigation and the appropriate application of the Fourth Amendment.

A. The CAAF's decision is contrary to federal precedent and, if adopted, would upend how seizures are analyzed in a vast array of criminal and civil cases.

1. This Court, in promulgating Federal Rule of Criminal Procedure 41, determined that warrants "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information" to be reviewed later. Fed. R. Crim. P. 41(e)(2)(B); *see also* 28 U.S.C. § 2072(a). The Seventh Circuit, in *United States v. Huart*, 735 F.3d 972, 974 n.2 (7th Cir. 2013), similarly reasoned that the warrant for data was executed when the phone was seized. *See also United States v. Carrington*, 700 Fed. Appx. 224, 232 (4th Cir. Jul. 25, 2017) (reasoning that warrants "are deemed executed when the electronically stored information is seized and brought within the government's control [and] the phone already was in government custody pursuant to a lawful seizure.") *and United States v. Vedrine*, 2022 U.S. App. LEXIS 32849, *14 (11th Cir. Nov. 29, 2022) ("[O]nce data is seized and extracted by law enforcement, the warrant is considered executed for purposes of Rule 41 . . . .").

There is consensus among state courts as well. *See State v. Sanchez*, 476 P.3d 889, 893 (N.M. 2020) ("By seizing an electronic device, law enforcement takes control of both the device and the data on that device . . . ."); *Vietti v. State*, 2024 Nev. App. Unpub. LEXIS 296, *8 (Nev. Ct App. Jun. 20, 2024) ("[A] warrant is executed when the device containing electronic data is seized."); *State v. Drachenberg*, 998 N.W.2d 566, 579 (Wis. Ct. App. 2023) ("[P]olice here executed the search warrant within five days after it

was issued by finishing their search of the designated places for the designated digital devices and seizing them."). And as a leading commentator stated, if the hardware is taken "then surely the data it contains is seized along with the hardware." Orin Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J. 700, 704–05 (2010).[1]

Adopting the test by the CAAF that requires the person seizing the property to have "possession of the property and exercise[] dominion over it to the exclusion of all others" may force law enforcement to take additional steps in order to seize data. As it stands, a warrant for data is considered executed when the device storing the data is seized. *See* Fed. R. Crim. P. 41(e)(2)(B) *and Huart*, 735 F.3d at 974 n.2.

---

[1] While the CAAF stands alone in holding a seizure of data does not occur when the device is seized, there is confusion among lower courts about what other actions could constitute a seizure. *See Bills v. Aseltine*, 958 F.2d 697, 707 (6th Cir. 1992) (reasoning that taking pictures of evidence is not a seizure); *United States v. Mancari*, 463 F.3d 590, 596 (7th Cir. 2006) (same); *United States v. Thomas*, 613 F.2d 787 (10th Cir. 1980) (same); *In re Search Warrant No. 16-960-M-01*, 232 F. Supp. 3d 708, 720 (E.D. Pa. 2017) ("[e]lectronically transferring data from a server in a foreign country to Google's data center in California does not amount to a 'seizure' because there is no meaningful interference with the account holder's possessory interest in the user data."); *United States v. Espinoza*, 641 F.2d 153, 167 (4th Cir. 1981) (reasoning that taking photographs is a seizure); *United States v. Ganias*, 824 F.3d 199, 201 (2nd Cir. 2016) (accepting the panel's holding that copying data on a hard drive constitutes a seizure but deciding the case on other grounds), *cert denied*, 580 U.S. 1019 (2016); *People v. Seymour*, 536 P.3d 1260, 1273 (Colo. 2023) (holding that copying internet search history "meaningfully interfered with [a] possessory interest in that data and constituted a seizure subject to constitutional protection.").

This allows law enforcement to copy or analyze the data after the 14 days in which a warrant must be executed. *See* Fed. R. Crim. P. 41(e)(2)(A)(i). The CAAF's test, however, could require law enforcement to copy the data, or take some other unclear actions, to ensure they have "possession of the property and exercise[] dominion over it to the exclusion of all others." App., *infra*, 14a. This more stringent requirement may lead to the suppression of otherwise legally obtained evidence.

2. The CAAF attempted to insulate its opinion by stating that its new test is "for purposes of Article 131e, UCMJ." App., *infra*, 2a. But the CAAF cannot distinguish away the test for a seizure, a legal term of art, laid out by this Court in *Jacobsen*. Congress has the authority to redefine legal terms of art. *See Sackett v. EPA*, 598 U.S. 651, 671 (2023). Congress chose to not do so here.

The UCMJ, moreover, is "a 'uniform code.'" *United States v. Briggs*, 592 U.S. 69, 73 (2020) (quoting *Burns v. Wilson*, 346 U.S. 137, 141 (1953)). Congress, admittedly, only uses the word seize one other time in the UCMJ—in the context of kidnapping. *See* Article 125, UCMJ, 10 U.S.C. § 925. But the Manual for Courts-Martial—promulgated by the President in accordance with Article 36, UCMJ, 10 U.S.C. § 836—uses the word seize extensively, and nearly always in the context of the Fourth Amendment. *See* Manual for Courts-Martial, United States, (2016 ed.), Military Rule of Evidence 311(a) ("Evidence obtained as a result of an unlawful search or seizure made by a person acting in a governmental capacity is inadmissible . . . ."); *id.*, Military Rule of Evidence 316(c)(1) ("Evidence is admissible when seized based

on a reasonable belief . . . ."). Congress is presumed to be aware of how the President has previously acted within his delegated authority. *Khan v. Hart*, 943 F.2d 1261, 1264 (10th Cir. 1991) (citing *United States v. Herd*, 29 M.J. 702, 707 (A. Ct. Mil. R. 1989)). This awareness by Congress of how the President used the word seize elsewhere in the Manual for Courts-Martial, and its decision to not provide a different definition for its new statutory offense, suggests acquiescence—if not an embrace—of the already existing usage crafted by this Court in 1984. The *Jacobsen* test is the correct one here.

3. The proper result, applied to these facts, is straightforward. Law enforcement seized the data on petitioner's phone when they seized her phone. At that point, petitioner was incapable of using the phone in the way it was intended, even if she was able to access some data via other means. She could no longer use her phone to make calls, text, search the internet, take pictures, or buy things. It was a significant interference with her possessory interest in the data on the phone, as this Court noted in *Riley*. 573 U.S. at 395 ("[I]t is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate.").

But importantly, and as the CAAF did not disclaim, petitioner's ability to access the data on her cell phone was not only changed—the record does not support she had any access to the data beyond a remote reset. Nothing suggests she could—even from another device—manipulate, copy, view, or access the data. The only ability petitioner retained once law

enforcement took her phone was the ability to remotely wipe it. Just as the ability to freeze a stolen credit card does not suggest a thief has not meaningfully interfered with one's finances, petitioner's mere ability to wipe her phone did not curb law enforcement's interference with her interest in the data.

4. Besides data, other evidence can be seized without knowing the information contained within it. A "compulsory administration of a blood test . . . plainly involves the broadly conceived reach of a search and seizure under the Fourth Amendment." *Schmerber v. Cal.*, 384 U.S. 757, 767 (1966). In the case of blood, the drawing of the blood from the person would be the seizure, and the subsequent test of the blood would be the search. *Cf. Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 617 n.4 (1989) (recognizing that the collection of bodily fluids may be deemed a seizure, but determining that making that finding was unnecessary as treating the collection and testing of the fluids as a search vindicated the privacy interests).

When a phone has been seized, there has been a meaningful interference in the owner's possessory interest in the data on that phone. Law enforcement knows there is data on the phone. The fact that law enforcement cannot yet read, or interpret, the data is immaterial to whether a seizure occurred. *Cf. Riley*, 573 U.S. at 387 (noting officers' knowledge that data existed on the phone and that the data could not harm them removed justification for a search of the phone incident to arrest).

5. Finally, as Judge Maggs noted in his dissent, even if this is a close case of statutory interpretation petitioner prevails under the rule of lenity. App., *infra*, 29a. To uphold petitioner's conviction the CAAF created a novel test for data—unmoored from the statute and this Court's precedent. The judicial activism by the CAAF violates the requirement "that ambiguities about the breadth of a criminal statute should be resolved in the defendant's favor." *United States v. Davis*, 588 U.S. 445, 464 (2019). The rule of lenity has been much discussed recently by this Court. *Compare Wooden v. United States*, 595 U.S. 360, 376–78 (2022) (Kavanaugh, J., concurring) ("[T]he rule of lenity rarely if ever comes into play.") *with id.* at 384–397 (Gorsuch, J., concurring) ("[P]unishments should never be products of judicial conjecture about this factor or that one."). This case does not present a close call; law enforcement seized the data on the phone when they seized the phone. But even if this case is a close one, it is one in which petitioner prevails under the rule of lenity.

B. This case presents the ideal vehicle to decide the issue.

This petition is in the optimal procedural posture. The issue of whether the seizure was complete was raised at every stage of review. The parties, and all reviewing courts, agree on the relevant facts: the phone itself was seized, the record does not support petitioner could do anything with the data on her phone besides delete it, and if the data is determined to be seized petitioner's crime would be beyond the reach of the statute. Additionally, a ruling in petitioner's favor would not decriminalize the conduct of remotely wiping evidence upon a phone's seizure by law enforcement. The government maintains the ability to charge similar actions under Article 131b, UCMJ, 10 U.S.C. § 931b (Obstructing Justice).

Lastly, this case presents an opportunity to address the ever-important issue of the responsibility and limitations of the government when dealing with the seizure of data.

CONCLUSION

For all these reasons, this Honorable Court should grant the petition for a writ of certiorari.

Respectfully submitted.

SEAN PATRICK FLYNN
Counsel of Record
9275 Gunston Road
Fort Belvoir, VA 22060
(703) 693-1238
sean.p.flynn40.mil@army.mil

JEFFREY T. GREEN
Green Law Chartered LLC
5203 Wyoming Road
Bethesda, MD 20816
jeff@greenlawchartered.com

PHILIP M. STATEN
Chief
U.S. Army
Defense Appellate Division
AUTUMN R. PORTER
Deputy Chief
JONATHAN F. POTTER
Senior Appellate Counsel

Counsel for Petitioner

FEBRUARY 2025

APPENDIX

TABLE OF CONTENTS

APPENDIX A

This opinion is subject to revision before publication.

UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES
Appellee

v.

Ladonies P. STRONG, Staff Sergeant
United States Army, Appellant

No. 23-0107
Crim. App. No. 20200391

Argued October 11, 2023—Decided August 22, 2024

Military Judge: G. Bret Batdorff

For Appellant: *Major Sean Patrick Flynn* (argued); *Colonel Philip M. Staten*, *Major Mitchell D. Herniak*, *Major Brian A. Osterhage*, and *Jonathan F. Potter*, Esq. (on brief); *Colonel Michael C. Friess*.

For Appellee: *Major Timothy R. Emmons* (argued); *Colonel Christopher B. Burgess*, *Lieutenant Colonel Jacqueline J. DeGaine*, and *Captain Alex J. Berkun* (on brief).

Judge JOHNSON delivered the opinion of the Court, in which Chief Judge OHLSON, Judge SPARKS, and Judge HARDY joined. Judge MAGGS filed a separate dissenting opinion.

Judge JOHNSON delivered the opinion of the Court.[1]

This case raises the question of when a seizure of digital evidence is complete. For the reasons set forth below, we hold that the seizure of digital evidence is complete for purposes of Article 131e, Uniform Code of Military Justice (UCMJ), 10 U.S.C. § 931e (2018), when the digital content is in the exclusive control of authorized personnel, secure from unauthorized manipulation or destruction. We further hold that authorized personnel are endeavoring to seize digital evidence while they are executing processes to acquire such exclusive control. We therefore affirm the decision of the United States Army Court of Criminal Appeals (ACCA).

I. Background

Contrary to her pleas, on July 18, 2020, Appellant was convicted by a general court-martial panel composed of officer and enlisted members of one specification of negligent homicide in violation of Article 134, UCMJ, 10 U.S.C. § 934 (2018), and one specification of preventing an authorized seizure of property in violation of Article 131e, UCMJ. The latter charge arose when Appellant remotely reset her Apple iPhone to the original factory settings, effectively deleting the digital content stored on the iPhone, after Army Criminal Investigation Division

[1] The Court heard oral argument in this case at Joint Base Lewis-McChord, Washington, as part of the Court's "Project Outreach." Project Outreach seeks to expand awareness of the military justice appellate process by taking appellate hearings to military bases and educational institutions around the country. We thank the participants.

(CID) agents seized the iPhone pursuant to a valid search authorization. The court-martial sentenced Appellant to reduction to the grade of E-1, confinement for three years, and a bad-conduct discharge.

Appellant appealed to the ACCA, challenging the legal and factual sufficiency of her convictions. *United States v. Strong*, 83 M.J. 509, 511 (A. Ct. Crim. App. 2023) (en banc).[2] With respect to the offense of prevention of authorized seizure of property, Article 131e, UCMJ, "criminalizes actions taken by an accused to prevent the seizure of property by authorized personnel," *id.* at 513-14, when the accused then knew that the authorized personnel "were seizing, about to seize, or endeavoring to seize the property," *Manual for Courts-Martial*, *United States*, pt. IV, para. 86.b.(1) (2019 ed.) (*MCM*). Appellant argued that her conduct was beyond the reach of the statute because it does not apply to conduct occurring after property is seized, and in this case, her iPhone had already been seized when she remotely deleted its digital content. *Strong*, 83 M.J. at 513.

The ACCA noted that because the digital contents of a cell phone such as Appellant's iPhone can be manipulated remotely:

> it is no longer enough for law enforcement officials executing a warrant for digital media to simply take possession of the physical

[2] The ACCA summarily concluded that the negligent homicide conviction was both legally and factually sufficient. *Strong*, 83 M.J. at 511. That ruling is not at issue in this appeal.

> 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.

Id. at 515.

After listing various protective measures to prevent remote access to the digital contents of a cell phone, the ACCA noted that none are "foolproof" because "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." *Id.* at 515-16. Therefore, the ACCA found:

> 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[icle] 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.

Id. at 516.

Applying these principles, the ACCA concluded that the seizure of digital content on Appellant's iPhone was ongoing at the time that she erased it because Appellant "still had sufficient access to the data on the phone, whether 'authorized' or not, to dispose of it in precisely the manner the seizing authority sought to prevent." *Id.* at 517 (footnote omitted). Having determined that Appellant destroyed the digital content on her iPhone while authorized personnel were endeavoring to seize it, in violation of Article 131e, UCMJ, a majority of the en banc ACCA held that her conviction was both legally and factually sufficient. *Id.* at 517-18.[3]

We granted review to determine whether the ACCA erred when it concluded that agents were still endeavoring to seize the digital content on Appellant's iPhone after they had already seized the iPhone.[4]

---

[3] Three judges dissented, concluding, inter alia, that the evidence was factually and legally insufficient to support the conviction because Appellant deleted digital content from her iPhone after it was seized. *Strong*, 83 M.J. at 523 (Arguelles, J., with whom Smawley, C.J., and Penland, J., joined, dissenting). The dissent argued that "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." *Id.* (quoting *United States v. Jacobsen*, 466 U.S. 109, 120 (1984) (additional citation omitted)).

[4] We granted review of the following issues:

> I. Whether the Army Court erred when it determined that agents were still "endeavoring to seize" the digital media on Appellant's phone after agents had already seized the phone.

II. Facts

On the morning of June 6, 2019, a convoy of vehicles was transporting a group of United States Military Academy (USMA) cadets to a land navigation site for a training exercise. Appellant was driving one of the vehicles. At around 6:41 a.m., Appellant's vehicle flipped over while in transit, killing one cadet and injuring others.

CID responded to the scene and interviewed the truck commander, who said that he saw Appellant on her Apple Watch when the vehicle rollover incident occurred. At approximately 10:55 p.m., CID obtained authorization to seize and search Appellant's Apple Watch, as well as her iPhone, which was connected to the watch.

> II. Whether Appellant was prejudiced where the [military judge] failed to instruct the panel in accordance with the plain language of the charge sheet; and
>
> III. Whether Appellant was deprived of her constitutional right to a unanimous verdict.

United States v. Strong, 83 M.J. 392, 392-93 (C.A.A.F. 2023) (order granting review).

In a September 11, 2023, order, we vacated our grant of review of Issue II. *United States v. Strong*, 83 M.J. 481, 481 (C.A.A.F. 2023) (order vacating Issue II).

Issue III was not argued or briefed as it was held as a trailer to *United States v. Anderson*, 83 M.J. 291 (C.A.A.F. 2023), *cert. denied*, 144 S. Ct. 1003 (2024). Based upon the decision in *Anderson*, we hold that Appellant was not deprived of the right to a unanimous verdict.

Immediately after obtaining authorization, CID Special Agent (SA) ST was escorted by Appellant's noncommissioned officer (NCO) to Appellant's living quarters to seize the devices. SA ST left the NCO alone with Appellant as she got dressed and instructed the NCO to not let Appellant use her Apple Watch or iPhone. SA ST heard the NCO tell Appellant several times that she was not allowed to be on her iPhone, and when SA ST stepped inside Appellant's living quarters, she saw Appellant trying to use her iPhone.

At 11:07 p.m., after advising Appellant that CID was authorized to seize her Apple Watch and iPhone, SA ST seized the devices. According to SA ST,[5] Appellant became "belligerent" and tried to take her Apple Watch and iPhone back several times. SA ST cautioned her, "At ease, Sergeant"—the first time in her career that she had to admonish a subject in that way.

SA ST testified that law enforcement officials are trained to place a seized cell phone in airplane mode and to place it in a Faraday bag, which blocks any signals from being sent or received by the cell phone. These precautions prevent anyone with access to the user's account from remotely wiping the digital contents of the cell phone.

CID sought to protect the Apple Watch and iPhone from remote manipulation or destruction so they could be examined to determine whether Appellant was using one of the devices at the time

[5] ST had retired from the Army and was no longer a CID special agent when she testified at Appellant's court-martial.

that the vehicle flipped over. Accordingly, CID attempted to put the iPhone in airplane mode but was unsuccessful. CID placed the iPhone into a bag labeled as a Faraday bag and transported it to a CID office, where a CID forensic examiner would remove the digital content from the iPhone for analysis.

The record is unclear as to whether the bag malfunctioned, was mislabeled, or was not properly sealed. In any case, by 1:25 p.m. on June 7, 2019, CID learned that the iPhone had been remotely reset, erasing the digital content from the iPhone and with it, most of the digital content from the Apple Watch.[6] According to CID, the factory reset occurred while the iPhone was in transit to a CID lab. CID was unable to access the remaining digital content from the Apple Watch because it was encrypted and encoded protected. Unable to access digital content from the Apple Watch or iPhone, CID could not determine whether Appellant was operating either device when the vehicle rolled over.

Through authorized search and seizure warrants pursuant to 18 U.S.C. § 2703,[7] CID acquired information from Apple, the manufacturer of Appellant's watch and cell phone, and Verizon, Appellant's cell phone carrier. This information

---

[6] A CID forensic examiner testified that "probably 95 percent" of the relevant digital content from the watch would have been found on the iPhone.

[7] The Stored Communications Act, 18 U.S.C. § 2703 (2018), generally requires the government, under specified circumstances, to obtain a warrant in order to compel service providers to disclose the contents of electronic or wire communications or records pertaining to subscribers or customers of such services.

revealed that about an hour after CID's seizure of the Apple Watch and iPhone, someone using Appellant's iCloud account[8] searched the Internet for "find my iphone," accessed webpages related to the service "Find My iPhone,"[9] and issued a command to erase the digital content from Appellant's iPhone.[10] The command came from an IP address in New York through an Apple MacBook Pro of the same model as one owned by Appellant. Execution of the command returned Appellant's iPhone to factory settings. Although the command to erase Appellant's iPhone was given shortly after midnight on the day after the iPhone was seized, it took some time for the iPhone to receive the signal. As a result, the iPhone's digital content was not erased until approximately 10:50 a.m. on June 7, 2019.

After the command was sent to erase Appellant's iPhone, information from Appellant's iCloud account revealed continued research for information related to Find My iPhone, including a search for "Erase

---

[8] An iCloud account is an Apple account that stores information in a remote location that can be accessed by various devices. Appellant's Apple Watch, iPhone and MacBook Pro were all registered to the same iCloud account.

[9] "Find My iPhone" is a service offered by Apple that enables a user to remotely wipe devices, such as phones and watches. The service can be accessed through an internet browser using the iCloud website or through an application on an Apple device.

[10] CID seized Appellant's Apple Watch and iPhone at 11:07 p.m. on June 6, 2019. Someone logged into Appellant's iCloud account through a web browser at 12:17 a.m. on June 7, 2019, and three minutes later, at 12:20 a.m., gave the command to erase Appellant's iPhone.

Your Device With Find My iPhone." According to a CID forensic examiner, this could have indicated that someone was trying to research how to erase an Apple Watch.

III. Discussion

The question in this case is whether CID was "endeavoring to seize" the digital content of Appellant's iPhone when Appellant erased it. Applying the plain meaning of the terms of the statute, we conclude (1) that seizure of the digital content was not complete when CID seized the iPhone and placed it in the Faraday-labeled bag, and (2) that CID was still endeavoring to seize the digital content when Appellant erased it.

A. Standard of Review

"Questions about the meaning of statutes, including the meaning of the UCMJ's punitive articles, are questions of law that this Court reviews de novo." *United States v. Mays*, 83 M.J. 277, 279 (C.A.A.F. 2023) (citing *United States v. Bennitt*, 72 M.J. 266, 268 (C.A.A.F. 2013)).

B. Law

The elements of the offense of prevention of an authorized seizure under 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, para. 86.b.[11]

"It is a general rule of statutory construction that if a statute is clear and unambiguous—that is, susceptible to only one interpretation—we use its plain meaning and apply it as written." *United States v. Schmidt*, 82 M.J. 68, 73 (C.A.A.F. 2022). Thus, "'[t]he first step [in statutory interpretation] is to determine whether the language at issue has a plain and unambiguous meaning with regard to the particular dispute in the case. The inquiry ceases if the statutory language is unambiguous and the statutory scheme is coherent and consistent.'" *United States v. McPherson*, 73 M.J. 393, 395 (C.A.A.F. 2014) (quoting *Barnhart v. Sigmon Coal Co., Inc.*, 534 U.S. 438, 450 (2002)). "When the words of a

---

[11] As the ACCA noted:

> 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.

Strong, 83 M.J. at 514 n.6.

statute are unambiguous, then, this first canon is also the last: 'judicial inquiry is complete.'" *Connecticut Nat'l Bank v. Germain*, 503 U.S. 249, 254 (1992) (quoting *Rubin v. United States*, 449 U.S. 424, 430 (1981)). The plain meaning of the words of a statute controls, "so long as that meaning does not lead to an absurd result." *United States v. Ortiz*, 76 M.J. 189, 192 (C.A.A.F. 2017).

Whether statutory language is ambiguous "'is determined by reference to the language itself, the specific context in which that language is used, and the broader context of the statute as a whole.' " *Schmidt*, 82 M.J. at 76 (Ohlson, C.J., with whom Erdmann, S.J., joined, concurring in the judgment) (quoting *Robinson v. Shell Oil Co.*, 519 U.S. 337, 341 (1997)). Where the statute does not define the relevant phrase, "we must seek to discern its ordinary meaning through an analysis of its constituent words." *United States v. Badders*, 82 M.J. 299, 303 (C.A.A.F. 2022). "Words are to be understood in their ordinary, everyday meanings—unless the context indicates that they bear a technical sense." Antonin Scalia & Bryan A. Garner, *Reading Law: The Interpretation of Legal Texts* 69 (2012).

C. Analysis

Because Article 131e, UCMJ, criminalizes action taken with the intent to *prevent* an authorized seizure of property, the unlawful action must occur *before* the seizure is complete. Specifically, it must occur while authorized personnel are "seizing, about to seize, or endeavoring to seize" the property in question, and the accused must act "with intent to

prevent the seizure thereof." *MCM* pt. IV, para. 86.b.(1)-(2). Applying the plain meaning of the statute, we conclude that law enforcement agents were endeavoring to seize the digital content of Appellant's iPhone when she remotely wiped the iPhone to prevent the seizure of its digital content.

The first element of the Article 131e, UCMJ, offense of preventing an authorized seizure requires the government to prove that an authorized individual is "seizing, about to seize, or endeavoring to seize certain property." *MCM* pt. IV, para. 86.b.(1). "[S]eizing" and "endeavoring to seize" describe ongoing actions, while "about to seize" describes an action that has not yet occurred. Once a seizure is complete, no one is about to seize or is in the process of seizing or endeavoring to seize the property in question.

The second element requires proof "[t]hat the accused destroyed, removed, or otherwise disposed of that property with intent to prevent the seizure thereof." *MCM* pt. IV, para. 86.b.(2). One cannot intend to prevent an event that has already occurred. The plain meaning of these terms indicates that a violation of Article 131e, UCMJ, can only occur before a seizure is complete.[12]

As Article 131e, UCMJ, applies only before a seizure is complete, in order to determine whether Appellant's conduct fell within the reach of the

---

[12] Article 131e, UCMJ, differs in scope from its civilian corollary, 18 U.S.C. § 2232(a) (2018), which can be violated "before, during, or *after* any search for or seizure of property." (Emphasis added.)

statute we must first identify when a seizure is complete. According to *Black's Law Dictionary*, "seize" is defined as "[t]o forcibly take possession (of a person or property)" and "[t]o be in possession (of property)." *Seize*, *Black's Law Dictionary* (10th ed. 2014). "[P]ossession" is defined as "[t]he fact of having or holding property in one's power; the exercise of dominion over property" and "[t]he right under which one may exercise control over something to the exclusion of all others; the continuing exercise of a claim to the exclusive use of a material object." *Possession*, *Black's Law Dictionary* (10th ed. 2014). The plain meaning of these terms, taken together, establishes that a seizure is complete for purposes of Article 131e, UCMJ, when a person authorized to seize certain property has possession of the property and exercises dominion over it to the exclusion of all others.

Next, we must examine the meaning of "endeavoring to seize" in Article 131e, UCMJ. "[E]ndeavor" is defined as "[a] systematic or continuous effort to attain some goal; any effort or assay to accomplish some goal or purpose." *Endeavor*, *Black's Law Dictionary* (10th ed. 2014). As the pertinent "goal or purpose" in the context of Article 131e, UCMJ, is to seize, applying the above definition of "seize" we conclude that the plain meaning of "endeavoring to seize certain property" is to be in the process of exerting effort to exercise dominion over property to the exclusion of all others.

With these definitions in place, we turn to the question presented in this case: whether authorized personnel were endeavoring to seize the digital content of Appellant's iPhone after they seized the

iPhone itself. Appellant contends that the digital content of the iPhone was seized at the same time CID seized the device itself. According to Appellant, because the seizure was already complete, CID was not endeavoring to seize the digital content of the iPhone when she erased it. In the alternative, Appellant argues that agents were no longer endeavoring to seize the iPhone's digital content once they placed the iPhone into what they thought was a functioning Faraday bag. We are unpersuaded by either argument.

We conclude, first, that the seizure of Appellant's iPhone did not constitute seizure of the digital content of the iPhone. We agree with the ACCA that in light of the ethereal nature of digital evidence and its capacity for remote manipulation, "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." *Strong*, 83 M.J. at 515. In order to seize the digital content of the iPhone, CID had to take additional steps to protect it from unauthorized remote manipulation or destruction, whether by moving or copying the digital content to a secure location or by some other means. In this case, the iPhone was remotely reset and its digital content was erased before CID could complete the necessary additional steps to secure the iPhone's digital content. The fact that Appellant was able to remotely delete the digital content even after the iPhone was seized conclusively demonstrates that CID did not have exclusive control over the digital content even if they had control over the iPhone itself. Therefore, the seizure was not complete when the iPhone was seized or placed in the Faraday-labeled bag.

Second, we conclude that CID was endeavoring to seize the digital content of Appellant's iPhone when Appellant wiped the iPhone. As stated above, a seizure is complete for purposes of Article 131e, UCMJ, when a person authorized to seize certain property has possession of the property and exercises dominion over it to the exclusion of all others. In this case, CID attempted to secure the digital content from remote manipulation or destruction by attempting to put it in airplane mode and placing it in the Faraday-labeled bag. Then CID sought to remove the digital content from the iPhone for forensic analysis, stopping only upon discovering that the digital content had been wiped. CID had not achieved the purpose of the seizure—possession of and exclusive dominion over the digital evidence—when Appellant wiped the iPhone. By engaging in continuing efforts to take exclusive possession of the digital content on Appellant's iPhone even after it was erased, CID was endeavoring to seize the digital content when Appellant wiped the iPhone.[13]

---

[13] Thus, we agree with the lower court's determinations that:

> [(1)] 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. . . . [and (2) f]or purposes of Art. 131e, UCMJ, . . . 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.

Strong, 83 M.J. at 516.

Although the plain meaning of the language in Article 131e, UCMJ, is dispositive of the issue before this Court, we note that our analysis of the statutory language is consistent with this Court's precedent regarding when a seizure is complete.

In *United States v. Hahn*, we stated that "'[a] seizure of property occurs when there is some meaningful interference with an individual's possessory interests in that property.'" 44 M.J. 360, 362 (C.A.A.F. 1996) (internal quotation marks omitted) (quoting *United States v. Jacobsen*, 466 U.S. 109, 113 (1984)). In that case, the appellant challenged the providence of his plea to preventing the seizure of property by authorized law enforcement agents, arguing that his conduct was outside of the scope of the statute[14] because a seizure had already occurred. *Id.*

The Court described the circumstances in *Hahn* as follows:

> During a consensual search of another sailor's house, [Naval Investigative Service (NIS)] agents found property that they suspected appellant had stolen. In order to confirm the identity of the thief, the agents suggested that the sailor telephone appellant and tell him that the NIS was going to search the house that evening and that appellant had to remove the property beforehand. When appellant arrived shortly thereafter and removed the

[14] In *Hahn*, the appellant was charged with the prevention of authorized seizure of property, then an Article 134, UCMJ, offense. 44 M.J. at 361; *see also supra* note 11.

> items to his car, surveilling agents swarmed in and apprehended him.

Id. at 361. The appellant argued that NIS gained physical control of the stolen property once they had entered the home, searched for the stolen property, identified the stolen property, and then waited until the appellant arrived. *Id.* at 362.

We declined to adopt the appellant's theory, which:

> 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. Such a holding would be inconsistent with the concept of seizure as set out in *Jacobsen* and is without any basis in legal theory of which we are aware.

Id.

Instead, we concluded that there was no meaningful interference with the appellant's possessory interest in the property, as evidenced by "the ease with which appellant was able to gather up the property and move it to his car." *Id.* Therefore, the property had not been seized when the appellant moved it in an attempt to prevent its seizure. *Id.*

In *United States v. Hoffmann*, we applied the same definition of when a seizure is complete in the context of a motion to suppress the fruits of a search of the appellant's electronic media. 75 M.J. 120, 124

(C.A.A.F. 2016) (citing *Jacobsen*, 466 U.S. at 113). The appellant in that case initially consented to a search of his barracks room, but then he revoked his consent when he noticed that agents were collecting his electronic media. *Id.* at 123. The agents terminated the search but did not return the items they had already collected. *Id.* The military judge denied the appellant's motion to suppress the fruits of the subsequent search of the electronic media, finding that the seizure was lawful because the appellant revoked his consent only after investigators had seized the electronic media. *Id.*

We reversed, holding that the seizure of the media did not occur until after the appellant revoked his consent. *Id.* at 124. We reasoned:

> A "seizure" of property occurs when there is some meaningful interference with an individual's possessory interests in that property." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (emphasis added). By employing the term "meaningful interference," the Supreme Court must have "contemplated excluding *inconsequential interference* with an individual's possessory interests." *United States v. Va Lerie*, 424 F.3d 694, 706 (8th Cir. 2005) (en banc). . . . A seizure requires law enforcement agents to exercise a fair degree of dominion and control over the property. *See Jacobsen*, 466 U.S. at 120 (field testing contents of a package for illegal substances was "meaningful interference"); *Hudson v. Palmer*, 468 U.S. 517, 544 (1984) (completely destroying the property was "meaningful control").

> Appellant withdrew his consent while the media were still sitting in his room. While the agents may have moved the media to a central location in the room, they did not meaningfully interfere with it until they removed it. As the seizure of the media occurred after Appellant had withdrawn his consent, the seizure violated the Fourth Amendment.

Id.

Although *Hahn* and *Hoffman* addressed the seizure of physical property, their analysis is equally applicable to the attempted seizure of digital content in this case. CID was endeavoring to seize but had not yet seized the digital content on Appellant's iPhone because, even as CID was attempting to "exercise a fair degree of dominion and control over the property," *Hoffman*, 75 M.J. at 124, Appellant was able to easily "gather up the property and move it." *Hahn,* 44 M.J. at 362.

This is true even if the taking of the iPhone limited Appellant's ability to access its digital content. Although Appellant could no longer access the digital content in the same manner after the iPhone was physically taken from her by law enforcement, she was able to access and delete it by using another device. The ability to remotely delete digital content is a common feature of cell phones, and Appellant did not have to take extraordinary measures in order to accomplish it. Her ability to completely remove all of the digital content from the iPhone with a readily available function shows that notwithstanding any limitations on her access, law enforcement had not yet established "a fair degree of

dominion or control over the [digital content]." *Hoffman*, 75 M.J. at 124.

In light of the foregoing analysis, we conclude that authorized personnel were "endeavoring to seize" the digital media on Appellant's iPhone when she remotely erased the digital content on it. We answer the remaining granted issue in the negative.

IV. Conclusion

The decision of the United States Army Court of Criminal Appeals is affirmed.

Judge MAGGS, dissenting.

The Court and I agree on a key proposition in this case: the legal sufficiency of the evidence turns on whether the alleged misconduct—erasing the digital content of a cell phone—occurred *after* government agents had "seized" the phone and its contents. This proposition flows directly from the text of Article 131e, Uniform Code of Military Justice (UCMJ), 10 U.S.C. § 931e (2018), under which Appellant was found guilty of "[p]revention of authorized seizure of property." By its terms, the article concerns only obstructive acts committed while government agents "are seizing, are about to seize, or are endeavoring to seize property." Misconduct occurring after government agents have already seized the property cannot violate Article 131e, UCMJ. Whether such misconduct might violate some other punitive article is not at issue in this appeal.

The Court and I, however, disagree about the test for when a "seizure" occurs. The Court holds today that a seizure is not complete until "a person authorized to seize certain property *has possession of the property and exercises dominion over it to the exclusion of all others*." (Emphasis added.) I cannot agree with this holding because it is contrary to long-standing precedent establishing that a seizure occurs "when there is some meaningful interference with an individual's possessory interests in that property." *United States v. Hahn*, 44 M.J. 360, 362 (C.A.A.F. 1996) (quoting *United States v. Jacobsen*, 466 U.S. 109, 113 (1984)). With its new holding, the Court has fundamentally transformed the definition of what constitutes a "seizure" so that, in determining whether a seizure occurred, the Court no longer

focuses on whether government agents have interfered with an individual's possession of property but instead focuses on whether government agents have acquired the same exclusive possession as the property owner. This is an unwarranted departure from precedent that significantly raises the bar for what constitutes a seizure. I therefore respectfully dissent.

I. Analysis

Article 131e, UCMJ, provides:

> Any person subject to this chapter who, knowing that one or more persons authorized to make searches and seizures are seizing, are about to seize, or are endeavoring to seize property, destroys, removes, or otherwise disposes of the property with intent to prevent the seizure thereof shall be punished as a court-martial may direct.

The specification at issue in this case alleged that Appellant violated Article 131e, UCMJ, "[i]n that [she] 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 cellphone."

Appellant contends that the Government failed to prove that the erasure of the digital content occurred when agents were "seizing, [were] about to seize, or [were] endeavoring to seize property." She argues that the erasure happened *after* the seizure had already occurred and that the seizure occurred either when the agents took possession of her phone or

when they placed it in a Faraday bag[1] to prevent it from receiving signals. Appellant contends that the agents had effectively seized her digital data when they had secured her physical phone and, thus, that the agents were no longer seizing, about to seize, or endeavoring to seize the digital content of the phone.

I agree with Appellant's position based on this Court's precedent in two decisions: *Hahn*, 44 M.J. 360, and *United States v. Hoffmann*, 75 M.J. 120 (C.A.A.F. 2016). Both of these cases rely on the Supreme Court's decision in *Jacobsen*, 466 U.S. 109.

In *Hahn*, the appellant removed stolen property from a house after learning that government agents were planning to search the house. 44 M.J. at 361. The appellant pleaded guilty to an enumerated offense under Article 134, UCMJ, that was very similar to the offense now codified in Article 131e, UCMJ. *Id.* (citing *Manual for Courts-Martial, United States* pt. IV, para. 103 (1995 ed.)). On appeal, the appellant attacked the providence of his plea, arguing that he did not prevent government agents from "*seizing or* [*interfere when they*] *were about to seize or . . . endeavoring to seize*" the property. *Id.* at 361-62 (internal quotation marks omitted). He asserted that the government agents had already effectively seized the property when they had both located the property and had the opportunity to take physical custody of it before it was removed by the appellant. *Id.* The Court rejected this argument, holding that a "seizure" of property occurs "*when there is some meaningful interference with an*

[1] The investigating agents do not deny that they placed the phone in a bag, but testimony revealed that the Faraday bag they used was faulty.

individual's possessory interests in that property." *Id.* at 362 (emphasis added) (internal quotation marks omitted) (quoting *Jacobsen*, 466 U.S. at 113). The Court decided that such interference had not occurred because the government had not "even touched the property in question" and because of "the ease with which [the] appellant was able to gather up the property and move it to his car." *Id.*

Applying the test in *Hahn* to this case, I conclude that the Government agents "seized" Appellant's cell phone and its digital content when they took the physical cell phone from her possession, because taking the cell phone *meaningfully interfered* with her possessory interest. "A person's '*possessory* interest' in property 'derives from rights in property delineated by the parameters of law.'" *United States v. Visser*, 40 M.J. 86, 90 (C.M.A. 1994) (quoting *United States v. LaFrance*, 879 F.2d 1, 7 (1st Cir. 1989)). One such right is "[t]he right to exclude," which is "'one of the most treasured' rights of property ownership." *Cedar Point Nursery v. Hassid*, 594 U.S. 139, 149 (2021) (quoting *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419, 435 (1982)). In addition, "[p]ossession . . . involves the exercise of dominion and control over the thing allegedly possessed." *United States v. Myers*, 20 C.M.A. 269, 270-71, 43 C.M.R. 109, 110-11 (1971) (citing *United States v. Romano*, 382 U.S. 136 (1965)). "By its very nature possession is unique to the *possessor*." *Id.* at 271, 43 C.M.R. at 111 (emphasis added) (internal quotation marks omitted).

Thus, a seizure occurs when the government "deprives the *individual* of dominion over his or her person or property." *Horton v. California*, 496 U.S.

128, 133 (1990) (emphasis added). That is what occurred in this case before the phone was wiped. And although Appellant later appears to have found a way to erase the phone's data remotely, she could not use the phone or freely access its contents using the cell phone's screen as she could have done if she still had possession of the phone. Thus, both her possession of the physical phone—which neither the Government nor the Court denies was seized—and its digital data were seized before the alleged misconduct occurred.

Although the Court cites *Hahn* in its opinion, the Court departs from *Hahn*'s holding that a seizure of property occurs "when there is some meaningful interference with an individual's possessory interests in that property." 44 M.J. at 362. The Court instead adopts a new standard, contrary to precedent, that a seizure occurs only "when a person authorized to seize certain property *has possession of the property and exercises dominion over it to the exclusion of all others*." (Emphasis added.) In so doing, the Court turns on its head the test of when a seizure occurs. The test established in *Hahn* focuses on whether the government has interfered with an *individual's* possession. The Court's new test improperly focuses instead on whether the *government* has acquired so great a possessory interest in property that no one else can interfere with it. The Court thereby seemingly creates an unobtainable seizure standard because the government does not acquire the same property interest as the property owner when it takes possession of property for law enforcement purposes.[2]

---

[2] The new "dominion . . . to the exclusion of all others" test is not only higher than *Hahn*'s "meaningful interference" test,

Second, in *Hoffmann*, the accused initially consented to a search of his quarters but withdrew his consent shortly after investigators started gathering his "digital media," which included a laptop.[3] 75 M.J. at 123. The appellant withdrew his consent while the physical media was still sitting in the room. *Id.* Although investigators terminated the search, they then removed the digital media items they had started collecting during the search. *Id.* A dispute arose about whether the investigators had already seized the media before the appellant withdrew his consent while the media was still sitting in the room, or if they had not yet seized the media until they removed the physical items from the room after the appellant withdrew his consent. *Id.* at 123-24. Applying the test in *Hahn*, the Court held that the digital media had not been seized before the appellant withdrew his consent, explaining: "While the agents may have moved the media to a central location in the room, they did not *meaningfully interfere* with it until they removed it."

---

but it is so high that it is seemingly impossible to satisfy. For example, suppose the government takes physical evidence from the accused and locks it in a government building, but the accused is still able to destroy the evidence by burning down the building. *See United States v. Mix*, 35 M.J. 283, 289 (C.M.A. 1992) (concerning an appellant who was charged with burning down the staff judge advocate's office and courtroom, presumably to destroy evidence). If the test is "dominion . . . to the exclusion of all others," the conclusion must be that the physical evidence locked in the government building, which was physically inaccessible to the accused, had not yet been seized because accused could still destroy it.

[3] The opinion of the Court of Criminal Appeals in this case clarified that the "digital media" included a laptop, thumb drives, and DVDs. *United States v. Hoffmann*, 74 M.J. 542, 546 (N-M. Ct. Crim. App. 2014), *rev'd*, 75 M.J. 120 (C.A.A.F. 2016).

Id. at 124 (emphasis added). Accordingly, the seizure occurred after the appellant had withdrawn his consent. *Id.* Notably, throughout its opinion, the Court made no distinction between the seizure of the physical computer equipment and its digital content.

In this case, the seizure of Appellant's phone went far beyond the "*inconsequential interference*" that occurred in *Hoffmann*. *Id.* (citation omitted) (internal quotation marks omitted). And like the Court in *Hoffmann*, I see no legal distinction in this case between the seizure of Appellant's phone and the digital content of the phone. Accordingly, based on *Hahn* and *Hoffmann*, I would conclude that the seizure of both the phone and the data was complete before the phone was remotely wiped.

Two remaining points require attention. First, the Government argues that a seizure of the digital content could not occur "until the law enforcement agents were able to extract the contents of Appellant's cell phone," which had not happened before the cell phone was wiped. The Government, however, cites no precedent in support of this proposition and does not attempt to reconcile it with the Court's analysis in *Hoffmann*. The Government's proposal that a seizure does not occur until digital content is extracted, if adopted, would also have sweeping consequences. Although this case involves digital content, the logic of the proposed test would suggest that a recording of a wiretap does not constitute a seizure until agents listen to the recording. This is contrary to Supreme Court precedent. *See Katz v. United States*, 389 U.S. 347, 353 (1967) (recording oral statements is a seizure). For these reasons, I cannot accept the Government's

position.

The second point concerns the rule of lenity, which the dissenting opinion in the United States Army Court of Criminal Appeals briefly addressed. *See United States v. Strong,* 83 M.J. 509, 519 n.16 (A. Ct. Crim. App. 2023) (Arguelles, J., dissenting). This rule generally provides that "criminal statutes are to be strictly construed, and any ambiguity resolved in favor of the accused." *United States v. Thomas,* 65 M.J. 132, 135 n.2 (C.A.A.F. 2007). For the reasons stated above, I would not find any ambiguity in the application of Article 131e, UCMJ, to digital data. But if the disagreement between the Court and me suggests that the seizure of digital content in this case makes application of the words of Article 131e, UCMJ, and this Court's precedent effectively ambiguous, then the Court should resolve the ambiguity in Appellant's favor using the rule of lenity.

II. Conclusion

The evidence in this case was legally insufficient to show that Appellant's conduct violated Article 131e, UCMJ. Whether Appellant's conduct might have violated some other punitive article is not an issue before this Court. I therefore would set aside the finding that Appellant is guilty of violating Article 131e, UCMJ, and remand the case for a sentence reassessment or a new hearing on sentencing.

APPENDIX B

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

---

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

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 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,

---

[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.

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 Ml085 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 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]

---

[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 13 l(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

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)).

---

defense to violation of the statute that a search or seizure was defective, further belying the necessity of a warrant to prove the charge.

> 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

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

carefully attending to the words it chose rather 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]

---

[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

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 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

---

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.

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.*

---

[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.

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

---

[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.merriamwebster.com/dictionary/present%20participle (last visited 29 Sep 2022)

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 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

---

[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

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 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

---

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.

or copied. Appellant's conviction is both legally and factually sufficient. [15]

---

[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.

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 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]

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

---

[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.3 l 6(c)(l), (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. 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.").

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 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]

---

[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

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,* l M.J. 50, 53 (C.M.A. 1975); *United States v. McGee,* l 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*

---

able to delete her data remotely while the agents were still waiting for Apple to respond, such conduct would fit the Article 13 le, 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.

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:
>
> 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

[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.

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 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 13 le, 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.

APPENDIX C

United States Court of Appeals
for the Armed Forces
Washington, D.C.

United States,
Appellee

USCA Dkt. No. 23-0107/AR
Crim.App. No. 20200391

v.

O R D E R

Ladonies P.
Strong,
Appellant

On consideration of Appellant's petition for reconsideration of the decision issued by the Court, __MJ.__ (C.A.A.F. 2024), it is, by the Court, this 20th day of September, 2024,

ORDERED:

That the petition for reconsideration is hereby denied.

For the Court,

Malcolm H. Squires, Jr.
Clerk of the Court

cc: The Judge Advocate General of the Army
Appellate Defense Counsel (Flynn)
Appellate Government Counsel (Emmons)