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. Ladonies P. Strong,		<u>ORDER</u>
	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.		

/s/ Malcolm H. Squires, Jr. Clerk of the Court

For the Court,

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

UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES

UNITED STATES

Appellee

 \mathbf{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 (CID) agents seized the iPhone pursuant to a valid search authorization. The courtmartial 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

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.

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 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.

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.

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:

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.

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

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.

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. 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.

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 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

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

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 revealed that about an hour after CID's seizure of the Apple Watch and iPhone, someone using Appellant's iCloud account⁸ searched the Internet for "find my iphone," accessed webpages related to the service "Find My iPhone," and issued a command to erase the digital content from Appellant's iPhone. The command came from an IP

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.

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.

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 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 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

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.

¹¹ As the ACCA noted:

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 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.

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.)

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

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

Strong, 83 M.J. at 516.

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.

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 statute¹⁴ 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 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.

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.

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 bag¹ 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*,

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.

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 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. Ro*mano, 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, 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)

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." 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

⁽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).

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.