UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES

UNITED STATES Appellee

v.

Ethan R. SHIELDS, Staff Sergeant United States Marine Corps, Appellant

No. 22-0279

Crim. App. No. 202100061

Argued February 21, 2023-Decided April 28, 2023

Military Judges: Derek D. Butler (arraignment) and Eric A. Catto (motions and trial)

For Appellant: *Lieutenant Aiden J. Stark*, JAGC, USN (argued).

For Appellee: Captain Tyler W. Blair, USMC (argued); Colonel Joseph M. Jennings, USMC, Lieutenant Gregory A. Rustico, JAGC, USN, and Brian K. Keller, Esq. (on brief); Lieutenant James P. Wu Zhu, JAGC, USN.

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

Chief Judge OHLSON delivered the opinion of the Court.

This Court again confronts the issue of what constitutes a reasonable search of a servicemember's phone. And as always, the resolution of this issue depends on the specific facts of the case.

In the instant case, Appellant's phone was lawfully seized to search for location data generated on a specified date. After a digital forensic examiner extracted images from Appellant's phone, he sorted them by file size rather than first filtering them by the date specified in the search authorization. Upon doing so, the forensic examiner saw a thumbnail image of what he suspected was child pornography. After obtaining an expanded search authorization, the examiner indeed found evidence of child pornography, as well as indecent recordings, and Appellant was eventually charged and convicted of offenses related to those images.

At trial, Appellant filed a motion to suppress this evidence obtained from his phone on the grounds that the search violated his Fourth Amendment rights. The military judge denied the motion. We granted review of the following issue:

> Where the search authorization only sought materials from one date, but the government looked at images irrespective of that date, did the military judge abuse his discretion by finding the search did not violate the Fourth Amendment?

United States v. Shields, 83 M.J. 95 (C.A.A.F. 2022) (order granting review).

For the reasons set forth below, we hold that the search did not infringe upon Appellant's constitutional rights. Accordingly, we hold that the military judge did not abuse his discretion in denying the defense motion to suppress. We therefore affirm the judgment of the United States Navy-Marine Corps Court of Criminal Appeals (NMCCA).

I. Background

On December 23, 2018, nine Marine recruits reported to their chain of command that the driver of a car exposed his genitals to them while they were walking on base at the Marine Corps Recruit Depot, Parris Island. A preliminary investigation pointed to Appellant as the culprit. To confirm Appellant's whereabouts on December 23, law enforcement obtained a search authorization that permitted them to search for "all location data stored on [Appellant's] phone or within any application within the phone for 23 Dec [20]18." By searching Appellant's phone for location data, law enforcement hoped to pinpoint Appellant at the scene of the exposure. For reasons unclear in the record, this search authorization was not issued until May 2, 2019.

Appellant surrendered his iPhone to military law enforcement that same day. It was then sent to the Defense Cyber Crime Center (DC3) which extracted all data from the iPhone for digital forensic analysis. The designated forensic examiner was provided with a copy of the search authorization which he read before beginning his search. He then used software known as Cellebrite Physical Analyzer (Cellebrite) to organize the extracted data into a readable format so he could begin his search. He initially searched through the "parsed data," which is sorted into categories, such as "device locations," "internet history," "texts," and "images." The examiner next searched within the "device locations" category but was unable to find any relevant location data from December 23, 2018. Since the most obvious place to search was unfruitful, the examiner determined he needed to broaden his search.

Based on his training and experience, the examiner knew that image files often contain embedded unparsed Global Positioning System (GPS) location information. With this in mind, he proceeded to open the "images" category. This placed the over 200,000 images extracted from Appellant's phone into "row after row after row of little thumbnail views" of individual pictures. With a single click of his computer mouse, the examiner reorganized these

images into a "table view." This table view arranged each thumbnail image in its own row with corresponding columns which contained pertinent data such as filename, file size, and date the file was created. Once in table view, the examiner was able to further sort and filter these images. The examiner then sorted the images by file size in descending order. This step bumped previously unseen images to within his view. In other words, the images taking up the most digital storage percolated to the top of the examiner's screen. The examiner testified that his intent after sorting the images from largest to smallest was to begin filtering by date. However, before he could apply a date filter to isolate images from December 23, he immediately noticed a thumbnail image of what he believed to be a depiction of child pornography. The examiner testified that this image was visible within his screen without scrolling. The examiner did not click on, open, or manipulate the suspected contraband image. Instead, he stopped his search and consulted with his supervisor. Together, they determined not to continue with the search until after obtaining a new search authorization. The examiner resumed his search once he received an additional search authorization allowing him to search for suspected child pornography. This broadened search uncovered evidence of additional misconduct, including child pornography and indecent recordings, for which Appellant was eventually charged.

Before trial, Appellant moved to suppress evidence obtained from the expanded search. Appellant claimed the original search violated his Fourth Amendment rights because the examiner sorted by file size *before* filtering by date. Essentially, Appellant argued the examiner exceeded the scope of the search authorization. To support this claim, the defense hired a digital forensic expert. An Article 39(a), Uniform Code of Military Justice (UCMJ),¹ session was held where the parties presented additional evidence and offered oral argument. The defense expert testified that the examiner should not have initiated his search by

¹ 10 U.S.C. § 839(a) (2018).

sorting by file size, and that if he had not done so the contraband image would not have come into the examiner's view. Fundamentally, Appellant argued that there was no proper reason for the examiner to first sort by file size and by doing so, the examiner violated Appellant's Fourth Amendment rights.

After considering the defense motion, the Government's response, and the evidence and arguments presented by counsel, the military judge denied the motion to suppress. The military judge found that the search of the content of Appellant's iPhone "was conducted lawfully, since it was conducted in a reasonable manner and did not exceed the scope" of the search authorization. The military judge explained that the examiner saw the suspected image of child pornography during the "process of trying to sort the images by size and date." He noted that the suspect image was the tenth image from the top of the screen, "not something like the 300th image out of 220,141, which suggests that this contraband image was in plain view."

After the military judge's denial of the motion to suppress, Appellant entered into a plea agreement with a mix of conditional and unconditional pleas. The conditional guilty pleas allowed Appellant the right to appeal the military judge's suppression rulings, including his motion regarding the phone search. Pursuant to Appellant's unconditional pleas, a military judge, sitting alone as a general court-martial, found Appellant guilty of one specification of indecent exposure, in violation of Article 120c, UCMJ, 10 U.S.C. § 920c (2018). Pursuant to Appellant's conditional pleas, the military judge convicted Appellant of one specification of attempted indecent visual recording, one specification of wrongful use of a controlled substance, one specification of indecent visual recording, and one specification of viewing child pornography, in violation of Articles 80 and 120c, UCMJ, 10 U.S.C. §§ 880, 920c (2012), and Articles 112a and 134, UCMJ, 10 U.S.C. §§ 912a, 934 (2018). The military judge then sentenced Appellant to a dishonorable discharge, confinement for fifty-two months, reduction to the grade of E-1, and forfeiture of all pay and allowances

for fifty-two months. The convening authority approved the sentence as adjudged.

On appeal to the NMCCA, Appellant asserted two assignments of error, including whether "the forensic search of Appellant's cellphone constituted an unlawful general search in violation of the Fourth Amendment." *United States v. Shields*, No. NMCCA 202100061, 2022 CCA LEXIS 448, at *1, 2022 WL 2966378, at *1 (N-M. Ct. Crim. App. July 27, 2022) (per curiam) (unpublished). In rendering its opinion, the NMCCA determined:

While we find the DC3 examiner's search methodology concerning, we find no abuse of discretion in the military judge's ruling....

. . . .

... [W]e do not find that the military judge clearly erred when he found "no evidence to suggest that [the examiner] was rummaging through areas of [Appellant's phone] where the [search authorization] did not allow him to look." Although the examiner's search methodology was less than ideal, it was directed toward finding location data for 23 December 2018, in compliance with the search authorization. There is nothing in the record that indicates he was deliberately searching for child pornography, and once he saw the image at issue he immediately halted the search without further manipulating it and sought a new authorization.

Id. at *12-16, 2022 WL 2966378, at *5-6 (second, third, and fourth alterations in original) (footnotes omitted).

After considering Appellant's other assignment of error, the lower court affirmed the findings and sentence. We granted review to determine whether the military judge abused his discretion by not suppressing the evidence from the forensic examiner's search.

For the reasons articulated below, we hold that the military judge did not abuse his discretion when he concluded that the forensic examiner's search was conducted lawfully.

II. Standard of Review

"This Court reviews a military judge's ruling on a motion to suppress evidence for an abuse of discretion." United States v. White, 80 M.J. 322, 327 (C.A.A.F. 2020). An abuse of discretion occurs when a military judge's "findings of fact are clearly erroneous, the court's decision is influenced by an erroneous view of the law, or the military judge's decision on the issue at hand is outside the range of choices reasonably arising from the applicable facts and the law." United States v. Finch, 79 M.J. 389, 394 (C.A.A.F. 2020) (citation omitted) (internal quotation marks omitted). "An abuse of discretion must be more than a mere difference of opinion. The challenged action must be arbitrary, fanciful, clearly unreasonable, or clearly erroneous." United States v. Black, 82 M.J. 447, 451 (C.A.A.F. 2022) (citation omitted) (internal quotation marks omitted). "A finding of fact is clearly erroneous when there is no evidence to support the finding, or when, although there is evidence to support it, the reviewing court on the entire evidence is left with the definite and firm conviction that a mistake has been committed." United States v. Criswell, 78 M.J. 136, 141 (C.A.A.F. 2018) (citations omitted) (internal quotation marks omitted). "When reviewing a lower court's decision on a military judge's ruling, we 'typically have pierced through that intermediate level and examined the military judge's ruling, then decided whether the Court of Criminal Appeals was right or wrong in its examination of the military judge's ruling." United States v. Blackburn, 80 M.J. 205, 211 (C.A.A.F. 2020) (quoting United States v. Shelton, 64 M.J. 32, 37 (C.A.A.F. 2006)).

"In reviewing a ruling on a motion to suppress, the evidence is considered in the light most favorable to the party that prevailed on the motion," which in this case is the Government. *Id*.

III. Applicable Law

The Fourth Amendment protects "against unreasonable searches and seizures." U.S. Const. amend. IV. These constitutional protections fully apply to cell phone

searches. *Riley v. California*, 573 U.S. 373, 386 (2014). A search conducted pursuant to a search authorization is presumptively reasonable. *United States v. Wicks*, 73 M.J. 93, 99 (C.A.A.F. 2014).

Appellant does not contend that the search authorization was facially invalid or that it failed the particularity requirement. Rather, the crux of the dispute before us is whether the search methodology employed by the examiner was unreasonable and, therefore, unconstitutional. As we have previously advised, it "is folly for a search warrant to attempt to structure the mechanics of the search and a warrant imposing such limits would unduly restrict legitimate search objectives." United States v. Richards, 76 M.J. 365, 369 (C.A.A.F. 2017) (internal quotation marks omitted) (quoting United States v. Burgess, 576 F.3d 1078, 1094–95 (10th Cir. 2009)). And as emphasized by the Supreme Court, "the manner in which a warrant is executed is subject to later judicial review as to its reasonableness." Dalia v. United States, 441 U.S. 238, 258 (1979). "Instead of attempting to set out bright line rules for limiting searches of electronic devices, the courts have looked to what is reasonable under the circumstances." Richards, 76 M.J. at 369.

> [O]ne exception to the warrant requirement for items not otherwise subject to a lawful search is the plain view doctrine, which allows law enforcement officials conducting a lawful search to seize items in plain view if they are acting within the scope of their authority and have probable cause to believe the item is contraband or evidence of a crime.

United States v. Gurczynski, 76 M.J. 381, 387 (C.A.A.F. 2017). "A prerequisite for the application of the plain view doctrine is that the law enforcement officers must have been conducting a lawful search when they stumbled upon evidence in plain view." *Id.* at 388; see also Military Rule of Evidence (M.R.E.) 316(c)(5)(C) (The plain view doctrine permits an investigator to seize evidence, without a search authorization, if that "person while in the course of otherwise lawful activity observes in a reasonable fashion . . .

evidence that the person has probable cause to seize."). In other words, for the plain view exception to apply here: (1) the examiner must not have violated the Fourth Amendment in arriving at the spot from which he plainly viewed the suspected incriminating image; (2) the incriminating character of the image must have been immediately apparent to the examiner; and (3) the examiner must have had lawful access to Appellant's iPhone. *See Richards*, 76 M.J. at 371.

In Arizona v. Hicks, 480 U.S. 321 (1987), the Supreme Court identified two principles closely related to the plain view doctrine. One is that "[m]erely inspecting" items that come into view while conducting a lawful search for other items produces "no additional invasion" of an individual's privacy interests. *Id.* at 325. But on the other hand, "taking action, unrelated to the objectives of the authorized intrusion, which expose[] to view concealed [items]" invades privacy protected by the Fourth Amendment. *Id.*

IV. Discussion

Appellant asserts that two acts by the examiner constituted a Fourth Amendment violation. First, the examiner initially sorted the extracted image files by size. Appellant maintains that sorting by size first, rather than filtering by date, was "unexplainable and patently unreasonable." Brief for Appellant at 25, *United States v. Shields*, No. 22-0279 (C.A.A.F. Dec. 21, 2022). Second, Appellant alleges that after sorting by size, the examiner could not have seen the suspected child pornography photograph without scrolling. According to Appellant, Cellebrite's table view function only displayed eight images at one time. Because the suspected contraband was purportedly the tenth image, the examiner necessarily scrolled through the list, and this scrolling meant that the image was not initially in plain view. We address each of Appellant's claims in turn.

A. The initial sorting

Appellant claims that the military judge's decision to deny the suppression motion was predicated on three clearly erroneous findings of fact. First, the military judge

erroneously determined there was no evidence to suggest that the examiner was searching unauthorized areas of Appellant's phone. Second, the military judge erroneously determined the examiner saw the suspected contraband image during the process of trying to sort the images by size and date. Finally, the military judge erred in finding the examiner attempted to stay within the scope of the search authorization. We are not persuaded in regard to any of these points raised by Appellant.

When the Fourth Amendment and technology intersect—as is the case here—military judges may need to hear from, and rely on, expert witnesses. And here, the military judge properly heard from two experts with conflicting views on best practices when using the Cellebrite software. Given the evidence in the record before us and recognizing that the military judge was entitled to credit one expert over another, we do not find that any of these findings by the military judge were clearly erroneous, especially when the evidence is viewed in a light most favorable to the Government. (We caution, however, that a different military judge could have properly credited the defense expert's testimony and then concluded that the forensic examiner's search methods were improper and constituted a violation of the Fourth Amendment.)

We reiterate that as "'always under the Fourth Amendment, the standard is reasonableness.'" *Richards*, 76 M.J. at 369 (quoting *United States v. Hill*, 459 F.3d 966, 974 (9th Cir. 2006)). And when it comes to cell phones and computers, although one search method may be objectively "better" than another, a search method is not unreasonable simply because it is not optimal. Here, the examiner was not rummaging through Appellant's phone, even though the defense expert pointed to a different—and perhaps even better—way to conduct the search.

After the examiner unsuccessfully searched the iPhone's location data, he appropriately determined he needed to broaden his search. *See, e.g., United States v. Loera*, 923 F.3d 907, 920 (10th Cir. 2019) ("The reasonableness of a search evolves as the search progresses and as the

searching officer learns more about the files on the device that he or she is searching.").

The examiner articulated his reason for then looking in other areas of the cell phone that might contain location information. He testified that based on his training and personal experience, Cellebrite's sorting function often misses data. The examiner expressed his belief that had he relied solely on this sorting software, he would have missed potentially relevant data. He testified that he then decided to search for GPS data within user-generated photographs because those files often contain location data. He stated that larger image files are more likely to be user-generated photographs. The examiner reasoned that sorting by size first would bring user-generated images to the top of his screen, and therefore he would see an array of files that were more likely to contain location data. He further described his thought process that, by taking this approach, he would not have to re-sort every time he applied a new filter. He confirmed that after sorting by file size, his next step was going to be filtering for the date indicated in the authorization. Accordingly, the examiner was in the process of sorting the images by date when he came across the suspected image of child pornography.

In an exhibit filed with the defense motion to suppress, the examiner elaborated in an email on why he did not first apply a date filter when searching Appellant's phone:

> I had a conversation with one of our top examiners, he is very much in agreement that my thought process was reasonable as it is well known that photos are often embedded with GPS data, and my job is to analyze ALL DATA on the device, and not just throw the extraction into a tool and start filtering for dates that may or may not include all data.

Appellant latches onto this "ALL DATA" language as a clear articulation of the examiner's supposed disregard of the parameters of the search authorization. But the record indicates that Appellant misapprehends the meaning of the examiner's statement. The search authorization was

for "all location data stored on the phone or within any application within the phone" for December 23, 2018. Thus, the examiner was authorized to search "all data" on the device for files containing location information corresponding to a specific date. The examiner's "ALL DATA" comment, taken in context with the rest of his statement, indicates that by using this term he was solely referring to the fact that he was not restricted to certain *types* of data, (e.g., images, texts, internet browsing history), when searching Appellant's phone for location information from December 23, 2018. Therefore, the examiner was not searching "unauthorized areas" of the cell phone, and his email is not evidence of "intentional disregard" of the limitations of the search authorization.

This brings us to what may appear to be the circuitous nature of the examiner's search. If the examiner *knew* the specific date to search—December 23, 2018—then why didn't he *first* filter by date and *then* sort by size? Indeed, it was feasible for him to do so. But again, based on that fact alone we cannot conclude that the examiner's actions here amounted to the "general exploratory rummaging" that the Fourth Amendment is designed to prevent. *Richards*, 76 M.J. at 369 (internal quotation marks omitted) (quoting *United States v. Carey*, 172 F.3d 1268, 1272 (10th Cir. 1999)).

It may be difficult for an individual lacking firsthand experience with Cellebrite or other digital forensic software (such as a military judge, perhaps) to have an informed opinion on the reasonableness of an examiner's methodology. Thus, it was permissible for the military judge in this case to rely on expert testimony to assist him in assessing this important issue. *See* M.R.E. 702(a) (providing that an expert witness may provide testimony if it "will help the trier of fact to understand the evidence or to determine a fact in issue"). Here, the military judge recognized the forensic examiner as an expert in digital forensic examinations, and Appellant does not challenge that finding on

appeal.² Nonetheless, we acknowledge that the defense expert concluded that the forensic examiner "employed poor forensic search techniques" and that the search should have been conducted according to the procedures outlined in the defense expert's report. But at bottom, the examiner and the defense expert simply disagreed on the best methodology for searching Appellant's phone.

Appellant claims the military judge "wholly disregarded the directly contradicting testimony" from the defense expert. Brief for Appellant at 32, United States v. Shields, No. 22-0279. But the military judge, as the trier of fact, had the discretion-indeed, responsibility-to credit one expert over another. See United States v. Sanchez, 65 M.J. 145, 153 (C.A.A.F. 2007) (noting that the trier of fact "'must decide among the conflicting views of different experts'" (quoting Kumho Tire Co. v. Carmichael, 526 U.S. 137, 153) (1999))); Wipf v. Kowalski, 519 F.3d 380, 385 (7th Cir. 2008) ("[I]n a case of dueling experts . . . it is left to the trier of fact, not the reviewing court, to decide how to weigh the competing expert testimony."); United States v. Pervis, 937 F.3d 546, 554 (5th Cir. 2019) ("Though we are to take a hard look at the record, it is not our task, as an appellate court, to relitigate the battle of the experts." (alteration in original removed) (citation omitted) (internal quotation marks omitted)). Because the military judge was entitled to credit the forensic examiner over the defense expert, there is sufficient evidence in the record to support the military judge's findings in this case. And upon reviewing the

² Appellant does, however, argue the examiner's Cellebrite certification had expired, and therefore the examiner was less credible than the defense expert, who had *three* active certifications related to Cellebrite. But the status of certifications is not dispositive of such an issue, and the military judge still had the authority to recognize the examiner as an expert. See M.R.E. 702 (permitting an expert to be qualified by reason of knowledge, skill, or experience rather than education); United States v. Flesher, 73 M.J. 303, 316 (C.A.A.F. 2014) (noting "experience in a field may offer another path to expert status" (internal quotation marks omitted) (quoting United States v. Frazier, 387 F.3d 1244, 1260-61 (11th Cir. 2004))).

entire record before us, we are not "left with the definite and firm conviction that a mistake has been committed." *Criswell*, 78 M.J. at 141 (citation omitted) (internal quotation marks omitted).

In light of the evidence before us, we conclude the military judge reasonably found that the forensic examiner discovered the suspected contraband while trying to sort the images by size and date, and that the examiner attempted to stay within the scope of the authorization. We do not deny that the defense expert might have conducted a narrower search. But given the examiner's explanation of whyhe sorted by file size first, and the competing expert testimony, we cannot conclude that his methodology was unreasonable. See Dalia, 441 U.S. at 257 ("[I]t is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant").

B. The alleged scrolling

Appellant next argues that the military judge abused his discretion by failing to find that the forensic examiner needed to scroll through the images in order to find the suspected child pornography, an act which may have negated the applicability of the plain view doctrine to this case. Appellant seeks to support his contention by pointing to the fact that at the Article 39(a) session, the examiner testified to his recollection that out of over 200,000 images listed in table view after sorting by file size, the suspected contraband image was the tenth picture from the top of his screen. (Consistent with this testimony, the military judge found that "[t]his image was the tenth image from the top" of the examiner's screen.) Appellant maintains, however, that the defense expert's declaration and corresponding testimony establish that Cellebrite's table view function displays only eight lines at one time, and because the image at issue was on the tenth line, the examiner necessarily must have scrolled down in order to view the incriminating image. According to Appellant, "scrolling through two images (the two images beyond the eight initially displayed on [the examiner's] monitor after he sorted them by size)

must have" meant that the offending image was initially out of plain view. Brief for Appellant at 33, *United States v. Shields*, No. 22-0279. But as shown below, the evidence is not as clear-cut as the defense apparently believes.

Here, the examiner—who was recognized as an expert in digital forensics—testified that the contraband image "was visible within [his] screen without even scrolling." In addition, the defense expert's testimony did not establish that table view only displays eight lines; he merely stated that "the *default* is eight lines." (Emphasis added.) Indeed, the examiner testified that the number of lines visible in table view "depends on things like screen resolution, how big your monitor is, [and] how you have the tool adjusted." Thus, it was permissible for the military judge to conclude that the forensic examiner had a larger monitor or had changed the software's settings allowing him to immediately see this tenth image.

It is true the military judge did not *explicitly* state that the examiner did not scroll, but it is reasonably implied in his findings. The military judge found that before the examiner could filter by date, he "saw that one of the first ten images, out of over 200,000 images, appeared to be an image containing child pornography." Furthermore, the military judge found that the examiner "did not open or further manipulate the suspect image file." Finally, the military judge cited approvingly the examiner's testimony that the suspect image "was visible within his screen without even scrolling." Therefore, the record adequately supports the military judge's finding that the examiner did not need to scroll through the images to see the suspected child pornography and we are in no position to second guess that finding.³ And because the military judge found that the examiner did not need to scroll through the images to see the suspected child pornography, the examiner did not take "action, unrelated to the objectives of the authorized

³ Even if less than full deference *were* to apply to the military judge's findings, as urged by Appellant, it is entirely unclear why this Court should then fully credit Appellant's version of events.

intrusion, which exposed to view concealed [items]" in violation of the principles of *Hicks*, 480 U.S. at 325.

C. Conclusion

The record before us does not establish that this search was one of the "wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). Indeed, in light of our discussion above, we conclude the military judge did not abuse his discretion in finding that the search did not violate the Fourth Amendment. Consequently, because the contraband was discovered in plain view during a lawful search, the exclusionary rule is not implicated. *See Horton v. California*, 496 U.S. 128, 141 (1990) (noting that "an object in plain view does not involve an intrusion on privacy").

V. Judgment

The judgment of the United States Navy-Marine Corps Court of Criminal Appeals is affirmed.⁴

⁴ It is noted that the decision of the United States Navy-Marine Corps Court of Criminal Appeals incorrectly summarized the findings. As mentioned, Appellant was convicted of attempted indecent visual recording, wrongful use of a controlled substance, indecent exposure, indecent visual recording, and viewing child pornography, in violation of Articles 80, 112a, 120c, and 134, UCMJ. The lower court mistakenly stated that he also was convicted of wrongful possession of a controlled substance and possession and production of child pornography, in violation of Articles 112a and 134, UCMJ.