IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES

UNITED STATES, Appellee v. Ethan R. SHIELDS Staff Sergeant (E-6) United States Marine Corps, Appellant	**BRIEF ON BEHALF OF APPELLANT** Crim.App. Dkt. No. 202100061 USCA Dkt. No. 22-0279/MC

TO THE JUDGES OF THE UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES:

Aiden J. Stark
LT, JAGC, USN
Appellate Defense Counsel
Navy-Marine Corps Appellate Review Activity
1254 Charles Morris Street, SE
Building 58, Suite 100
Washington, DC 20374
(202) 685 - 7292
aiden.j.stark2.mil@us.navy.mil
CAAF Bar No. 37598

Index of Brief

Table of Cases, Statutes, and Other Authorities

Issue Presented

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?

Introduction

This case involves a Fourth Amendment violation of systemic proportions. An organization of Government investigators utilize what the lower court called "an unwritten policy of defaulting to manual review of data files, even where a search authorization contains specific search limitations."[1] They apply this unwritten policy while rummaging through what may be the most inherently private database held by individuals today: the cell phone.

The cell phone search authorization in this case was extremely narrow. It was intentionally so. The Commanding Officer who signed it only wanted investigators to seek materials from one date: December 23, 2018—and nothing further.

The Government ignored this extremely narrow parameter. Its investigator rummaged through the largest-sized files of over two hundred thousand images irrespective of their date. He knew he could have filtered the files by date to limit what he looked at; in fact, he planned to sort by date *after* rummaging through the largest of thousands of materials from innumerable dates. But he did not. He believed—and his organization agreed—he had the right to review *everything*.

His deliberate, culpable, and flagrant disregard of the search authorization's limitations was precisely what the exclusionary rule was designed to curb.

[1] *United States v. Shields*, No. 202100061, 2022 CCA LEXIS 448, at *15 (N-M. Ct. Crim. App. July 27, 2022).

Statement of Statutory Jurisdiction

The Convening Authority approved a court-martial sentence that included a dishonorable discharge. Accordingly, the lower court had jurisdiction under Article 66(b)(3), Uniform Code of Military Justice (UCMJ).[2] This Court has jurisdiction under Article 67(a)(3), UCMJ.[3]

Statement of the Case

A military judge in a general court-martial convicted SSgt Shields, consistent with his conditional pleas, of violating Article 80, UCMJ (attempted indecent recording); Article 112a, UCMJ (use of controlled substance); Article 120c, UCMJ (indecent exposure and visual recording); and Article 134, UCMJ (viewing child pornography). The military judge sentenced him to fifty-two months' confinement, total forfeitures, reduction to E-1, and a dishonorable discharge.

On July 27, 2022, the lower court affirmed the findings and sentence.[4]

[2] 10 U.S.C. § 866 (2020).
[3] 10 U.S.C. § 867 (2020).
[4] *Shields*, No. 202100061, 2022 CCA LEXIS at *22.

Statement of Facts

A. Law enforcement was authorized to search SSgt Shields's cell phone only for location data from December 23, 2018.

Nine recruits reported that on December 23, 2018, a man in a dark gray Honda exposed his genitals onboard Marine Corps Recruit Depot ("MCRD") Parris Island.[5] The Criminal Investigation Division ("CID") learned that a gray Honda registered to SSgt Shields departed MCRD Parris Island twice that day.[6] Two recruits identified him in a photographic lineup.[7] CID interviewed SSgt Shields three times.[8] He admitted he may have been onboard MCRD Parris Island on December 23, 2018 and that he changed his clothing in his vehicle after going to the gym.[9] Video footage confirmed he was at the gym that day.[10]

On May 2, 2019, SSgt Shields's Commanding Officer signed a search authorization.[11] It authorized CID to search SSgt Shields's phone for location data generated on December 23, 2018.[12]

---

[5] J.A. at 164, 198.
[6] J.A. at 205-07, 214.
[7] J.A. at 215-232.
[8] J.A. at 239, 241, 243-44, 271.
[9] J.A. at 239, 241, 243-44, 271.
[10] J.A. at 265-66.
[11] J.A. at 276-77.
[12] J.A. at 277.

B. The Commanding Officer intentionally limited the scope of the search authorization by date.

The Commanding Officer testified that he signed the search authorization because "I need[ed] something that puts him at a place and a time."[13] He explained that "what I was looking for was, I need[ed] something definitive . . . [that] places him at that intersection at that time and place."[14] The Commanding Officer testified that he purposefully "limited" CID's ability to search the phone with the understanding that the search:[15]

> isn't free reign. You don't get to go into everything on the phone. He still does have privacy. It is limited to what you are looking for, which is location and place. Beyond that, you know, you just can't go in and it is not a free for all on the phone.

The Commanding Officer explained, "what we were concerned about was, look, you know, you don't just go into the phone and start searching for whatever you want. It's very limited and it is scoped and it is down to your specific objectives."[16] He testified that he did not intend to have the entire phone searched

[13] J.A. at 506 (emphasis added).
[14] J.A. at 496.
[15] J.A. at 506.
[16] J.A. at 509.

but rather wanted to "limit [the search] to certain things . . . all I cared about was time and place."[17]

The Commanding Officer's intent was clearly conveyed in the search authorization. As the trial counsel explained, the search authorization "was actually very specific in what he [the Commanding Officer] was looking for, which was location data for a particular date."[18]

C. The Government's digital examiner rummaged through the largest of over two hundred thousand images irrespective of their date.

Understanding that the search authorization only sought location data from one particular date, CID forwarded the cell phone to the Defense Cyber Crime Center ("DC3") to be searched.[19] CID expected DC3 to only seek materials from December 23, 2018 because, as CID's agent testified, "I believed that they would try [to limit their search] and that they had the capability to."[20]

Mr. Carl Smith, a "master forensic examiner" at DC3, was assigned to search the phone pursuant to the search authorization.[21] Mr. Smith understood the date limitation of the search authorization and, before beginning his analysis, wrote that it sought location data from December 23, 2018.[22]

---

[17] J.A. at 532.
[18] J.A. at 661.
[19] J.A. at 419, 474, 483.
[20] J.A. at 483.
[21] J.A. at 090-95, 106, 549-51.
[22] J.A. at 106, 553-54, 562 ("it was requesting location data from a certain date").

After downloading the contents of the cell phone, Mr. Smith installed the 'Cellebrite' analyzer forensic software to his computer.[23] The Cellebrite software allowed him to search the contents of the phone and organize them into categories derived from "parsed data"—meaning extracted data that had been converted into a readable format.[24] Using the software, he first searched the "device location" category, but the phone did not contain any parsed location data from December 23, 2018.[25] He then looked for location data in other places to see if it had been improperly categorized.[26]

Mr. Smith opened the "images" category in his analyzer because location coordinates are often embedded in photographs.[27] The "images" category contained 215,767 thumbnail images—some of which displayed on Mr. Smith's monitor.[28] Mr. Smith re-organized the thumbnail images into a "table view" that displayed each file in its own row with corresponding columns such as file name and size.[29] In this view, Mr. Smith had the ability to sort the images by column, and he could filter them by date.[30]

---

[23] J.A. at 555.
[24] J.A. at 556-58, 615.
[25] J.A. at 557-59.
[26] J.A. at 559.
[27] J.A. at 560.
[28] J.A. at 109.
[29] J.A. at 561-62.
[30] J.A. at 561-62.

But Mr. Smith did not filter the images by date. Instead, he *sorted* the images by descending file size to view the largest-sized files of over two hundred thousand images irrespective of their date.[31] He stated he "was going to *eventually* filter down" but that he "wanted to look at them first, *see if there were a significant amount of photos* with GPS data, and start filtering from there."[32]

D. Mr. Smith admitted that he did not have to search the phone this way, but claimed that he had his reasons.

Mr. Smith admitted that he could have applied a filter before sorting the images by size and looking at the largest of over two hundred thousand images irrespective of their date.[33] He understood that "with a sort, you're typically going to see everything; but with a filter, you're not."[34] He gave several explanations as to why he sorted the images by size rather than apply a date filter.

One explanation Mr. Smith provided was that he began manually searching through all files on the phone because he felt it was necessary to look through unparsed data on the cellular phone.[35] However, he later admitted that "photographs are parsed data."[36] Mr. Peden, the defense digital forensics expert, likewise explained that images on cell phones are parsed data—which is why they were in

[31] J.A. at 561-62.
[32] J.A. at 573, 586, 595 (emphasis added).
[33] J.A. at 107, 595, 597.
[34] J.A. at 605.
[35] J.A. at 569.
[36] J.A. at 587.

the "images" category on Cellebrite to begin with—and hence they can be searched using Cellebrite's filter tool.[37]

A second explanation Mr. Smith gave was that he began rummaging through the largest of over two hundred thousand images rather than filtering them by date because he had to "trust but verify everything[.]"[38] However, he also admitted that he had not found any issues with images properly parsing on the cell phone.[39] Mr. Smith explained that, even if photographs have misleading dates, they cannot have incorrect dates and their correct dates could still be parsed.[40] Mr. Smith noted that nothing in this case gave him particular reason to believe the images had not parsed correctly but, anyways, "you always verify" because "relying on filtering . . . [is] incomplete."[41] Mr. Peden explained that this approach, which allowed Mr. Smith to "manually go through every image[,] . . . basically gives you a free for all on the phone to look at anything you want to."[42]

A third explanation Mr. Smith provided was that sorting the images by size before looking through "a significant amount of photos" and filtering by date allowed him to look at user-taken photos rather than internet icons and other small

[37] J.A. at 119, 644, 657-58.
[38] J.A. at 109, 565.
[39] J.A. at 580-81.
[40] J.A. at 607, 609.
[41] J.A. at 588, 593-94.
[42] J.A. at 640.

files.[43] But he never stated that internet icons or small files, as opposed to photographs, would not contain location data from the pertinent date. In fact, he testified that websites can "run passively in the background" of cellular phones and download internet-based files that actually contain location data.[44] And while he believed it unlikely, he admitted that images from websites could contain geolocation data.[45]

A fourth explanation he provided was that he did not apply a date filter because "my thought processes [sic] is as I filter, the larger ones will stay at the top and I don't have to re-sort every time I apply the filter."[46] Mr. Peden explained that, in his professional opinion, this approach deviated from common sense.[47]

The lower court agreed with Mr. Peden, noting "we find the DC3 examiner's search methodology concerning[.]"[48] The lower court reasoned that "since his intention was to 'set a filter to only show photos with metadata that contains location data,' that would seem to obviate the need to sort by file size at all[.]"[49] Overall, the

[43] J.A. at 561, 586.
[44] J.A. at 571.
[45] J.A. at 583.
[46] J.A. at 562, 596.
[47] J.A. at 655-56; *see also* J.A. at 116 ("common sense would dictate that you would not start looking at pictures when only textual data values are authorized").
[48] *Shields*, No. 202100061, 2022 CCA LEXIS at *12.
[49] *Id*. at *13-14.

lower court found "it difficult to follow the examiner's logic in sorting the data in this manner[.]"[50]

E. Mr. Smith believed his job was to analyze "ALL DATA" on the phone. His colleague agreed—finding that Mr. Smith followed organizational procedures.

Mr. Smith wrote the following e-mail further explaining why he did not apply a date filter when searching the phone:[51]

> 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. I can argue that since I am also required to look for exculpatory evidence that I would be remiss for leaving this GPS data unexamined. We feel that filtering down to a date range up front will only lead to missed evidence in any exam, and there is no such "SOP" for examiners.

The Government later submitted an affidavit from Mr. Alexander Zaferiou, a highly experienced digital computer forensic examiner at DC3 who reviewed Mr. Smith's search.[52] As a computer examiner (rather than a cell phone examiner), Mr. Zaferiou did not present any certification to operate the Cellebrite software or conduct cell phone forensic searches.[53] Regardless, Mr. Zaferiou wrote that based on his years of training and experience Mr. Smith searched the phone in a reasonable manner according to normal DC3 procedures.[54]

---

[50] *Id*. at *13.
[51] J.A. at 113.
[52] J.A. at 396-400.
[53] *Compare* J.A. at 396 *with* J.A. at 639.
[54] J.A. at 396, 400.

Considering how Mr. Smith's actions were supported by another examiner at DC3, the lower court held that "[s]uch an unwritten policy of defaulting to manual review of data files, even where a search authorization contains specific search limitations, is problematic[.]"[55] The court found that such an "unwritten policy" runs against "the dangers posed by allowing digital searches to devolve into the sort of 'wide-ranging exploratory searches the Framers intended to prohibit.'"[56]

F. Mr. Smith was not certified to operate the monthly-updated Cellebrite software.

Despite being recognized by the military judge as a digital forensics expert, Mr. Smith's Cellebrite software operating certification expired by the time he conducted the search in this case.[57] He explained during his testimony in the year 2020 "[a]ll our training is basically on hold this year."[58] But his certification had not expired that year or even the previous year.[59] He was last certified in 2016, and his certification should have been renewed every two years.[60] He thus should have renewed his certification twice prior to searching Appellant's cellular phone.[61]

---

[55] *Shields*, No. 202100061, 2022 CCA LEXIS at *15.
[56] *Id*.
[57] J.A. at 550, 577.
[58] J.A. at 577.
[59] J.A. at 577.
[60] J.A. at 577.
[61] J.A. at 577.

Doing so would have allowed him to keep up with the software that, as he explained, was updated "maybe once a month."[62]

The Cellebrite software had been focused on analyzing images extracted from cell phones "for over a decade."[63] The software "is designed to not only speed up the examination for the examiner, but it is also designed to protect the right[s] and privacy of individuals . . . The tool allows the examiner to be able to comply with [limitations] and to provide what the Court ordered them to do."[64]

Not only was Mr. Smith not certified to use Cellebrite at the time of his search, but he was also not certified to conduct cell phone forensic searches at all.[65] Mr. Smith had not renewed his two types of "mobile device examiner" certifications since 2009 and 2011.[66] Although he had taken a smartphone course in 2019, the course did not renew his certifications.[67] His certifications as a forensic computer expert examiner and a Department of Defense digital forensic examiner likewise did not establish him as a certified cell phone examiner.[68] He noted in his affidavit that

[62] J.A. at 559.
[63] J.A. at 618.
[64] J.A. at 616-17.
[65] J.A. at 392, 549, 632.
[66] J.A. at 392
[67] J.A. at 392.
[68] *Compare* J.A. at 639 *with* J.A. at 392.

"I am required to demonstrate my competency annually and I have successfully done so every year that I have worked as a *computer* forensic examiner."[69]

G. Of the two expert witnesses the military judge recognized, only one was certified in cell phone forensics and the Cellebrite software: Mr. Peden.

Mr. Peden was certified to operate the Cellebrite software.[70] At the time of his testimony, and unlike Mr. Smith, he was also a certified mobile phone examiner.[71] He was the only expert the military judge recognized that was certified in cell phone forensics and Cellebrite software.[72]

Mr. Peden reviewed Mr. Smith's search and searched the cell phone himself.[73] He noted that, of the over two hundred thousand images that Mr. Smith began to look through by size and irrespective of their date, none were dated from December 23, 2018 and one was dated from December 24, 2018.[74] Mr. Peden agreed with Mr. Smith's assertion that a filter could have been immediately applied upon opening the images folder—without sorting by size.[75] Mr. Peden noted that Mr. Smith "was

---

[69] J.A. at 393 (emphasis added).
[70] J.A. at 613.
[71] J.A. at 613; *compare* J.A. at 392, 549, 632 *with* J.A. at 114, 613.
[72] J.A. at 613-14; *compare* J.A. at 392, 549, 632 *with* J.A. at 114, 613. Mr. Peden explained that Cellebrite operator certifications, Cellebrite analyzer certifications, and mobile phone examiner certifications are "different certifications." J.A. at 613. Mr. Peden had all three certifications. J.A. at 114, 613.
[73] J.A. at 116-19, 629.
[74] J.A. at 620, 629.
[75] J.A. at 528.

aware he was supposed to look for specific dates, so he should have applied the filters that would have made it in compliance with those specific dates."[76]

H. After sorting the images, Mr. Smith began to scroll down. He saw contraband while scrolling through the largest of over two hundred thousand images from random dates.

After sorting over two hundred thousand images on the phone by size and irrespective of their date, Mr. Smith saw suspected child pornography, stopped searching, and notified CID.[77] He claimed that the image "was visible within my screen without even scrolling."[78] "[I]t was the tenth picture from the top."[79]

Mr. Peden—the only digital forensics expert witness in this case certified to use Cellebrite's monthly-updated software (and the only certified mobile phone examiner)—explained that the Cellebrite 'table view' function Mr. Smith used only shows eight images on a monitor at a time.[80] He explained that, because the contraband was the tenth-listed image, it would not have been visible on Mr. Smith's

[76] J.A. at 637.
[77] J.A. at 110, 563.
[78] J.A. at 562-63.
[79] J.A. at 562.
[80] J.A. at 638; *compare* J.A. at 392, 549-50, 632 *with* J.A. at 563-64. Mr. Peden also noted that the 'table view' function "is not the norm for reviewing images because it takes way too long. If you imagine, there is eight on a screen and there's 220,000-plus images on the device. To go through those manually in this view would take you forever. So that's what the gallery view is for." J.A. at 638.

monitor after Mr. Smith sorted the images by size.[81] The contraband "wouldn't have been visible without scrolling down."[82]

This was the second time that Mr. Smith scrolled through materials on this cell phone.[83] When Mr. Smith first looked at the 'device locations' folder (prior to looking at images and then sorting them by size) he searched for location data by "scrolling down to the date annotated in the CASS."[84] Mr. Smith did not include this first instance of scrolling in his search report or in his initial conversations with the trial counsel, although he later admitted to it.[85]

Regardless, Mr. Peden explained that the contraband "would have not ever been discovered at all had he [Mr. Smith] applied the correct filters."[86]

I. The military judge denied the Defense motion to suppress evidence.

The Defense filed a motion to suppress evidence derived from Mr. Smith's "impermissible and unconstitutional fishing expedition" that failed to look for material from December 23, 2018 and resulted "in a rummaging of the device."[87]

---

[81] J.A. at 637-38.
[82] J.A. at 638.
[83] *Compare* J.A. at 390 *with* J.A. at 562, 638.
[84] J.A. at 390.
[85] J.A. at 390.
[86] J.A. at 637.
[87] J.A. at 23, 47-48, 663.

The military judge denied the motion.[88] In his written findings, he found that Mr. Smith sorted the images by size "since he believed that user-taken photos might have location meta-data."[89] He wrote that Mr. Smith's "plan was to next sort the images by date" but that Mr. Smith saw the contraband "during the process of trying to sort the images by size and date."[90] He wrote that Mr. Smith conducted his search reasonably without exceeding the scope of his authorization and that there was "no evidence to suggest that Mr. Smith was rummaging through areas of the iPhone where the CASS did not authorize him to look."[91] Ultimately, the military judge believed that Mr. Smith "was in a location he was authorized to be" and that suppression would not deter DC3 because "Mr. Smith attempted to stay within the scope of the CASS."[92]

Although the military judge noted that Mr. Smith testified to viewing the contraband without scrolling through images, the military judge did not make any findings as to whether Mr. Smith actually did not scroll through the images.[93] Instead, he merely noted that "This image was the tenth image from the top, not

[88] J.A. at 695.
[89] J.A. at 691.
[90] J.A. at 691-92.
[91] J.A. at 679, 691-92.
[92] J.A. at 692, 694.
[93] J.A. at 691-92.

something like the 300th image out of 220,141 which suggests that this contraband image was in plain view."[94]

The military judge made no findings pertaining to Mr. Peden's testimony that, if the image was the tenth-listed image after sorting by size, it could only have been viewed by scrolling down.[95] In fact, his findings did not discuss Mr. Peden (the only digital forensics expert recognized by the military judge who was certified to conduct cell phone searches) at all.[96] And the military judge made no findings pertaining to Mr. Smith's lack of certifications.[97]

The military judge never explained why it was reasonable for Mr. Smith to look at the largest of over 200,000 images irrespective of their date, when the search authorization only allowed him to look for material from one particular date.

[94] J.A. at 692.
[95] *Compare* J.A. at 638 *with* J.A. at 691-94.
[96] J.A. at 673-95
[97] J.A. at 673-95.

Summary of Argument

Sorting and viewing the largest of over two hundred thousand images irrespective of their date, despite the extremely narrow date limitation in the search authorization, violated the Fourth Amendment. Denial of the suppression motion was outside the military judge's range of reasonable options because sorting the images did nothing to advance Mr. Smith's search and was nothing more than an unnecessary and wide-ranging exploratory search. The denial was also an abuse of discretion because it was based on three clearly erroneous factual findings.

Scrolling and continuing to view the largest of over two hundred thousand images (after sorting them by size irrespective of their date) also violated the Fourth Amendment. Denial of the suppression motion was thus also an abuse of discretion because the military judge's ruling was based on a clearly erroneous factual finding, he failed to make any findings pertaining to the scrolling, he was influenced by an erroneous view of the law, and—because the scrolling was so clearly unreasonable—denial of the motion was outside his range of reasonable options.

The plain view doctrine does not apply because Mr. Smith was not in a lawful position when he viewed the images.

Finally, the military judge abused his discretion by not applying the exclusionary rule. Mr. Smith wrote in all-caps that he was authorized to view "ALL DATA" on the phone, and he intentionally disregarded the limitations of the search

authorization. The exclusionary rule should not only apply because Mr. Smith intentionally flouted the parameters of the search authorization, but also because of his organization's systemic negligence. If the exclusionary rule is not applied, DC3 agents will continue disregarding extremely narrow search authorizations. Applying the exclusionary rule will preserve commanding officers' control of law enforcement, protect the particularity requirement of search authorizations, and preserve the Fourth Amendment.

The search authorization in this case could exist in any case, and Fourth Amendment violations as flagrant as the one here must be prohibited.

Argument

MR. SMITH VIOLATED APPELLANT'S FOURTH AMENDMENT RIGHTS WHEN HE SEARCHED AND VIEWED IMAGES ON APPELLANT'S PHONE AFTER (1) ARRANGING IMAGES IN ORDER OF SIZE, WITHOUT REGARD FOR THE DATE LIMITATION OF THE SEARCH AUTHORIZATION, AND (2) SCROLLING THROUGH ADDITIONAL IMAGES OUTSIDE THE SCOPE OF THE SEARCH AUTHORIZATION. THE MILITARY JUDGE ABUSED HIS DISCRETION IN DENYING THE DEFENSE MOTION TO SUPPRESS.

Standard of Review

A military judge's ruling on a motion to suppress evidence is reviewed for an abuse of discretion.[98]

Discussion

A military judge abuses their discretion when (1) their findings of fact are clearly erroneous; (2) their decision is influenced by an erroneous view of the law; (3) their decision is outside of their range of reasonable choices when facts are applied to law; or (4) they fail to consider important facts.[99]

[98] *United States v. White*, 80 M.J. 322, 327 (C.A.A.F. 2020).
[99] *White*, 80 M.J. at 327; *United States v. Commisso*, 76 M.J. 315, 321 (C.A.A.F. 2017) (internal citation omitted).

A. The Fourth Amendment protects the cell phone—an unparalleled database of personal and private information—from wide-ranging exploratory searches.

The Fourth Amendment protects "against unreasonable searches and seizures."[100] Protection against "the security of one's privacy against arbitrary intrusions . . . [is] at the core of the Fourth Amendment."[101] Although searches conducted pursuant to search authorizations are presumptively reasonable, search authorizations must be sufficiently particular to "prevent a general exploratory rummaging in a person's belongings."[102] The particularity requirement ensures that searches are "carefully tailored to [their] justifications, and [do] not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit."[103]

Searches conducted pursuant to an authorization remain subject to an "ex post reasonableness analysis."[104] This analysis assesses whether such searches struck the appropriate balance between being "expansive enough to allow investigators access to places where incriminating materials may be hidden, yet not so broad that they become the sort of free-for-all general searches the Fourth Amendment was designed

---

[100] U.S. Const. amend. IV.
[101] *Wolf v. Colorado*, 338 U.S. 25, 27 (1949).
[102] *United States v. Richards*, 76 M.J. 365, 369 (C.A.A.F. 2017) (internal quotations omitted).
[103] *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).
[104] *Richards*, 76 M.J. at 370.

to prevent."[105] This analysis involves determining whether the search is conducted "strictly within the bounds set by the warrant."[106] Searches are reviewed for reasonableness in the context of their specific circumstances.[107] Sufficient probability "is the touchstone of reasonableness under the Fourth Amendment."[108]

Rather than set *ex ante* limitations to digital searches, courts look at whether searches are "reasonably directed at uncovering evidence."[109] However, Fourth Amendment protections of cellular phones present "distinct" issues.[110] Reviewing courts must be cautious of allowing unfettered access to "the enormous amount of data that computers can store."[111]

According to the Supreme Court, "[m]odern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'"[112] "More than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of

---

[105] *Id*.
[106] *Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*, 403 U.S. 388, 394 n.7 (1971).
[107] *United States v. Christie*, 717 F.3d 1156, 1166 (10th Cir. 2013); *United States v. Hill*, 459 F.3d 966, 974-77 (9th Cir. 2006).
[108] *Garrison*, 480 U.S. at 87.
[109] *Richards*, 76 M.J. at 370; *United States v. Loera*, 923 F.3d 907, 916-17 (10th Cir. 2019).
[110] *Richards*, 76 M.J. at 369-70.
[111] *Loera*, 923 F.3d at 916-17.
[112] *Riley v. California*, 573 U.S. 373, 403 (2014).

their lives—from the mundane to the intimate."[113] In finding that the Fourth Amendment protects the reasonable expectation of privacy in cellular phones, the Supreme Court noted that "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions."[114]

B. Sorting and viewing images in order of size and irrespective of their date violated the Fourth Amendment.

1. Mr. Smith failed to employ a reasonable search method because he looked in the obscure before the obvious.

The Tenth Circuit in *United States v. Loera* understood the dangers surrounding the "needle-in-a-haystack problem" resulting from "unlimited electronic searches."[115] There, the court reviewed the execution of a warrant authorizing the search of CD-ROMs for evidence of fraud.[116] The court discussed how search methods constituting a "sweeping, comprehensive search of a computer's hard drive" were generally prohibited.[117] But because the warrant in *Loera* authorized all file types to be searched (unlike here, where the authorization only applied to one date), and any file could have contained evidence of fraud (unlike

[113] *Id*. at 395.
[114] *Id*. at 394.
[115] *Loera*, 923 F.3d at 916 (internal quotations omitted).
[116] *Loera*, 923 F.3d at 912; *see United States v. Loera*, 59 F. Supp. 3d 1089, 1099 (D.N.M. 2014).
[117] *Loera*, 923 F.3d at 917-18 (internal quotations omitted).

here, where the vast majority of images would not be from December 23, 2018), it was reasonable to search all files on CDs.[118] Critically, the court noted that, in cases where looking through all files was not necessary (such as here—where Mr. Smith could have used a date filter), agents must employ "[n]arrowly tailored search methods that begin looking in the most obvious places and then progressively move from the obvious to the obscure."[119]

Mr. Smith began at the wrong end of that spectrum—looking in the obscure before the obvious. Rummaging through the largest of over two hundred thousand images irrespective of their date was obviously not where he would find material from one date. The chances of doing so were not only obscure, speculative, and exceptionally unlikely—they were unreasonable. Mr. Smith ignored the clearly delineated and extremely narrow date limitation of the search authorization. Applying a date filter to the images—which he intended to do *after* "see[ing] if there were a significant amount of photos"—was the obvious first step he should have employed.[120] Deciding to only apply a date filter after looking at the largest images was unexplainable and patently unreasonable.

[118] *Id*. at 922.
[119] *Id.* at 920 (internal quotations omitted).
[120] J.A. at 586.

2. Sorting the images by size did nothing to advance Mr. Smith's search. Doing so violated SSgt Shields's Fourth Amendment rights.

Mr. Smith had no legitimate reason for sorting over two hundred thousand images by size and irrespective of their date. Doing so replaced the images on his screen that were outside the scope of the authorization with other images that were also outside its scope. It was thus unnecessary and avoidable.

Sorting the images by size did nothing to advance Mr. Smith's search. He explained that he intended to apply a date filter after looking at the largest of over two hundred thousand images, but he had no reasonable basis for looking at the largest-sized files. He could have applied a date filter without looking at them at all.

As the Supreme Court held in *Maryland v. Garrison*, "[P]robable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom."[121] Mr. Smith's search was the functional equivalent of law enforcement, looking for the lawnmower they know is in the garage, climbing up a ladder to the upstairs bedroom to make their way to the garage. It was unnecessarily circuitous and not narrowly tailored.

If sufficient probability "is the touchstone of reasonableness under the Fourth Amendment," then Mr. Smith violated the Fourth Amendment.[122] There was no realistic probability that material from one particular date would be found by looking

[121] *Garrison*, 480 U.S. at 81.
[122] *Id*. at 87 (citing *Hill v. California*, 401 U.S. 797, 803-04 (1971)).

at the largest of over two hundred thousand images irrespective of their date. The vast majority of files Mr. Smith began to look at would not have contained evidence from December 23, 2018. The unnecessary and extra steps he employed in his circuitous search was precisely the type of "wide-ranging exploratory searches the Framers intended to prohibit."[123] It thus exceeded the scope of the search authorization and violated SSgt Shields's Fourth Amendment rights.

3. The military judge based his denial of the motion on three clearly erroneous findings of fact:

i. "There is no evidence to suggest that Mr. Smith was rummaging through [unauthorized] areas of the iPhone[.]"[124]

Contrary to the military judge's finding, there was evidence suggesting that Mr. Smith rummaged through unauthorized areas of the cell phone. The search authorization itself is evidence—it had an extremely narrow date parameter that Mr. Smith disregarded and only adhered to *after* rummaging through the largest of over two hundred thousand images.

That Mr. Smith sorted the images by size prior to applying a date filter is also evidence of his rummaging. Doing so took him from looking at images not from December 23, 2018 to looking at other images that were also obviously from the wrong date. His unnecessary steps did nothing to advance his search.

---

[123] *Garrison*, 480 U.S. at 84.
[124] J.A. at 692.

Thus, the military judge's finding that there was no evidence of unauthorized rummaging was clearly erroneous.

ii. Mr. Smith's "plan was to next sort the images by date[.]" He saw the contraband "[d]uring the process of trying to sort the images by size and date."[125]

Mr. Smith was not in the process of sorting the images by date. He admitted as much when he testified that he would "eventually" apply a date filter, but he "wanted to look at them first, see if there were a significant amount of photos with GPS data, and start filtering from there."[126] Finding that Mr. Smith was "in the process" of applying a date filter is the equivalent of finding that someone is "in the process" of going home for the day when that person comes to work at 7:30 in the morning. One is not "in the process" of doing something until that person actually begins to do that thing. *Merriam-Webster* defines "in the process" (the idiom) as "while doing something."[127] Mr. Smith did not see the contraband while applying a date filter. He had not begun to apply a date filter and his next step (which he began by scrolling down) was to rummage through the largest images—not apply a date filter. Finding otherwise was clearly erroneous.

---

[125] J.A. at 691-92.
[126] J.A. at 573, 586.
[127] *In the process*, MERRIAM-WEBSTER (Nov. 28, 2022 10:05 AM), https://www.merriam-webster.com/dictionary/in%20the%20process.

iii. "Mr. Smith attempted to stay within the scope of the CASS."[128]

Mr. Smith understood that the search authorization in this case had an extremely narrow parameter: December 23, 2018. He admitted "[t]he intent, as I understand it, was to look for location or GPS data from a certain date."[129] But he did not look for GPS data from a certain date. He deliberately disregarded the date parameter of the search authorization and only planned to abide by that parameter *after* rummaging through the largest of over two hundred thousand images. He could not have more clearly articulated his intentional disregard for the limitations of the search authorization when he wrote (using all-caps), "My job is to analyze ALL DATA on the device."[130]

Thus, the military judge's finding that Mr. Smith attempted to stay within the scope of the search authorization was clearly erroneous.

4. For these reasons, the military judge abused his discretion.

Because sorting the images by size and irrespective of their date violated the Fourth Amendment, and because the military judge based his decision on three clearly erroneous findings of fact, the military judge's denial of the motion to suppress was an abuse of his discretion.

---

[128] J.A. at 694.
[129] J.A. at 553.
[130] J.A. at 113.

Even if this Court does not believe that these three findings of fact were clearly erroneous, the military judge's decision was nonetheless outside of his range of reasonable options. Mr. Smith's search was not narrowly tailored to adhere to the extremely narrow date limitation of the search authorization, sorting the images by size did nothing to advance his search, and his circuitous rummaging was purely exploratory. Mr. Smith's search undermined Fourth Amendment protections of what may be the most inherently private database held by individuals today: the cell phone. For these reasons, the military judge's only reasonable option was to find that the Fourth Amendment was violated.

C. Scrolling through the largest images irrespective of their date and viewing even more images outside the scope of the search authorization continued to violate the Fourth Amendment.

1. The military judge's factual finding that there was no evidence of unauthorized rummaging failed to consider that the contraband was the tenth-listed image.

The military judge's finding of fact that there was "no evidence" of unauthorized rummaging was (in addition to the reasons provided above) clearly erroneous because Mr. Peden provided clear evidence that Mr. Smith began to scroll through the images after sorting them by size. Mr. Smith admitted that the contraband was the tenth-listed image, and Mr. Peden explained that the Cellebrite 'table view' function Mr. Smith used only displayed eight images at a time. Thus,

the military judge was presented with evidence that Mr. Smith began to scroll through the images after sorting them by size.

Scrolling through the largest of over two hundred thousand images irrespective of their date is hardly a narrowly tailored or reasonable search method considering the search authorization's extremely narrow date limitation. Finding that there was no evidence of unauthorized rummaging was thus a clearly erroneous finding of fact for this additional reason.

2. The military judge failed to consider facts pertaining to Mr. Smith's scrolling. This was an abuse of discretion.

A military judge's failure to consider pertinent facts can constitute an abuse of discretion, and such is the case here.[131] Mr. Smith and Mr. Peden directly contradicted one another on the issue of whether Mr. Smith scrolled through the images after sorting by size. While Mr. Smith claimed he immediately stopped searching after sorting by size because the contraband immediately appeared on his screen as the tenth-listed image, Mr. Peden testified that the tenth-listed image could only have been viewed by scrolling down. As directly contradicting perspectives, both could not be correct.

While the military judge noted that Mr. Smith "testified that the image . . . was visible within his screen without even scrolling[,]" he did not make any findings

[131] *See United States v. Solomon*, 72 M.J. 176, 181 (C.A.A.F. 2013) (finding an abuse of discretion resulting from the military judge's failure to consider important facts).

as to whether Mr. Smith's testimony was accurate.[132] He failed to provide factual findings on this central issue.

Without resolving this issue, the military judge could not have possibly determined whether Mr. Smith violated the Fourth Amendment by scrolling through the largest of over two hundred thousand images irrespective of their date. That the military judge wholly disregarded the directly contradicting testimony from the only expert certified to operate Cellebrite or conduct cell phone searches was compounded by his failure to provide any findings pertaining to Mr. Peden's credibility. His findings did not discuss Mr. Peden at all let alone explain how Mr. Smith's lack of pertinent certifications should be weighed in comparison to Mr. Peden's directly contradicting and highly qualified testimony.

3. The military judge was influenced by an erroneous view of the law. It did not matter whether Mr. Smith scrolled through two additional images or three hundred images—neither constitute plain view.

Rather than make any findings pertaining to Mr. Smith's decision to scroll through the images, the military judge noted, "This image was the tenth image from the top, not something like the 300th image out of 220,141 which suggests that this contraband image was in plain view."[133]

[132] J.A. at 691.
[133] J.A. at 692.

For incriminating material to be in plain view, the investigator must not violate the Fourth Amendment in arriving at the spot from which the material was viewed.[134] Thus, what matters is whether Mr. Smith violated the Fourth Amendment by sorting and then scrolling—not by the amount of images he scrolled through. The military judge indicated that scrolling through three hundred images would constitute a violation of the Fourth Amendment. But if scrolling through three hundred images would have taken Mr. Smith out of plain view, then scrolling through two images (the two images beyond the eight initially displayed on Mr. Smith's monitor after he sorted them by size) must have also taken him out of plain view. The military judge's ruling on plain view should have been based on Mr. Smith's scrolling (and sorting images by size) rather than the amount of images beyond the number that would have initially appeared on his screen.

Thus, the military judge based his decision on an erroneous view of the law.

4. After affording the military judge less deference because he did not make any findings regarding the scrolling, it is clear that his decision was outside of his range of reasonable options.

This Court has held that, where a military judge fails to make essential findings, his decisions relating to those findings are afforded less deference.[135] Such is the case here.

---

[134] *Richards*, 76 M.J. at 371 (discussing *Horton v. California*, 496 U.S. 128 (1990)).
[135] *United States v. Flesher*, 73 M.J. 303, 312 (C.A.A.F. 2014).

Because the military judge did not make any findings pertaining to whether Mr. Smith began to scroll through the images after sorting them by size, this Court should not give more deference on the issue of scrolling to Mr. Smith's testimony than Mr. Peden's. Mr. Smith admitted that the contraband was the tenth-listed image, and Mr. Peden explained that Cellebrite's 'table view' function only displayed eight images at a time and therefore Mr. Smith must have scrolled down to view the tenth image. Mr. Peden was the only expert recognized by the military judge who was certified to operate Cellebrite software—Mr. Smith's certification of four years prior had expired despite the software's monthly updates. These facts are enough for this Court to find that, even if sorting by size was reasonable, subsequently scrolling through the images constituted an unreasonable violation of the Fourth Amendment.

Scrolling took Mr. Smith further beyond the limitations of his search authorization. The likelihood that the largest of over hundred thousand images were from December 23, 2018 was so patently obscure and unrealistic that it was unreasonable. It was precisely the type of "wide-ranging exploratory searches the Framers intended to prohibit."[136]

Thus, the military judge's denial of the motion was outside of his range of reasonable options.

[136] *Garrison*, 480 U.S. 79, 84 (1987).

5. For these additional reasons, the military judge abused his discretion.

The military judge thus made four critical errors pertaining to Mr. Smith scrolling through the images after sorting them by size. First, he made a clearly erroneous finding of fact. Second, he failed to make essential findings pertaining to the scrolling. Third, he based his ruling on an erroneous view of the law. Fourth, his decision was outside of his range of reasonable options. The military judge thus abused his discretion.

D. The contraband was not in plain view.

This Court in *United States v. Richards* was mindful of the need to curtail "general exploratory rummaging" when considering the "distinct issues" surrounding searches of electronic devices.[137] There, a search authorization limited the scope of a search of electronics seeking communications between 2010 and 2011.[138] Investigators searched two hard drives and a laptop, and found child pornography.[139] The hard drives were shut down years earlier—in 2006 and 2008.[140] This Court noted that "Assuming the shutdown dates [of the hard drives] were indicative of the timing of their last use, these materials were outside the scope of the search authorization."[141] However, the laptop was shut down in 2011—within

[137] *Richards*, 76 M.J. at 369-70 (internal quotations omitted).
[138] *Id*. at 368-71.
[139] *Id*. at 368.
[140] *Id*. at 371.
[141] *Id*.

the scope of the search authorization—and the communications could have existed anywhere on the laptop.[142] Thus, the search of the laptop reasonably fell within the scope of the authorization.[143] Because the search authorization allowed all file types to be searched, and any file could have contained the sought communications, it was reasonable to search all files on the laptop.[144] And because the agent was in a lawful spot when he viewed the contraband, he viewed it in plain view.[145]

In contrast, here, the search authorization did not authorize all file types to be searched and the vast majority of files would not have contained evidence from December 23, 2018. Unlike the authorization in *Richards*, the authorization here was extremely narrow—covering only one particular day rather than two years. The vast majority of files were not from December 23, 2018. As discussed, sorting the images by size did nothing to reasonably advance Mr. Smith's search, and neither did scrolling through the largest images. Mr. Smith departed the authorized boundaries of his search authorization. Because he was not in a lawful place when he viewed the contraband, he did not view the contraband in plain view.

Thus, applying the plain view doctrine was outside of the military judge's range of reasonable options and constituted an abuse of discretion.

---

[142] *Id*. at 370.
[143] *Id*. at 371.
[144] *Id*. at 370-71.
[145] *Id*. at 371.

E. Mr. Smith's deliberate disregard of the search authorization and the benefits of exclusion should have triggered the exclusionary rule.

Evidence obtained as result of an unlawful search may only be excluded from trial if exclusion results in appreciable deterrence of future unlawful searches and the benefits of such deterrence outweigh the costs to the justice system.[146] "[T]he exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence."[147]

Denial of the defense suppression motion was outside the military judge's range of reasonable options, and thus was an abuse of discretion, for at least five reasons:

1. Mr. Smith deliberately disregarded the limitations of the search authorization.

Mr. Smith could not have more clearly articulated his intentional disregard of the search authorization when he wrote, "My job is to analyze ALL DATA on the device."[148] He understood the date limitation of the search authorization, and he disregarded it. His unnecessary and circuitous search was conducted with the intent of only abiding by the date parameter *after* rummaging through the largest of over two hundred thousand images. This is the precise type of culpable, deliberate, and unlawful misconduct that the exclusionary rule is designed to curb.

---

[146] Mil. R. Evid. 311(a); *Herring v. United States*, 555 U.S. 135, 144 (2009).
[147] *Herring*, 555 U.S. at 144.
[148] J.A. at 113.

2. Exclusion would deter DC3's systemic negligence.

Mr. Smith's actions were the product of a systemic failure. He provided as much when he wrote that he did not violate any standard operating procedure at DC3 and that a top examiner at his organization was "very much in agreement that my thought process was reasonable."[149] Mr. Zaferiou, the experienced examiner at DC3, likewise provided that Mr. Smith appropriately followed DC3 procedures.

These facts show that any digital forensic examiner at DC3 would have deliberately taken the same actions as Mr. Smith and searched "ALL DATA."[150] Despite being specifically limited to material from December 23, 2018, DC3's organizational posture was that its examiners could search *entire* phones irrespective of date limitations in search authorizations.

The lower court agreed. It held that the "unwritten policy of defaulting to manual review of data files," despite the limitations of the search authorization, runs against "the dangers posed by allowing digital searches to devolve into the sort of 'wide-ranging exploratory searches the Framers intended to prohibit.'"[151]

Thus, the failure in this case is an organizational failure as well as an individual one. That Mr. Smith followed normal DC3 procedures and experienced investigators at DC3 supported his decision to ignore the authorization's parameters

[149] J.A. at 113.
[150] J.A. at 113.
[151] *Shields*, No. 202100061, 2022 CCA LEXIS at *15.

is troubling. If DC3 agreed that Mr. Smith was authorized to search "ALL DATA," then DC3 will continue to follow this logic in future cases.

Applying the exclusionary rule will thus correct this issue on a widespread scale—preventing numerous additional constitutional violations such as this one.

3. Exclusion would preserve control of law enforcement for commanding officers.

The Commanding Officer could not have been clearer that he intended his search authorization to prohibit the precise search Mr. Smith conducted. He testified that he limited CID's ability to only search for materials from one date in order to prevent a "free for all on the phone."[152] And the text of the authorization clearly conveyed as much—as is demonstrated by Mr. Smith's acknowledgment prior to his search that he was only supposed to seek material from one date. Yet Mr. Smith disregarded the date parameter of the authorization—only intending to abide by it *after* rummaging through the largest of thousands of images.

Applying the exclusionary rule will thus preserve commanding officers' authority by ensuring they are able to control their own investigations.

4. Exclusion would protect the particularity requirement.

The particularity requirement is supposed to ensure that searches are "carefully tailored to [their] justifications, and [do] not take on the character of the

[152] J.A. at 506.

wide-ranging exploratory searches the Framers intended to prohibit."[153] But here, despite that the search authorization was particular and extremely narrow, Mr. Smith's search was not carefully tailored to its justifications. Allowing the narrow parameters of a search authorization to be disregarded as such undermined the particularity requirement as it applies to digital searches.

Thus, applying the exclusionary rule will ensure particularly narrow search authorizations—such as the extremely narrow one in this case—are adhered to.

5. Exclusion would preserve Fourth Amendment protections in cell phones—one of the most inherently private databases in the modern world.

Mr. Smith searched what may be the most private type of materials on a cell phone—photographs. Location data is relevant in the prosecution of any crime, and just about every Sailor and Marine owns a cell phone. If the scope of this CASS allows the Government to look through "ALL DATA," then the Government could conduct unfettered inspections of cell phones in any case. Fourth Amendment protections of cell phones would lose all meaning.

Applying the exclusionary rule would thus protect Fourth Amendment protections of the most personal and private database that individuals hold today.[154]

---

[153] *Garrison*, 480 U.S. at 84.
[154] *See Riley*, 573 U.S. at 395-403.

Conclusion

Mr. Smith knew better. His admission that he "wanted to look at them first" before applying a date filter indicates as much.[155] He flouted clearly defined search parameters and rummaged through the largest of over two hundred thousand images without legitimate purpose. And his organization's unwritten policy sanctioning his decision is indeed "concerning."[156]

DC3's support of Mr. Smith casts a dark shadow upon the future of criminal investigations in the digital era. This law enforcement organization has effectively excised commanding officers' control of their own investigations. They stand by their agents ignoring the particularity requirement despite using a tool "designed to protect the right and the privacy of individuals . . . to be able to comply with [search authorization limitations] and to provide what the Court ordered them to do."[157]

If such an obvious violation of a search authorization goes without penalty, what will happen in less clear cases? Granting relief will set digital forensic searches in the armed forces on a clear course. It will ensure that investigators comply with search authorization parameters. And it will protect the key to the "privacies of life . . . [the] digital record of nearly every aspect of [Sailors' and Marines'] lives."[158]

---

[155] J.A. at 586.
[156] J.A. at 113; *Shields*, No. 202100061, 2022 CCA LEXIS at *12.
[157] J.A. at 616-17.
[158] *Riley*, 573 U.S. at 395-403.

Relief Requested

This Court should dismiss the conditionally pleaded charges.[159]

Respectfully submitted.

Aiden J. Stark
LT, JAGC, USN
Appellate Defense Counsel
Navy-Marine Corps Appellate Review Activity
1254 Charles Morris Street, SE
Building 58, Suite 100
Washington, DC 20374
(202) 685 - 7292
aiden.j.stark2.mil@us.navy.mil
CAAF Bar No. 37598

[159] Appellant conditionally pleaded guilty to Charge I, Charge II, Charge IV, and Additional Charge I in order to preserve appellate review of the military judge's abuse of discretion in ruling that the search of his phone did not violate his Fourth Amendment rights. J.A. at 698-701, 707-08. Should this Court find that such error occurred, Appellant withdraws his pleas to the conditionally entered charges. Accordingly, this Court should dismiss the findings of the conditionally pleaded charges: Charge I, Charge II, Charge IV, and Additional Charge I.

Certificate of Filing and Service

I certify that the original and seven copies of the foregoing were delivered to the Court on December 21, 2022, that a copy was securely transmitted to Deputy Director, Appellate Government Division, and that a copy was securely transmitted to Director, Administrative Support Division, Navy-Marine Corps Appellate Review Activity, on December 21, 2022.

Aiden J. Stark
LT, JAGC, USN
Appellate Defense Counsel
Navy-Marine Corps Appellate Review Activity
1254 Charles Morris Street, SE
Building 58, Suite 100
Washington, DC 20374
(202) 685 - 7292
aiden.j.stark2.mil@us.navy.mil
CAAF Bar No. 37598

Certificate of Compliance with Rule 24(d)

This Supplement complies with the type-volume limitations of Rule 24(c) because it does not exceed 14,000 words, and complies with the typeface and style requirements of Rule 37. The brief contains 8,571 words. Undersigned counsel used Times New Roman, 14-point type with one-inch margins on all four sides.

Aiden J. Stark
LT, JAGC, USN
Appellate Defense Counsel
Navy-Marine Corps Appellate Review Activity
1254 Charles Morris Street, SE
Building 58, Suite 100
Washington, DC 20374
(202) 685 - 7292
aiden.j.stark2.mil@us.navy.mil
CAAF Bar No. 37598