No. _____

IN THE

Supreme Court of the United States

ETHAN R. SHIELDS,
Petitioner,

v.

UNITED STATES,
Respondent.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Armed Forces

PETITION FOR A WRIT OF CERTIORARI

REBECCA S. SNYDER
Counsel of Record
Navy-Marine Corps Appellate Review Activity
1254 Charles Morris St., SE
Building 58, Suite 100
Washington, DC 20374
(202) 685 – 7094
rebecca.s.page5.civ@us.navy.mil

AIDEN J. STARK
Lead Counsel for Petitioner
Navy-Marine Corps Appellate Review Activity
1254 Charles Morris St., SE
Building 58, Suite 100
Washington, DC 20374
(202) 685 – 7292
aiden.j.stark2.mil@us.navy.mil

Counsel for Petitioner

July 12, 2023

QUESTIONS PRESENTED

1. Whether this Court should endorse the Tenth Circuit framework for assessing the reasonableness of digital forensic searches under the Fourth Amendment.

2. Whether Petitioner's rights under the Fourth Amendment were violated, and the military judge abused his discretion, where a digital forensic examiner was authorized to only search for materials from one particular date but instead searched through images irrespective of their date.

PARTIES TO THE PROCEEDING

All parties appear in the caption of the case on the cover page.

RELATED PROCEEDINGS

Court of Appeals for the Armed Forces

United States v. Shields, No. 202100061, 2022 CCA LEXIS 448 (N-M. Ct. Crim. App. July 27, 2022).

Navy-Marine Court of Criminal Appeals

United States v. Shields, No. 22-0279, 2023 CAAF LEXIS 270 (C.A.A.F. Apr. 28, 2023).

TABLE OF CONTENTS

Page

TABLE OF CONTENTS[1]

(continued)

Page

[1] All pages in this Petition and its appendices comply with this Court's formatting requirements. *See* Supreme Court Rules, Rule 33.1. Although the appendices have been re-formatted to comply with this Court's rules, their substance have not been altered.

TABLE OF AUTHORITIES

Cases

PETITION FOR WRIT OF CERTIORARI

Petitioner, Staff Sergeant Ethan Shields, United States Marine Corps, respectfully petitions for a writ of certiorari to review the decision of the United States Court of Appeals for the Armed Forces.

INTRODUCTION

"Modern 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.'"[2] "More than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate."[3] "The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions."[4]

The Fourth Amendment protects "the security of one's privacy against arbitrary intrusion."[5] This protection is "at the core of the Fourth Amendment."[6] The Founding Fathers, in drafting the Fourth Amendment, could not have fathomed its complexities in this digital age. Information is more ubiquitous than ever, and the dangers of unnecessarily leaking private information are greater than ever. Without adequate protections, cell phone searches by law

---

[2] *Riley v. California*, 573 U.S. 373, 403 (2014).

[3] *Id.* at 395.

[4] *Id.* at 394.

[5] *Wolf v. Colorado*, 338 U.S. 25, 27 (1949).

[6] *Id.*

enforcement will undoubtedly result in viewing far greater amounts of private information than searching physical spaces.

This case presents an opportunity to protect people's intimate digital information from unlawful Government intrusion. The Tenth Circuit created an analytical framework that applies Fourth Amendment caselaw precedent to the unique and ever-evolving digital realm. Both the Government and the Petitioner agree that the Tenth Circuit's framework should apply in reviewing whether digital forensic searches are conducted legally within the scope of search warrants. But the Court of Appeals for the Armed Forces declined to endorse this helpful, guiding, and necessary application of law. Without the proper lens to review digital searches, in this age when the overwhelming majority of people carry troves of information in their pockets, courts will not have the proper guidance to ensure that privacy in our most inherently private spaces remain protected.

OPINIONS BELOW

The Court of Appeals for the Armed Forces' published opinion appears at pages 1a through 16a of the appendix to this petition. It is reported at 2023 CAAF LEXIS 270. The unpublished opinion of the United States Navy-Marine Corps Court of Criminal Appeals appears at 17a through 30a of the appendix. It is reported at 2022 CCA LEXIS 448.

JURISDICTION

The Court of Appeals for the Armed Forces entered judgment on April 28, 2023. The jurisdiction of this Court is invoked under 28 U.S.C. § 1259(3).

CONSTITUTIONAL PROVISIONS INVOLVED

The Fourth Amendment to the United States Constitution protects "against unreasonable searches and seizures."[7]

STATEMENT OF THE CASE

Nine Marine Corps recruits reported that on December 23, 2018, a man in a vehicle exposed his genitals onboard Marine Corps Recruit Depot ("MCRD") Parris Island.[8] A vehicle matching the recruits' description and registered to Petitioner departed MCRD Parris Island twice that day.[9] Petitioner's Commanding Officer signed a search authorization (the military equivalent of a search warrant) authorizing the search of Petitioner's cellular phone for location data generated on December 23, 2018.[10]

The phone was forwarded to an examiner at the Defense Cyber Crime Center ("DC3") to be searched pursuant to the search authorization.[11] The examiner read the authorization before beginning his search and understood that his search was to be limited by the search authorization's narrow December 23, 2018 parameter.[12]

---

[7] U.S. CONST. amend. IV.

[8] Pet. App. at 24a.

[9] Pet. App. at 24a.

[10] Pet. App. at 25a.

[11] Pet. App. at 25a.

[12] Pet. App. at 3a.

The examiner used the Cellebrite Physical Analyzer software to organize data extracted from the cell phone into readable data so he could begin his search.[13] The software allowed him to search the contents of the phone and organize them into categories such as "device locations," "SMS messages," "texts," and "images."[14] Using the software, he first searched the "device location" category, but the phone did not contain any location data from December 23, 2018.[15] He then looked for location data in other places to see if it had been improperly categorized.[16]

The examiner opened the "images" category in his analyzer because location coordinates are often embedded in photographs.[17] The "images" category contained more than two hundred thousand thumbnail images—some of which displayed on his monitor.[18] The examiner re-organized the thumbnail images into a "table view" that displayed each file in its own row with corresponding columns such as file name, size, and date created.[19] In this view, he had

---

[13] Pet. App. at 3a.

[14] Pet. App. at 25a.

[15] Pet. App. at 25a.

[16] Pet. App. at 25a-26a.

[17] Pet. App. at 26a.

[18] Pet. App. at 26a.

[19] Pet. App. at 26a.

the ability to sort the images by column, and he could filter them by date.[20]

The examiner did not filter the images by date. Instead, he *sorted* the images *by descending file size* to view the largest files of over two hundred thousand images irrespective of their date.[21] 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 [only then] start filtering from there."[22] Another examiner at DC3 later claimed that the examiner who conducted the search in this case did so reasonably and according to normal DC3 procedures.[23]

The examiner could have applied a date filter before sorting the images by size and looking at the largest of over two hundred thousand images irrespective of their date.[24] He explained that "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."[25] On appeal, the Navy-Marine Court of Criminal Appeals wrote "we find the DC3 examiner's search methodology concerning[.]"[26] It reasoned that "since his intention was to 'set a filter

---

[20] Pet. App. at 26a.

[21] Pet. App. at 26a.

[22] Pet. App. at 45a-46a (emphasis added).

[23] Pet. App. at 47a-57a.

[24] Pet. App. at 4a.

[25] Pet. App. at 26a.

[26] Pet. App. at 35a.

to only show photos with metadata that contains location data,' that would seem to obviate the need to sort by file size at all[.]"[27] The court found "it difficult to follow the examiner's logic in sorting the data in this manner[.]"[28]

Considering how the search in this case was conducted according to normal DC3 procedures, the Navy-Marine Court of Criminal Appeals 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[.]"[29] The court held this while keeping in mind "the dangers posed by allowing digital searches to devolve into the sort of 'wide-ranging exploratory searches the Framers intended to prohibit.'"[30]

After sorting over two hundred thousand images on the phone by size and irrespective of their date, the examiner stumbled upon suspected child pornography and stopped searching.[31] The examiner only stumbled upon this material because he had sorted over two hundred thousand images by their file size rather than filtered them to only look for those from the particular date he was supposed to look for.[32]

---

[27] Pet. App. at 36a.

[28] Pet. App. at 35a.

[29] Pet. App. at 37a.

[30] Pet. App. at 37a.

[31] Pet. App. at 26a-27a.

[32] Pet. App. at 26a.

At trial, the Defense filed a motion to suppress evidence derived from the examiner's search of the phone.[33] But the military judge denied the motion.[34] He found that the examiner sorted the images by size "since he believed that user-taken photos might have location meta-data."[35] Ultimately, the military judge found that the examiner did not exceed the scope of his search authorization.[36]

On appeal, both the Government and Petitioner argued that military courts should endorse the Tenth Circuit's caselaw analyzing digital forensic searches under the Fourth Amendment. The Navy-Marine Court of Criminal Appeals adopted that caselaw; however, the Court of Appeals for the Armed Forces, on review of the lower appellate court's decision, did not.[37]

REASONS FOR GRANTING THE PETITION

I. THIS COURT SHOULD ENDORSE THE TENTH CIRCUIT'S FRAMEWORK FOR APPLYING THE FOURTH AMENDMENT TO SEARCHES IN THE DIGITAL AGE.

A. The Tenth Circuit's Framework

"[T]he manner in which a warrant is executed is subject to later judicial review as to its

---

[33] Pet. App. at 27a.

[34] Pet. App. at 27a.

[35] Pet. App. at 27a.

[36] Pet. App. at 27a.

[37] Pet. App. at 1a-21a, 30a.

reasonableness."[38] Such analyses must be conducted on a case-by-case basis.[39] Generally, investigators executing a search authorization (which operates as a search warrant) can look anywhere that the evidence described in the warrant may conceivably be found.[40] "This limitation works well in the physical-search context to ensure that searches pursuant to warrants remain narrowly tailored, but it is less effective in the electronic-search context where searches confront what one commentator has called the 'needle-in-a-haystack' problem."[41]

To deal with this problem, the Tenth Circuit developed an analysis that allows reviewing courts to determine reasonableness in the highly evolved digital context. The Tenth Circuit "focused on 'how' the agents carried out the search, that is, the reasonableness of the search method the government employed."[42] This analysis constituted "a shift away from [the traditional Fourth Amendment analysis of] considering what digital location was searched and toward considering whether the forensic steps of the

---

[38] *Dalia v. United States*, 441 U.S. 238, 258 (1979).

[39] *Id.*

[40] *United States v. Ross*, 456 U.S. 798, 824 (1982).

[41] *United States v. Loera*, 923 F.3d 907, 916 (10th Cir. 2019) (quoting Orin S. Kerr, Digital Evidence and the New Criminal Procedure, 105 Colum. L. Rev. 279, 301 (2005)).

[42] *Loera*, 923 F.3d at 917 (citing *United States v. Burgess*, 576 F.3d 1078 (10th Cir. 2009); *United States v. Walser*, 275 F.3d 981 (10th Cir. 2001); *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999)).

search process were reasonably directed at uncovering the evidence specified in the search warrant."[43] Effectively, the reasonableness of an agent's search of digital materials "depends on the particular facts of a given case."[44]

The analysis is as follows: "Narrowly tailored search methods that begin looking 'in the most obvious places and [then] progressively move from the obvious to the obscure,' should be used where possible but are not necessary in every case."[45] In some cases, 'there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders.'"[46] "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."[47]

This analytical framework is not new—reasonableness was already the standard courts applied when reviewing the execution of search warrants.[48] Rather, the Tenth Circuit's analytical framework applied the pre-existing concept of determining reasonableness to the digital sphere. It

---

[43] *Loera*, 923 F.3d at 917.

[44] *Id.* at 920.

[45] *Id* at 920 (quoting *Burgess*, 576 F.3d at 1094).

[46] *Burgess*, 576 F.3d at 1094.

[47] *Loera*, 923 F.3d at 920.

[48] *Dalia*, 441 U.S. at 258.

did so in a manner that does not conflict with any federal court.[49]

B. By failing to apply this framework, the Court of Appeals for the Armed Forces left military courts in the dark.

On appeal, both the Government and the Petitioner agreed that the Tenth Circuit's analytical framework should be applied in the military jurisdiction. And in reviewing the digital search in this case, the Navy-Marine Court of Criminal Appeals likewise agreed, explicitly holding that examiners must "take great care to not only fully document their search methods, but also narrowly tailor them to 'begin looking in the most obvious places and [then] progressively move from the obvious to the obscure.'"[50] But the Court of Appeals for the Armed Forces, on review of the Navy-Marine Court of Criminal Appeals decision, did not apply this rule of law.

The Court of Appeals for the Armed Forces cited the Tenth Circuit to note that reasonableness evolves as a search progresses and an examiner learns

---

[49] *Loera*, 923 F.3d at 920 (noting that the Tenth Circuit decision brought it "in line with every circuit that has confronted this issue") (citing *United States v. Stabile*, 633 F.3d 219, 240 (3d Cir. 2011); *United States v. Williams*, 592 F.3d 511, 521-24 (4th Cir. 2010); *United States v. Miranda*, 325 F.App'x 858, 859-60 (11th Cir. 2009) (per curiam) (unpublished); *United States v. Wong*, 334 F.3d 831, 834 (9th Cir. 2003)).

[50] Pet. App. at 30a (quoting Loera, 923 F.3d at 920; Burgess, 576 F.3d at 1094).

more about the files on the device.[51] And cited its own prior holdings, which incorporated quotations from the Tenth Circuit providing that the Fourth Amendment is designed to prevent "general exploratory rummaging" and that a search warrant should not impose mechanical limits that would unduly restrict search objectives.[52] But the Court of Appeals for the Armed Forces did not incorporate the Tenth Circuit's critical explanation that assessing reasonableness in digital searches requires looking to whether narrowly tailored search methods beginning in the obvious places and moving to the obscure were possible, and whether they were employed.[53]

Without this critical framework, military courts reviewing digital searches are not provided the legal context of how reasonableness should be assessed in unique technological spheres. The Court of Appeals for the Armed Forces thus declined to confront "the 'needle-in-a-haystack' problem."[54]

Progress in this digital age requires increasing vigilance from law enforcement. The importance of endorsing the Tenth Circuit's obvious-to-obscure when possible method of assessing reasonableness cannot be understated. In this digital age, the Fourth Amendment protects an unprecedented sphere of

---

[51] Pet. App. at 13a-14a.

[52] Pet. App. at 10a, 16a.

[53] *Loera*, 923 F.3d at 920.

[54] *Id*. at 916 (10th Cir. 2019) (quoting Orin S. Kerr, Digital Evidence and the New Criminal Procedure, 105 Colum. L. Rev. 279, 301 (2005)).

privacy, what this Court has referred to as "[t]he sum of an individual's private life"—the cellular phone.[55] The Court of Appeals for the Armed Forces' failure to endorse this language, or even provide particularized guidance as to how to assess reasonableness in the unique digital sphere, leaves military courts in the dark as the digital world rapidly develops. Servicemembers who put their lives on the line do not have meaningful constitutional protections in their most private spaces—their phones.

II. THE TENTH CIRCUIT'S FRAMEWORK SHOWS THAT PETITIONER'S FOURTH AMENDMENT RIGHTS WERE VIOLATED. THE EXAMINER DISREGARDED OBVIOUS MEANS OF SEARCHING AND INSTEAD UTILIZED AN OBSCURE SEARCH METHOD TO RUMMAGE THROUGH INHERENTLY PRIVATE DIGITAL SPACES.

Applying the Tenth Circuit's method of assessing reasonableness shows that the agent in this case could have, but did not, employ "[n]arrowly tailored search methods that begin looking in the most obvious places and then progressively move from the obvious to the obscure."[56] Rather, the examiner began at the wrong end of that spectrum—looking in the obscure before the obvious.

The extremely narrow search authorization in this case should have limited the examiner's search to only seek material from one date: December 23, 2018. Rummaging through the largest of over two hundred

---

[55] *Riley*, 573 U.S. at 394.

[56] *Loera*, 923 F.3d at 920.

thousand images irrespective of their date was not where he would most obviously find material from one particular date. The chances of doing so were not only obscure, speculative, and exceptionally unlikely—they were unreasonable. The examiner ignored the search authorization's clearly delineated and extremely narrow date limitation. 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.[57] Deciding to only apply a date filter after looking at the largest images was unexplainable and patently unreasonable.

The examiner's actions were also the product of a systemic failure. He searched the phone according to his organization's normal procedure. His organization's posture was thus that its examiners could search *entire* phones irrespective of extremely narrow date limitations in search authorizations. The Navy-Marine Court of Criminal Appeals found that his search was the product of an "unwritten policy of defaulting to manual review of data files[.]"[58] Essentially, this law enforcement organization has a policy of ignoring the Fourth Amendment.

No legitimate reason supported the examiner's search or his organization's systemic practice. The examiner replaced the images on his screen that were outside the scope of his search authorization with other images that were also outside of its scope. Doing so did nothing to advance his search. He explained

---

[57] Pet. App. at 45a.

[58] Pet. App. at 37a.

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 files. He could have applied a date filter without looking at them at all.

As this 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."[59] The examiner's search was the functional equivalent of law enforcement, looking for the lawnmower they know is in the garage, climbing up a staircase 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 the examiner violated the Fourth Amendment.[60] There was no realistic probability that material from one particular date would be found by looking at the largest of over two hundred thousand images irrespective of their date. The vast majority of files the examiner began to look at would not have contained evidence from December 23, 2018. His unnecessary and circuitous steps were precisely the type of "wide-ranging exploratory searches the Framers intended to prohibit."[61]

The Tenth Circuit's obvious-to-obscure analysis makes the unreasonableness of this search clear. The

---

[59] *Garrison*, 480 U.S. at 81.

[60] *Id.* at 87 (citing *Hill v. California*, 401 U.S. 797, 803-04 (1971)).

[61] *Garrison*, 480 U.S. at 84.

examiner only had to search for material from one particular date, he had an obvious means of doing so (applying a date filter), but instead he looked in the most obscure places (by rummaging through the largest of over two hundred thousand images). His search was not narrowly tailored, and went to the obscure before the obvious.

Law enforcement agents across the nation conduct digital searches on a daily basis. Reviewing courts must be provided clear guidance on the proper lens to review the execution of digital warrants and search authorizations. This case presents the unique opportunity to do so. The Tenth Circuit's analytical framework not only adheres to and explains precedent, but actually clarifies the Fourth Amendment in the unique digital realm. This Court should grant review to ensure that reviewing courts have the tools to properly assess reasonableness in digital searches.

CONCLUSION

For the foregoing reasons, this Court should grant the petition for a writ of certiorari.

Respectfully submitted,

AIDEN J. STARK
Navy-Marine Corps Appellate
Review Activity
1254 Charles Morris St., SE
Building 58, Suite 100
Washington, DC 20374
(202) 685 – 7292
aiden.j.stark2.mil@us.navy.mil

REBECCA S. SNYDER
Counsel of Record
Navy-Marine Corps Appellate
Review Activity
1254 Charles Morris St., SE
Building 58, Suite 100
Washington, DC 20374
(202) 685 – 7094
rebecca.s.page5.civ@us.navy.mil

Counsel for Petitioner

July 12, 2022

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 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

[1] 10 U.S.C. § 839(a) (2018).

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

---

[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

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

---

(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))).

sufficient evidence in the record to support the military judge's findings in this case. And upon reviewing the 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 *why* he 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 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

---

[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.

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.

This opinion is subject to administrative correction before final disposition.

United States Navy–Marine Corps Court of Criminal Appeals

Before

GASTON, HOUTZ, and MYERS

Appellate Military Judges

UNITED STATES

Appellee

v.

Ethan R. SHIELDS

Staff Sergeant (E-6), U.S. Marine Corps

Appellant

No. 202100061

Argued: 21 June 2022 – Decided: 27 July 2022

Appeal from the United States Navy-Marine Corps Trial Judiciary

Military Judges:

Derek D. Butler (arraignment)

Eric A. Catto (motions and trial)

Sentence adjudged 30 October 2020 by a general court-martial convened at Marine Corps Recruit Depot Parris Island, South Carolina, consisting of a military judge sitting alone. Sentence in the Entry of Judgment: reduction to paygrade E-1, total forfeitures, confinement for 52 months, and a dishonorable discharge.

For Appellant:

Lieutenant Aiden J. Stark, JAGC, USN (argued)

Lieutenant Commander Daniel O. Moore, JAGC, USN (on brief)

For Appellee:

Captain Tyler W. Blair, USMC (argued)

Major Clayton L. Wiggins, USMC (on brief)

This opinion does not serve as binding precedent, but may be cited as persuasive authority under NMCCA Rule of Appellate Procedure 30.2.

PER CURIAM:

Appellant was convicted, pursuant to his pleas, of attempted indecent visual recording, wrongful possession and use of a controlled substance, indecent exposure, indecent visual recording, and possessing, viewing, and producing child pornography in violation of Articles 80, 112a, 120c, and 134, Uniform Code of Military Justice [UCMJ].[1] Appellant asserts two assignments of error: (1) the forensic search of Appellant's cellphone constituted an unlawful general search in violation of the Fourth Amendment; and (2) the military judge abused his discretion when he denied Appellant's motion for recusal for bias given his relationship to trial counsel and a victim in the case. We find no prejudicial error and affirm.

I. BACKGROUND

On 23 December 2018, nine Marine recruits reported to their chain of command that the driver of a car had exposed his genitals to them while they were walking aboard Marine Corps Recruit Depot Parris Island [MCRD]. Two of the recruits identified the make and model of the car, and investigators were able to identify a matching vehicle registered to Appellant that was driven onto MCRD twice that day. Appellant was subsequently identified in a photo lineup. When interviewed by Criminal Investigation Division [CID] agents, he denied committing the alleged offense but admitted being in the vicinity around the same time. CID reviewed video camera footage recorded on base which established that

---

[1] 10 U.S.C. §§ 880, 912a, 920c, 934.

Appellant had a cellphone in his possession around the time of the incident. Based on the investigation, Appellant's commanding officer authorized the seizure of Appellant's cellphone and authorized law enforcement to search it for "all location data stored on the phone or within any application within the phone for 23 Dec[ember] [20]18."[2]

After being presented with the search authorization, Appellant provided the phone and its passcode to CID, which then sent the phone to the Defense Cyber Crime Center [DC3] to be searched pursuant to the authorization. DC3 extracted all data from Appellant's phone and provided the extraction file to a digital forensic examiner to conduct the search. The examiner reviewed the search authorization and used the "Cellebrite" physical analyzer program to organize the phone's data into a readable format. This method separates the data into categories, or "parsed data," such as "device locations," "SMS messages," "texts," "images," and "internet history."[3]

The examiner first searched the "device locations" category, which yielded no relevant location data for the date in question. He next began "making a plan to start looking at the data that was not parsed properly or at all by [the] physical analyzer and . . . start looking at apps . . . likely to contain location data."[4] As he knew based on his training and

---

[2] App. Ex. XXVI at 55.

[3] R. at 237–39; App. Ex. XXV at 87.

[4] *Id*. at 240.

experience that photos commonly contain embedded global positioning system [GPS] data, he went to the "images" category in the physical analyzer. When he opened this category, the default review setting placed the over 200,000 images stored on Appellant's phone into "row after row after row of little thumbnail views of the individual pictures."[5] The examiner then reorganized the images into a "table view," which placed each thumbnail image in its own row next to columns of related data—such as filename, file size, and date created—that could be further sorted and filtered.[6]

The examiner then sorted the images by descending file size, so that he could "view the largest photos first, as they would likely be photos taken by the device," which could contain location data.[7] He testified that "once I got it into these columns and sorted largest to smallest I was going to begin filtering. My thought process[] 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."[8] His intent was to sort "for all photos that contain GPS [location data] and then . . . filter that with a date."[9] However, "before [he] could set a filter to only show photos with metadata that contains location data," he saw a thumbnail image of suspected

---

[5] *Id.*

[6] App. Ex. XXVI at 97.

[7] App. Ex. XXVI at 97; R. at 243.

[8] R. at 243.

[9] *Id.*

child pornography.[10] He then stopped the search, and law enforcement requested additional authorization to search Appellant's phone for child pornography. After the additional search authorization was obtained, the examiner resumed searching Appellant's phone and other electronic devices and uncovered evidence of additional misconduct, including child pornography and indecent recordings.

At trial, Appellant moved to suppress the evidence for violation of his Fourth Amendment rights during the search of his cellphone. Upon retracing the DC3 examiner's search methodology, Appellant's digital forensics expert testified that if the examiner had first filtered the 200,000+ images for only those containing location data, as opposed to sorting them by file size, the examiner would not have seen the thumbnail image of suspected contraband. The military judge denied Appellant's suppression motion, finding the examiner's search of the phone was "conducted in a reasonable manner and did not exceed the scope of the [search authorization]" and that the suspected contraband was discovered in plain view during the search for location data.[11]

Appellant subsequently entered into a plea agreement with the convening authority that conditioned his guilty pleas on his right to appeal the military judge's suppression ruling.

---

[10] App. Ex. XXVI at 97.

[11] App. Ex. LIII at 22.

II. DISCUSSION

A. "Reasonableness" of the Cellphone Search

We review a military judge's ruling on a motion to suppress evidence for abuse of discretion and consider the evidence in the light most favorable to the party that prevailed on the motion.[12] A military judge abuses his discretion if the findings of fact upon which he predicates his ruling are not supported by the evidence in the record, if he uses incorrect legal principles, or if he applies the legal principles to the facts in a way that is clearly unreasonable.[13] To constitute as an abuse of discretion, the decision must be "arbitrary, fanciful, clearly unreasonable or clearly erroneous."[14]

The Fourth Amendment provides,

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

---

[12] *United States v. Blackburn*, 80 M.J. 205, 210-11 (C.A.A.F. 2020).

[13] *United States v. Ellis*, 68 M.J. 341, 344 (C.A.A.F. 2010).

[14] *United States v. Sullivan*, 74 M.J. 448, 453 (C.A.A.F. 2015) (citation omitted).

persons or things to be seized.[15]

A search conducted pursuant to a warrant or search authorization is presumptively reasonable.[16] However, search authorizations must "describe the things to be seized with sufficient particularity to prevent a general exploratory rummaging in a person's belongings."[17] As the Supreme Court has explained, "[b]y limiting the authorization to search to the specific areas and things for which there is probable cause to search, the [particularity] requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit."[18]

Data stored within a cell phone falls within the Fourth Amendment's protections.[19] However, such devices present "distinct issues," and "[t]he prohibition of general searches is not to be confused with a demand for precise ex ante knowledge of the location and content of evidence."[20] Given "the dangers of too narrowly limiting where investigators

---

[15] U.S. Const. amend. IV.

[16] *See United States v. Wicks*, 73 M.J. 93, 99 (C.A.A.F. 2014) (citing *Katz v. United States*, 389 U.S. 347, 357 (1967)).

[17] *United States v. Richards*, 76 M.J. 365, 369 (C.A.A.F. 2017) (quoting *United States v. Carey*, 172 F.3d 1268, 1272 (10th Cir. 1999)).

[18] *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

[19] *Riley v. California*, 573 U.S. 373, 386 (2014).

[20] *Richards*, 76 M.J. at 369-70 (citation omitted).

can go," such searches may be properly limited "to evidence of specific federal crimes or specific types of material" without necessarily "requir[ing] particular search methods and protocols."[21] An authorization to search cell phone data meets constitutional particularity requirements when the areas to be searched are "clearly related to the information constituting probable cause."[22]

Nevertheless, such searches remain subject to an "ex post reasonableness analysis" to assess whether they have 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 to prevent."[23] One aspect of this analysis examines whether the person conducting the search does so "strictly within the bounds set by the warrant."[24] To that end, "[n]arrowly tailored search methods that begin looking 'in the most obvious places and [then] progressively move from the obvious to the obscure' should be used where possible, but are not necessary in every case."[25] The

---

[21] *Id*. at 370 (citation omitted).

[22] *United States v. Allen*, 53 M.J. 402, 408 (C.A.A.F. 2000).

[23] *Richards*, 76 M.J. at 370 (citations omitted).

[24] *Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*, 403 U.S. 388, 394 n.7 (1971).

[25] *United States v. Loera*, 923 F.3d 907, 920 (10th Cir. 2019) (quoting *United States v. Burgess*, 576 F.3d 1078, 1094 (10th Cir. 2009)).

Fourth Amendment standard is "reasonableness"[26] and courts assess the government's search methods after the fact "in light of the specific circumstances of each case."[27]

Evidence falling outside the scope of a warrant or search authorization may be seized if "[t]he person while in the course of otherwise lawful activity observes in a reasonable fashion property or evidence that the person has probable cause to seize."[28] In order for this "plain view" exception to apply, (1) the officer must not violate the Fourth Amendment in arriving at the spot from which the incriminating materials can be plainly viewed; (2) the incriminating character of the materials must be immediately apparent; and (3) the officer must have lawful access to the object itself.[29] In this regard, the Supreme Court has noted that the "distinction between looking at a suspicious object in plain view and moving it even a few inches is much more than trivial for the purposes of the Fourth Amendment," and the plain view exception must "not be used to extend a general exploratory search from one object to another until something incriminating at last emerges."[30]

---

[26] *United States v. Hill*, 459 F.3d 966, 974–77 (9th Cir. 2006) (upholding off-site search of all defendant's computer storage media for evidence of child pornography).

[27] *United States v. Christie,* 717 F.3d 1156, 1166 (10th Cir. 2013).

[28] Military Rules of Evidence [Mil. R. Evid.] 316(c)(5)(C).

[29] *Richards*, 76 M.J. at 371.

[30] *Arizona v. Hicks*, 480 U.S. 321, 325, 328 (1987) (citation and

Even where evidence is obtained as a result of an unlawful search or seizure, it may only be excluded from use at trial if such exclusion results in appreciable deterrence of future unlawful searches or seizures and the benefits of such deterrence outweigh the costs to the justice system.[31] As the Supreme Court has explained,

> [t]o trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system. As laid out in our cases, the exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence.[32]

Thus, "[t]he extent to which the exclusionary rule is justified by these deterrence principles varies with the culpability of the law enforcement conduct."[33] "Evidence should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth

---

internal quotation marks omitted).

[31] Mil. R. Evid. 311(a).

[32] *Herring v. United States*, 555 U.S. 135, 144 (2009).

[33] *Id*. at 143.

Amendment."[34]

Here, the military judge denied Appellant's suppression motion in a written ruling wherein he made detailed findings of fact, discussed the applicable law, and drew conclusions based upon his application of the law to the facts. He found that (1) the search authorization authorized the DC3 examiner to look in any applications on the phone where location data from the date 23 December 2018 could be located; (2) the examiner's approach to the search was intended to comply with the parameters of the search authorization and be efficient; (3) the examiner first searched the phone's parsed location data, which yielded no data for 23 December 2018; (4) based on his training and experience, the examiner then planned to search for location data within the phone's photos, which he understood to often contain location data; (5) to effect this search, he sorted the images by file size, since the "larger files were more likely to contain location data;" (6) after sorting by file size, he observed suspected child pornography in one of the first ten images, out of over 200,000; and (7) after seeing this image, he immediately stopped his search, contacted his supervisor, and received a new search authorization to search the files for child pornography.[35]

The military judge cited the Fourth Amendment particularity requirement's application to electronic devices, noting that "the courts have

---

[34] *Id*. (internal quotation and citation omitted).

[35] App. Ex. LIII at 6-7.

looked to what is reasonable under the circumstances" when determining whether a search was lawfully conducted within the scope of a search authorization.[36] Focusing specifically on the examiner's decision to search the images for location data, the military judge found that the examiner opened the images category because "photographs are a common place to store [location] data;" that he switched from the thumbnail view to the table view; and that he then sorted by file size, largest to smallest, because "he believed that user-taken photos might have location meta-data."[37] The military judge found that the examiner's "plan was to next sort the images by date," but that he stopped the search because after sorting the images by size he saw an image of suspected child pornography, which was "visible within [the examiner's] screen without even scrolling."[38]

On these facts, the military judge concluded the examiner's search was "conducted reasonably and did not exceed the scope of the [search authorization]."[39] He rejected Appellant's argument that the search should have been conducted according to the methodology proffered by Appellant's digital forensics expert because the examiner's search was conducted reasonably, which is all the Fourth Amendment requires. He further concluded that even if the search

---

[36] *Id*. at 12, 20.

[37] *Id*. at 20.

[38] *Id*.

[39] *Id*.

methodology was unreasonable, excluding the evidence would not appreciably deter future unlawful searches, since the examiner "attempted to stay within the scope of the [search authorization], only searching in areas of the phone authorized by the [search authorization] . . . , looking for images that would have been stored in the photo application of the phone, since pictures often contain location metadata."[40]

While we find the DC3 examiner's search methodology concerning, we find no abuse of discretion in the military judge's ruling. The findings of fact upon which the military judge predicated his conclusions are supported by the evidence in the record and are not clearly erroneous; he applied the correct legal principles to the facts in a reasonable manner; and the conclusions he reached are not arbitrary, fanciful, clearly unreasonable or clearly erroneous.

Appellant takes issue with the examiner's decision to first sort the 200,000+ images by file size before setting filters to narrow them to only (a) those containing location data and (b) those created on 23 December 2018. We, too, find it difficult to follow the examiner's logic in sorting the data in this manner, which appears to have been driven by mere convenience. As he testified, his plan was that "once [he] got it into these columns and sorted largest to smallest [he] was going to begin filtering. [His] thought process[] [was that] as [he] filter[ed,] the larger ones [would] stay at the top and [he wouldn't]

---

[40] *Id.*

have to re-sort every time [he] appl[ied] the filter . . . for all photos that contain GPS [location data] and then . . . filter[ed] that with a date."[41] But since his intention was to "set a filter to only show photos with metadata that contains location data,"[42] that would seem to obviate the need to sort by file size at all, since *every* image file filtered in this way would contain location data, not just the larger ones.

The real logic driving the examiner's decision may well be the apparent skepticism at DC3 that the Cellebrite data analyzer can accurately parse data in this fashion, and the consequent expectation that examiners will routinely review data files manually to crosscheck the accuracy of the Cellebrite filters. As the examiner himself noted, after discussing the issue with one of DC3's top examiners, his job was "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. . . . 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 [Standard Operating Procedure]' for examiners."[43] Similarly, another examiner at DC3 opined that "search authority that specifies 'all location data stored on the phone or within any application within the phone' should involve manual review. Without manual verification, an examiner would not be able to accurately state that all location

---

[41] R. at 243.

[42] *Id.*

[43] App. Ex. XXVI at 91.

data, especially within apps, was reviewed for relevance."[44]

Such an unwritten policy of defaulting to manual review of data files, even where a search authorization contains specific search limitations, is problematic from a plain view standpoint. As our superior court has noted,

> Courts have struggled to apply the plain view doctrine to search of digital devices, given the vast amount of information they are capable of storing and the difficulty inherent in tailoring searches of electronic data to discover evidence of particular criminal conduct. In light of these difficulties, the application of the plain view doctrine in a digital context poses a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant."[45]

And, as we have discussed before, we are mindful of the dangers posed by allowing digital searches to devolve into the sort of "wide-ranging exploratory searches the Framers intended to prohibit."[46]

---

[44] App. Ex. XXVI at 100.

[45] *United States v. Gurczynski*, 76 M.J. 381, 387 (C.A.A.F. 2017) (citations and internal quotation marks omitted).

[46] *United States v. Lee*, No. 202000239, 2022 CCA LEXIS, *32

Nevertheless, in this case, we 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."[47] 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.

We note, however, that another military judge might reasonably have concluded otherwise on similar facts. The plain view exception requires that each step of an authorized search comply with the Fourth Amendment in arriving at the spot from which the incriminating materials are plainly viewed. Digital forensic examiners must therefore take great care to not only fully document their search methods, but also narrowly tailor them to "begin looking 'in the most obvious places and [then] progressively move from the obvious to the obscure.'"[48] The examiner's search in this case was problematic in both respects. And in another case there may be additional evidence to

---

(N-M. Ct. Crim. App. Apr. 5, 2022) (unpublished) (quoting *Garrison*, 480 U.S. at 84).

[47] App. Ex. LIII at 20.

[48] *Loera*, 923 F.3d at 920 (quoting *Burgess*, 576 F.3d at 1094).

support a finding of not just mere negligence in this regard, but the sort of "gross[] [or] . . . recurring or systemic negligence" that the exclusionary rule is specifically designed to deter.[49]

B. Motion to Recuse

At trial the military judge disclosed that he had prior friendly, professional relationships with both the trial counsel and the trial defense counsel. Additionally, the trial defense counsel notified the military judge that one of the court reporters was a named victim in the case. After conducting voir dire about the military judge's relationships with the trial counsel and the court reporter, Appellant moved for the military judge's recusal. He argued that the military judge could not be impartial because of "implied bias," that the "public's confidence in military justice" would be undermined because of those relationships and that the military judge was required to recuse himself for apparent bias pursuant to Rules for Courts-Martial [R.C.M.] 902(a). After hearing argument, the military judge denied the motion.

Appellant then entered into a plea agreement in which he agreed to plead guilty to certain offenses conditioned upon his right to preserve certain issues for appeal—which did not include the denial of his recusal motion. He also agreed to plead guilty unconditionally to Charge III and its sole specification (indecent exposure in violation of Article 120c, UCMJ), and waived all motions except those that are non-waivable under R.C.M. 705(c)(1)(B) with respect to

---

[49] *Herring*, 555 U.S. at 144.

that offense. At trial, after agreeing to be tried and sentenced by the same military judge who had denied his recusal motion, Appellant confirmed that he understood these provisions and had freely and voluntarily agreed to them in exchange for what he believed to be a beneficial plea agreement.

1. Waiver

We review de novo the legal question of whether an appellant has waived an issue.[50] Forfeiture is the failure to make a timely assertion of a right whereas waiver is the intentional relinquishment or abandonment of a known right.[51] "Unlike claims based on actual bias, disqualification under R.C.M. 902(a) is subject to waiver after full disclosure on the record of the basis for disqualification."[52]

Here, the basis for Appellant's recusal motion under R.C.M. 902(a) was the relationship between the military judge and both the trial counsel and the court reporter, who was a named victim in Appellant's court-martial. We find that Appellant, having conducted voir dire of the military judge into these very issues, was fully informed and aware of the extent of the military judge's relationships with the individuals involved when he agreed to waive this issue to gain

---

[50] *United States v. Davis*, 79 M.J. 329, 331 (C.A.A.F. 2020).

[51] *Davis*, 79 M.J. at 331 (quoting *United States v. Gladue*, 67 M.J. 311, 313 (C.A.A.F. 2009)).

[52] *United States v. Black*, 80 M.J. 570, 574 (C.A.A.F. 2020) (citing Rules for Courts-Martial [R.C.M.] 902(e); *United States v. Quintanilla*, 56 M.J. 37, 77 (C.A.A.F. 2001)).

the benefit of his pretrial agreement. We find the knowing nature of this waiver further reinforced by Appellant's election to plead guilty before and be sentenced by the same military judge. Accordingly, we find that Appellant knowingly and intentionally waived the issue he now asserts as error.[53]

2. Apparent Bias

We generally do not review waived issues "because a valid waiver leaves no error for us to correct on appeal."[54] However, while there is no waiver provision present in Article 66, UCMJ, military courts of criminal appeals still must review the entire record and approve only that which "should be approved."[55] This includes reviewing "whether to leave an accused's waiver intact, or to correct error."[56] In this case we leave the waiver intact because even if we were to review his claim, we would find no prejudicial error.

A military judge's decision not to recuse himself is reviewed for an abuse of discretion.[57] Any error is reviewed for harmlessness.[58] An accused has a

---

[53] *See Gladue*, 67 M.J. at 314.

[54] *Davis*, 79 M.J. at 331 (quoting *United States v. Campos*, 67 M.J. 330, 332 (C.A.A.F. 2009)).

[55] *United States v. Chin*, 75 M.J. 220, 223 (C.A.A.F. 2016) (quoting Article 66, UCMJ).

[56] *Id.*

[57] *United States v. Sullivan*, 74 M.J. 448, 453 (C.A.A.F. 2015).

[58] *United States v. Roach*, 69 M.J. 17, 20 (C.A.A.F. 2010) (citing *Liljeberg v. Health Services Acquisition Corp.*, 486 U.S. 874

constitutional right to an impartial judge.[59] However, there is a "high hurdle" an appellant must clear to prove that a military judge was partial or appeared to be so, as the law establishes a "strong presumption" to the contrary.[60] R.C.M 902(a) states that "a military judge shall disqualify himself . . . in any proceeding in which that military judge's impartiality might reasonably be questioned."[61] Our higher court has articulated this standard as "[a]ny conduct that would lead a reasonable man knowing all the circumstances to the conclusion that the judge's impartiality might reasonably be questioned."[62]

Having a professional relationship or friendship is not, in and of itself, disqualifying. As our superior court has noted "[t]he world of career [judge advocates] is relatively small and cohesive, with professional relationships the norm and friendships common."[63] In most instances, professional or friendly relationships do not require a military judge to recuse himself. The real question is not whether there is a relationship but, rather whether the relationship between a military judge and a party raises "special

---

(1988)).

[59] *United States v. Butcher*, 56 M.J. 87, 90 (C.A.A.F. 2001) (quotation marks and citation omitted).

[60] *United States v. Quintanilla*, 56 M.J. 37, 44 (C.A.A.F. 2001).

[61] R.C.M. 902(a).

[62] *Hasan v. Gross*, 71 M.J. 416, 418 (C.A.A.F. 2012).

[63] *United States v. Uribe*, 80 M.J. 442, 447 (C.A.A.F. 2021) (citing *Butcher*, 56 M.J. at 91).

concerns," whether the relationship was "so close or unusual as to be problematic," and whether "the association exceeds what might reasonably be expected in light of the [normal] associational activities of an ordinary [military] judge."[64]

Here, the military judge made findings, stated the law he was applying, and made his ruling on the record denying Appellant's motion. He cited R.C.M. 902 and applied the "objective standard of whether a reasonable person, knowing the circumstances, would conclude that the military judge's impartiality might reasonably be questioned."[65] He then discussed his application of *United States v. Uribe*, noting that while Appellant "has the Constitutional right to an impartial judge," a judge also "has as much of an obligation to not disqualify himself when there's no reason to do so."[66] He also considered the factors from *Liljeberg v. Health Servs. Acquisition Corp.*, for recusal: (1) "the risk of injustice to the parties in the particular case," (2) "the risk that the denial of relief will produce injustice in other cases," and (3) "the risk of undermining the public confidence in the judicial process."[67]

We find an objectively reasonable person aware of all the relevant facts concerning the military judge's professional relationship with the trial counsel and a

---

[64] *Uribe*, 80 M.J. at 447 (cleaned up).

[65] R. at 30.

[66] *Id.*

[67] *Id.* at 31 (quoting *Liljeberg v. Health Servs. Acquisition Corp.*, 486 U.S. 847, 864 (1988)).

named victim in Appellant's court-martial would have no questions about the military judge's impartiality. We therefore find no error in the military judge's decision to deny Appellant's motion that he recuse himself.

III. CONCLUSION

After careful consideration of the record and briefs of appellate counsel, we have determined that the findings and sentence are correct in law and fact and that no error materially prejudicial to Appellant's substantial rights occurred.[68]

The findings and sentence are **AFFIRMED**.

FOR THE COURT:

S. TAYLOR JOHNSTON

Interim Clerk of Court

[68] Articles 59 & 66, UCMJ.

Q. Okay. And just to be clear, once you got into that photos folder and you sorted the photos by size, it was your intent for the next step, if not one of the next steps, to then filter that for that particular date that was noted in the CASS?

A. Yes. I was going to eventually filter down to, with GPS data. There is an option. And then I would narrow the date.

. . .

Q. So you mentioned that after you did you looked at the device locations, then you moved over to photos because you wanted to look for unparsed data?

A. That was my eventual goal. But I was going to have to -- I wanted to look at them first, see if there were a significant amount of photos with GPS data, and then start filtering from there. But yes, I was just verifying that what I see is what the tool is recording.

. . .

Q. Now, in the process that you used after you moved over to photos -- and again, you were there because you wanted to look for unparsed data?

A. I was there to review photos that had GPS coordinates in an attempt to eventually filter that down to one day.

Q. So you're there to review GPS coordinates. So you selected the photos. And at that point, you could have selected for the

coordinates to just display pictures that had coordinates?

A. That is where I was headed when --

Q. But you did not do that; correct?

A. I did not get to that because I observed a photo and I stopped.

Q. No. I'm saying before you sorted them, you selected the photos tab. At that point, you could have filtered for geolocation data?

A. Yes. Yes, I could have.

AFFIDAVIT

I, Alexader Zaferiou, Digital Forensic Examiner, DC3 Cyber Forensics Laboratory, having been duly sworn, do depose the following:

1. My name is Alexander Zaferiou. I have been a Computer Forensic Examiner at the DoD Cyber Crime Center Forensics Laboratory (DC3/CFL) continuously since August 2015 working in the Major Crimes & Safety Section. The Major Crimes & Safety Section is responsible for substantive analysis of digital media to develop evidence in the specialty area of computer forensics in support of Department of Defense criminal investigations. Prior to coming to DC3/CFL, I was an examiner with the Baltimore County Police Department's Digital and Multimedia Evidence Unit (DMEU) for five (5) years.

   My professional certifications include: Certified Forensic Computer Examiner and Department of Defense Digital Forensic Examiner.

   I have testified as an expert witness in digital forensics in State, Federal, and Military courts for the following cases:

US v. Salcedo (NAS Pensacola, Florida)

US v. Sparks (US District Court, Hartford, Connecticut)

State of Maryland v. Carlos Lomax (Baltimore County Circuit Court)

US v. Post (Joint Base Lewis-McChord, Washington) *US v. Ransier* (US District Court, Baltimore, Maryland) *US v. Sepulveda* (Grand Forks AFB, North Dakota)

State of Maryland v. Rashaan Williams (Baltimore County Circuit Court) *State of Maryland v. Linwood Tymais Smith* (Baltimore County Circuit Court) *State of Maryland v. Kenyon Travis Waller* (Baltimore County Circuit Court)

State of Maryland v. William Justin Campbell (Baltimore County Circuit Court)

DC3/CFL is accredited by the ANSI-ASQ National Accreditation Board (ANAB). Pursuant to the lab maintaining this accreditation, 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 at DC3/CFL.

2. I have reviewed the below listed documents in the case of US v. SHIELDS:

   200916 Shields Def MTS (particularity) w encls.pdf 2019-0440.[Fl}Initial_Request.pdf

   2019-0440.[F9]Lab_Notes.SMITHFINAL.pdf

   2019-0440.[F4]Lab_Report.FINAL.pdf

Questions submitted by Maj. Eric Skoczenski regarding the reviewed documents are addressed below.

3. *"Based on your training and experience, what was your interpretation of what the May 2019 CASS in this case authorized/requested?"*

   The specific language within the CASS was "all location data stored on the phone or within any application within the phone for 23Dec18." This would include a comprehensive manual review of the submitted iPhone for any location data that may not be parsed automatically by forensic tools.

4. *"Based on your training and experience, did the CASS presented to Mr. Smith appear to be facially deficient? Did it*

appear reasonable?"

The language appeared to be reasonable and consistent with other examinations in my experience.

5. *"What, in laymans terms, does 'parsing' mean, in the digital forensic context?"*

   Parsing essentially refers to analyzing and interpreting data in human readable formats. For example, a most devices do not store timestamps in a standard "mm/dd/yyyy hh:mm:ss" format. In the case of the iPhone, an unparsed timestamp would be stored in Apple's time format which could look something like 609821576 when viewed directly at the source on the device. When parsed into human readable format that time value would be 04/29/2020 02:52:56.

6. *"Is the method outlined in Afr. Peden's proffer how you would expect most analysts at DC3 (or anywhere else) to conduct a search pursuant to this CASS?"*

   No. Mr. Peden's method was more akin to a device preview using software functionality intended for untrained users rather than a forensic examination of the device. Cellebrite's Physical Analyzer software was used to filter automatically parsed and sorted data with no further work being

performed to manually verify findings or determine if there was any data missed by Physical Analyzer's parsers.

Mr. Peden's credentials outlined in the Defense motion included being "certified by Cellebrite Forensics for forensics related to cell phones." The prerequisites required to obtain certification as a Cellebrite Certified Physical Analyst (CCPA) include training courses which emphasize the limitations of Physical Analyzer and the necessity for an examiner to perform their own analysis and manually verify reported data.

Cellebrite also provides documentation titled "Preparing Testimony about Cellebrite UFED in a Daubert or Frye Hearing" which includes the following statement regarding expert qualifications, "As with any digital forensic tool or technique, it is not recommended that a mobile device examiner rely on a single UFED tool to interpret the data. Examiners should be trained and qualified to validate what is on the device and where it is located, especially after performing a physical extraction."

7. *"What are the shortcomings of the method Mr. Peden outlines in his proffer in the*

defense motion? Is there a danger of excluding evidence by utilizing that method? Why? Do most digital forensic analysis 'trust' the search tools to properly filter a search? Why or why not?"

Mr. Peden's outlined method introduces the danger of missing evidence that could be either probative or exculpatory. The rate at which technology changes and new apps or app updates are available makes it an impossible task to have a single tool that can provide support for every available app. Physical Analyzer's ability to parse, categorize, and display data from apps is limited by what parsers it includes and when they were last updated.

The search and filter functions in Physical Analyzer will only include data that has been parsed automatically by the tool. This brings the examiner back to the initial limitations of Physical Analyzer outlined in Cellebrite training and manuals. If Physical Analyzer does not support a particular app that contains location data, there will be no results to review within a search, a filter, or the "Locations" category. Unparsed app data could only be identified by an examiner through a manual review of the phone and actual forensic analysis.

8. *"What is a 'manual review' of a phone and*

how does that differ from what is proposed by Mr. Peden? Would digital forensic analysts typically conduct a 'manual review' of a phone.for a CASS of this nature? Why?"

Manual review essentially involves an examiner opening and analyzing files to verify accuracy of automated tool results or to identify data that a tool may have missed. A common example of manual review would be verifying Physical Analyzer's reporting on the number of text messages recovered on a phone. The examiner would open the relevant database containing text messages and perform an analysis to determine if there are any deleted messages that the tool was unable to identify automatically, or if any third party communication apps are present that the Physical Analyzer did not support.

Typically, search authority that specifies "all location data stored on the phone or within any application within the phone... " should involve manual review. Without manual verification, an examiner would not be able to accurately state that all location data, especially within apps, was reviewed for relevance.

9. *"How do iPhones track a person's location?"*

There are a variety of ways that an iPhone can track location. There are built-in services, such as Routine, which will regularly record the device's location in

order to establish potential routines for quality of life purposes. An example would be the iPhone identifying your morning commute via the Routine service and displaying a traffic report for your route.

Third party applications (apps) may also track device location separate from standard iPhone tracking such as Google Maps for navigation functionality, or Uber to determine your pickup address. The sheer number of apps available and rate at which they update makes it impossible for any single tool to automatically parse all relevant data without manual review.

10. *"Could you explain any other exams you've had involving location data that were not automatically parsed by forensic tools?"*

NCIS submitted an iPhone 7 to DC3/CFL in a case where a deceased Marine was discovered in their barrack's room. The case agent requested an analysis of location and other data from the iPhone 7 to create a timeline of the Marine's activities in the days prior to their death.

Physical Analyzer was used to initially generate a report for review by the case agent. Subsequent manual review

revealed that many relevant items were not included in this report as they were missed by the tool's deleted data recovery capabilities, or were within apps and files that were not supported by Physical Analyzer. As such, a review of the "Locations" category did not reveal all of the available location data on the iPhone.

Manual review of apps, files, and system logs was required to identify location data, correct automatic parsing errors, and create a timeline which ultimately generated investigative leads.

11. *"Is a review of photos typically part of an examination for location data, and would using a 'jilter' give you the same results as a manual review?"*

Pictures in general can play an important role in an examination for location data and does not solely involve photos taken with the phone's camera. Pictures are constantly being generated by apps while the iPhone is in use and can contain relevant information. Pictures identified in the previously mentioned NCIS death examination depicted portions of maps, screen captures of location searches, and other cached data of relevance to establishing a location timeline.

A limitation of using Physical Analyzer's filters to display pictures within a specific timeframe is that it relies on the tool to have accurately determined the dates associated with the pictures it identified. It may display incorrect date information derived from the files which contained the pictures as embedded data, or may not display dates at all. For example, a previous examination involving an iPhone 7 identified pictures which appeared relevant to the agent's request during manual review of app data. The pictures had no dates associated with them in Physical Analyzer's results and did not appear when filtering for the notable timeframe in the case. This was due to the pictures being embedded within files associated with the Kik chat app which Physical Analyzer did not have the capability to automatically parse correctly at the time of that examination. This evidence would not have been found based solely on a review of pictures filtered by date.

10. *"Based on your training and experience, and review of the evidence in this case, do you believe that Mr. Smith conducted this search in a reasonable manner and in*

compliance with normal procedures?"

Yes.

I declare under the penalty of perjury that the foregoing is true and correct per 28 USC§ 1746. Executed on 29 September 2020.