

IN THE UNITED STATES COURT OF APPEALS  
FOR THE ARMED FORCES

UNITED STATES,	)	ANSWER ON BEHALF OF
Appellee	)	APPELLEE
	)	
v.	)	Crim.App. Dkt. No. 202100061
	)	
Ethan R. SHIELDS,	)	USCA Dkt. No. 22-0279/MC
Staff Sergeant (E-6)	)	
U.S. Marine Corps	)	
Appellant	)	

TYLER W. BLAIR  
Captain, U.S. Marine Corps  
Appellate Government Counsel  
Navy-Marine Corps Appellate  
Review Activity  
Bldg. 58, Suite B01  
1254 Charles Morris Street SE  
Washington Navy Yard, DC 20374  
(202) 685-7433  
Bar no. 37601

GREGORY A. RUSTICO  
Lieutenant, JAGC, U.S. Navy  
Senior Appellate Counsel  
Navy-Marine Corps Appellate  
Review Activity  
Bldg. 58, Suite B01  
1254 Charles Morris Street SE  
Washington Navy Yard, DC 20374  
(202) 685-7686  
Bar no. 37338

JOSEPH M. JENNINGS  
Colonel, U.S. Marine Corps  
Director, Appellate Government  
Navy-Marine Corps Appellate  
Review Activity  
Bldg. 58, Suite B01  
1254 Charles Morris Street SE  
Washington Navy Yard, DC 20374  
(202) 685-7427, fax (202) 685-7687  
Bar no. 37744

BRIAN K. KELLER  
Deputy Director  
Appellate Government  
Navy-Marine Corps Appellate  
Review Activity  
Bldg. 58, Suite B01  
1254 Charles Morris Street SE  
Washington Navy Yard, DC 20374  
(202) 685-7682, fax (202) 685-7687  
Bar no. 31714

**Index of Brief**

**Table of Authorities** ..... viii

**Issue Presented** ..... 1

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?

**Statement of Statutory Jurisdiction** ..... 1

**Statement of the Case** ..... 1

**Statement of Facts**..... 2

A. The United States charged Appellant with indecent exposure, child pornography offenses, attempted indecent visual recording, indecent visual recording, and drug offenses..... 2

B. Appellant moved to suppress the search of his cell phone. The Parties presented evidence and argument on the Motion ..... 2

1. The Commanding Officer testified he issued a Search Authorization to search Appellant’s phone for location data from the day of the alleged offense..... 3

2. Law enforcement seized and searched Appellant’s phone ..... 4

3. The Defense Cyber Crime Center extracted raw data from the phone and delivered a copy to the Examiner ..... 4

4. The Examiner testified he first used the Cellebrite physical analyzer’s “viewer” to read “parsed data” automatically organized into a “location” category. He found no data relevant to December 23, 2018 ..... 4

5.	<u>The Examiner recognized the need to perform a confirmatory second search using the physical analyzer to search files for location data. While sorting the images and without scrolling, he saw a suspected child pornography image</u> .....	6
a.	<u>Knowing that the physical analyzer sometimes fails to properly or fully extract all file data, the Examiner planned a confirmatory second search</u> .....	6
b.	<u>The Examiner and his Supervisor explained the need to conduct “forensic analysis” to confirm the accuracy of the tool’s results due to the physical analyzer’s limitations in correctly parsing date and location data</u> .....	7
c.	<u>The Examiner conducted a second search aimed at uncovering unidentified or unparsed relevant location and date data in the device’s applications, starting with photos</u> .....	8
d.	<u>At the start of his confirmatory search, after sorting by size for efficiency and to sort out images that would likely not have location data, an image of child pornography appeared on the Examiner’s screen</u> .....	9
6.	<u>After seeing the suspected child pornography image, the Examiner stopped his search, notified his Supervisor, and obtained a Search Authorization for child pornography</u> .....	10
7.	<u>A later search of Appellant’s phone yielded evidence of additional misconduct</u> .....	11
8.	<u>Appellant’s Expert Consultant testified he believed the Examiner’s second search was unreasonable</u> .....	11
C.	<u>The Military Judge denied Appellant’s Motion in a written Ruling, concluding that the Examiner’s search of Appellant’s phone was “conducted in a reasonable manner and did not exceed the scope of the [Search Authorization].”</u> .....	12
1.	<u>The Judge found the Examiner’s search aimed to comply with the Search Authorization when he found the child pornography</u> .....	12

2.	<u>The Military Judge discussed the applicable law</u> .....	13
3.	<u>The Military Judge concluded that the Examiner reasonably conducted a lawful search of Appellant’s phone and saw the single image of child pornography in plain view</u> .....	13
D.	<u>Appellant pled not guilty to three offenses and pled guilty to the remaining offenses pursuant to a Plea Agreement, and was sentenced by the Military Judge</u> .....	15
E.	<u>The lower court affirmed the findings and sentence</u> .....	16
	<b>Argument</b> .....	16

THE MILITARY JUDGE DID NOT ABUSE HIS DISCRETION BY DENYING APPELLANT’S MOTION TO SUPPRESS. THE FORENSIC EXAMINER SEARCHED ONLY WITHIN THE SCOPE OF THE SEARCH AUTHORIZATION, CONDUCTED A REASONABLE SEARCH, FOUND AN IMAGE OF CHILD PORNOGRAPHY ON APPELLANT’S PHONE IN PLAIN VIEW, AND IMMEDIATELY STOPPED THE SEARCH. ....16

A.	<u>The standard of review is abuse of discretion</u> .....	17
B.	<u>Courts presume a search under a valid search authorization is reasonable and lawful under the Fourth Amendment</u> .....	17
C.	<u>Courts decline to impose <i>ex ante</i> search methodologies on search warrants or search authorizations of digital devices. The test remains reasonableness</u> .....	18
D.	<u>The Military Judge did not abuse his discretion by denying the Motion. The Examiner’s search was reasonable because (1) it was within the scope of the Search Authorization, and (2) he discovered the contraband image in plain view</u> .....	19
1.	<u>The Examiner conducted a reasonable search. He looked for unparsed location data in places the Record supports could contain that data. Nothing supports that he conducted a general search</u> .....	20

a.	<u>A search reasonably aimed at uncovering evidence that is the subject of a warrant does not exceed the warrant’s scope</u> .....	21
b.	<u>Agents exceed a warrant’s scope when they “abandon” their search to uncover evidence of crimes outside the scope of the warrant</u> .....	24
c.	<u>Like <i>Richards</i>, <i>Loera</i>, and <i>Burgess</i>, the Examiner did not exceed the authorization’s scope: his search aimed to uncover responsive evidence—location data embedded in pictures—that the physical analyzer could not identify</u> .....	25
d.	<u>No evidence supports that the Examiner exceeded the scope of the Search Authorization in sorting by size or that he scrolled through Appellant’s images, and Appellant fails to point to any</u> .....	27
e.	<u>Appellant misapplies <i>Garrison</i>: the Examiner conducted a search tailored to uncover relevant evidence</u> .....	28
2.	<u>The Examiner reasonably searched for unparsed location data—consistent with evidence about where that kind of data might be—when he sorted image files from largest to smallest</u> .....	29
a.	<u>Courts do not require specific search protocols for digital searches</u> .....	30
b.	<u>The Examiner reasonably started the search sorting by size, as user-generated photos with location data would likely be the largest images. Evidence supported that photos taken by Appellant would likely have unparsed location data responsive to the Search Authorization. Tailoring his search, the Examiner’s search was more limited than the lawful but un-tailored searches in <i>Richard</i>, <i>Giverson</i>, <i>Loera</i>, and <i>Burgess</i></u> .....	32
c.	<u>The Examiner reasonably began searching in “obvious” places and moved to “obscure” places when looking for location data. Appellant’s argument to the contrary fails</u> .....	35

3.	<u>The Military Judge’s Findings of Fact were supported by the Record. Appellant fails to show his Findings were clearly erroneous</u> .....	36
a.	<u>The Examiner’s search did not amount to a general search prohibited under the Fourth Amendment, and Appellant fails to show the Examiner “rummaged through unauthorized areas of the cell phone.”</u> .....	36
b.	<u>Appellant fails to show the Examiner did not intend to “next sort the images by date” or did not see the contraband while sorting the images. He also fails to show how the Examiner went outside “the scope of the CASS.”</u> .....	37
E.	<u>The Military Judge did not abuse his discretion by finding the contraband images admissible under the plain view doctrine</u> .....	38
1.	<u>The plain view doctrine permits the admissibility of evidence of additional illegality discovered during a lawful search</u> .....	38
2.	<u>The contraband was lawfully discovered in plain view because the Examiner (1) was acting under a valid Search Authorization, (2) immediately saw the image and stopped his search, and (3) was lawfully in the location where he saw the image because he believed he would find relevant evidence.</u> .....	39
3.	<u>Appellant’s arguments that the Military Judge misunderstood the law or should be afforded less deference are inapt because he applied the correct law to facts supported by the Record. He found the Examiner did not scroll through images because the Record supports that conclusion</u> .....	41
F.	<u>Even assuming the Military Judge abused his discretion, Mil. R. Evid. 311(a)(3) does not support exclusion</u> .....	42
1.	<u>Exclusion of evidence is required only when it would deter future unlawful searches that were the result of deliberate police misconduct</u> .....	42

2. There is no evidence law enforcement deliberately disregarded Appellant’s rights or that exclusion would deter improper conduct, so the exclusionary rule does not apply.....43

**Conclusion**.....46

**Certificate of Compliance**.....46

**Certificate of Filing and Service** .....47

## Table of Authorities

	Page
UNITED STATES SUPREME COURT CASES	
<i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018).....	36–37
<i>Dalia v. United States</i> , 441 U.S. 238 (1979).....	19
<i>Herring v. United States</i> , 555 U.S. 135 (2009) .....	43–44
<i>Horton v. California</i> , 496 U.S. 128 (1990) .....	39
<i>Maryland v. Garrison</i> , 480 U.S. 79 (1987).....	28–29
<i>Riley v. California</i> , 573 U.S. 373 (2014).....	<i>passim</i>
<i>United States v. Davis</i> , 564 U.S. 229 (2011).....	43–44
<i>United States v. Leon</i> , 468 U.S. 897 (1984) .....	42, 44
<i>United States v. Ross</i> , 456 U.S. 798 (1982).....	20
<i>Wong Sun v. United States</i> , 371 U.S. 471 (1963).....	42
UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES AND COURT OF MILITARY APPEALS CASES	
<i>United States v. Allen</i> , 53 M.J. 402 (C.A.A.F. 2000).....	18
<i>United States v. Bess</i> , 75 M.J. 70 (C.A.A.F. 2016).....	36–37
<i>United States v. Conklin</i> , 63 M.J. 333 (C.A.A.F. 2006).....	42
<i>United States v. Criswell</i> , 78 M.J. 136 (C.A.A.F. 2018).....	36, 38
<i>United States v. Downing</i> , 56 M.J. 419 (C.A.A.F. 2002).....	41
<i>United States v. Eppes</i> , 77 M.J. 339 (C.A.A.F. 2018).....	<i>passim</i>
<i>United States v. Flesher</i> , 73 M.J. 303 (C.A.A.F. 2014) .....	41
<i>United States v. Gurczynski</i> , 76 M.J. 381 (C.A.A.F. 2017) .....	25
<i>United States v. Hoffman</i> , 75 M.J. 120 (C.A.A.F. 2016) .....	17
<i>United State v. Mann</i> , 54 M.J. 164 (C.A.A.F. 2000).....	28
<i>United States v. McMahon</i> , 58 M.J. 362 (C.A.A.F. 2003).....	24, 38



<i>United States v. Richards</i> , 76 M.J. 365 (C.A.A.F. 2017).....	<i>passim</i>
<i>United States v. Shields</i> , No. 22-0279/MC, 2022 CAAF LEXIS 809 (C.A.A.F. Nov. 10, 2022).....	2
<i>United States v. Solomon</i> , 72 M.J. 176 (C.A.A.F. 2013) .....	28
UNITED STATES NAVY-MARINE CORPS COURT OF CRIMINAL APPEALS CASES	
<i>United States v. Shields</i> , No. 202100061, 2022 CCA LEXIS 448 (N-M. Ct. Crim. App. July 27, 2022).....	2, 16
UNITED STATES CIRCUIT COURTS OF APPEALS CASES	
<i>United States v. Burgess</i> , 576 F.3d 1078 (10th Cir. 2009) .....	<i>passim</i>
<i>United States v. Carey</i> , 172 F.3d 1268 (10th Cir. 1999).....	23–24
<i>United States v. Christie</i> , 717 F.3d 1156 (10th Cir. 2013) .....	19
<i>United States v. Evers</i> , 669 F.3d 645 (6th Cir. 2012) .....	20
<i>United States v. Giberson</i> , 527 F.3d 882 (9th Cir. 2008) .....	31
<i>United States v. Hill</i> , 459 F.3d 966 (9th Cir. 2006) .....	18–19
<i>United States v. Loera</i> , 923 F.3d 907 (10th Cir. 2019).....	<i>passim</i>
<i>United States v. Mann</i> , 592 F.3d 779 (7th Cir. 2010) .....	24–25, 31
<i>United States v. Miranda</i> , 325 F. App’x 858 (11th Cir. 2009).....	31
<i>United States v. Richards</i> , 659 F.3d 527 (6th Cir. 2011).....	20
<i>United States v. Sims</i> , 553 F.3d 580 (7th Cir. 2009).....	17
<i>United States v. Stabile</i> , 633 F.3d 219 (3d Cir. 2011) .....	31
<i>United States v. Ulbricht</i> , 858 F.3d 71 (2d Cir. 2017).....	34
<i>United States v. Walser</i> , 275 F.3d 981 (10th Cir. 2001).....	24
<i>United States v. Williams</i> , 592 F.3d 511 (4th Cir. 2010) .....	31
<i>United States v. Wong</i> , 334 F.3d 831 (9th Cir. 2003).....	31

UNIFORM CODE OF MILITARY JUSTICE, 10 U.S.C. §§ 801–946 (2018)

Article 66 .....1  
Article 67 .....1  
Article 80 .....1  
Article 112a .....1  
Article 120c .....1  
Article 134 .....1

MILITARY RULES OF EVIDENCE (2018)

Mil. R. Evid. 311 .....42, 44  
Mil. R. Evid. 315 .....17  
Mil. R. Evid. 316 .....13, 38

OTHER RULES, STATUTES, SOURCES

U.S. Const. amend. IV .....17

## **Issue Presented**

**WHERE THE SEARCH AUTHORIZATION ONLY SOUGHT MATERIALS FROM ONE DATE, BUT THE GOVERNMENT LOOKED AT IMAGES IRRESPECTIVE OF THAT DATE, DID THE MILITARY JUDGE ABUSE HIS DISCRETION BY FINDING THE SEARCH DID NOT VIOLATE THE FOURTH AMENDMENT?**

## **Statement of Statutory Jurisdiction**

The Navy-Marine Corps Court of Criminal Appeals had jurisdiction under Article 66, Uniform Code of Military Justice (UCMJ), 10 U.S.C. § 866 (2020), because Appellant's approved sentence included a dishonorable discharge and confinement for more than one year. This Court has jurisdiction under Article 67(a)(3), UCMJ, 10 U.S.C. § 867(a)(3) (2020).

## **Statement of the Case**

A military judge sitting as a general court-martial convicted Appellant, pursuant to his pleas, of attempted indecent visual recording, wrongful possession and wrongful use of a controlled substance, indecent exposure, possessing and viewing child pornography, indecent visual recording, and producing child pornography in violation of Articles 80 and 120c, UCMJ, 10 U.S.C. §§ 880, 920c, (2016) and Articles 112a, 120c, and 134, UCMJ, 10 U.S.C. §§ 912a, 920c, and 934 (2016). The Military Judge sentenced Appellant to fifty-two months of confinement, reduction to pay grade E-1, total forfeitures, and a dishonorable

discharge. The Convening Authority approved the sentence as adjudged and, except for the punitive discharge, ordered the sentence executed.

On review, the lower court affirmed the findings and sentence. *United States v. Shields*, No. 202100061, 2022 CCA LEXIS 448, at \*22 (N-M. Ct. Crim. App. July 27, 2022).

Upon Appellant's Petition, this Court granted review. (Appellant's Pet., Sept. 15, 2022; Appellant's Supp. Pet., Sept. 15, 2022); *United States v. Shields*, No. 22-0279/MC, 2022 CAAF LEXIS 809 (C.A.A.F. Nov. 10, 2022).

### **Statement of Facts**

- A. The United States charged Appellant with indecent exposure, child pornography offenses, attempted indecent visual recording, indecent visual recording, and drug offenses.

The United States charged Appellant with: one Specification of indecent exposure; one Specification each of possessing, producing, and viewing child pornography; one Specification of indecent visual recording; and, two Specifications of wrongful possession and use of a controlled substance. (J.A. 17–20.)

- B. Appellant moved to suppress the search of his cell phone. The Parties presented evidence and argument on the Motion.

Appellant moved to suppress the images of child pornography found during a search of his cell phone. (J.A. 23, 124.) The United States opposed. (J.A. 299.)

At the Article 39(a) session, the United States presented testimony from the

Investigating Agent, (J.A. 413); Appellant’s Commanding Officer, (J.A. 490); and the Forensic Examiner, (J.A. 547). The United States provided the Examiner’s Digital Laboratory Report, (J.A. 385–89), and Affidavits from the Forensic Examiner, (J.A. 392–395), and the Examiner’s Supervisor, (J.A. 396–400).

1. The Commanding Officer testified he issued a Search Authorization to search Appellant’s phone for location data from the day of the alleged offense.

The Investigating Agent’s Search Authorization Affidavit showed an investigation into allegations of indecent exposure led investigators to Appellant. (J.A. 349–50.) The Investigating Agent testified that after discussing digital forensic capabilities with the Defense Cyber Crime Center, he advised Appellant’s Commanding Officer that location data from the date of the offense could be found on Appellant’s phone. (J.A. 54–57; 418–422.) The Investigating Agent also had surveillance footage of Appellant on base that day with his phone in his hand. (J.A. 422, 504.)

The Commanding Officer signed a Search Authorization for law enforcement to seize Appellant’s cell phone and search for “all location data stored on the phone or within any application within the phone for 23Dec18,” the date of the incident. (J.A. 53, 503–05.) The Commanding Officer testified he “limited” the scope of the search because he did not want “a free for all on [Appellant’s]

phone” because of his “[right to] privacy” but still “need[ed] something that puts [Appellant]” at the crime scene—like location data. (J.A. 506.)

2. Law enforcement seized and searched Appellant’s phone.

The Investigating Agent testified he seized Appellant’s phone pursuant to the Command Authorization for Search and Seizure. (J.A. 423.) Law enforcement then sent the phone to the Defense Cyber Crime Center where a Digital Forensics Examiner conducted a search of Appellant’s cell phone, as noted in the Examiner’s Laboratory Report. (J.A. 385–89.)

3. The Defense Cyber Crime Center extracted raw data from the phone and delivered a copy to the Examiner.

The Examiner testified that “extraction personnel” at the Defense Cyber Crime Center extracted all unfiltered, raw data from Appellant’s phone, made a digital copy of the raw data, placed it in an extraction file, and provided the extraction file to the Examiner. (J.A. 551–52.)

The extraction personnel never sorted files or ran searches on Appellant’s phone when making the copy for the Examiner. (J.A. 552.)

4. The Examiner testified he first used the Cellebrite physical analyzer’s “viewer” to read “parsed data” automatically organized into a “location” category. He found no data relevant to December 23, 2018.

The Examiner testified he reviewed the Search Authorization. (J.A. 385, 553.) The Examiner ported the extraction file into the Cellebrite physical analyzer,

which “parsed” the phone’s unreadable data into a human-“readable” format. (J.A. 556–57.)

The parsed data was then viewable in a physical analyzer—a “tool which is kind of used as a viewer” that takes parsed data and makes it easier to review by categorizing it and putting it in one place—where it was further divided into various categories including “device locations,” “SMS messages,” “texts,” and “internet history.” (J.A. 388, 556–58.) The Examiner cautioned that “a physical analyzer can only parse so much of [a phone’s data]. And whatever it’s able to parse and put in a category, it will.” (J.A. 557.)

The physical analyzer uses a “tree-cable view” with a window on the left with categories that can be selected, that governs what is viewable on the right window. (J.A. 558.) Using the viewer, the user “pick[s] what category you’re interested in, and a lot of times there’s an arrow that we see to expand, and sometimes there will [be] subcategories within these categories.” (J.A. 558–59.)

The Examiner first picked the “device locations” category. (J.A. 557, 559.) There were fewer than 2,000 results overall for the “device location” category. (J.A. 112, 557.) The Examiner “thought the phone would hold substantially more than that” based on his experience. (J.A. 557.)

The physical analyzer noted no “device location” data for December 23, 2018. (J.A. 557–59.)

5. The Examiner recognized the need to perform a confirmatory second search using the physical analyzer to search files for location data. While sorting the images and without scrolling, he saw a suspected child pornography image.
  - a. Knowing that the physical analyzer sometimes fails to properly or fully extract all file data, the Examiner planned a confirmatory second search.

The Examiner testified that he needed to “start 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.” (J.A. 559.) He explained that “as dates change, as applications update,” “there are several applications that would not be properly parsed,” and the physical analyzer may not be able to fully parse all the data in an extraction. (J.A. 559, 566.) He said “it is well known and is taught during . . . training that one tool does not necessarily parse an entire device.” (J.A. 559.)

He “found often that . . . items or artifacts . . . were not parsed by [the] physical analyzer.” (J.A. 559.) He agreed that if he relied solely on the physical analyzer, he would have missed data that might not have been properly parsed. (J.A. 560.)



- b. The Examiner and his Supervisor explained the need to conduct “forensic analysis” to confirm the accuracy of the tool’s results due to the physical analyzer’s limitations in correctly parsing date and location data.

The Examiner testified he knew if he limited his search “only to data successfully parsed [by the physical analyzer] tool,” then “partial result[s]” or data currently unsupported by the physical analyzer, when date or location filters were applied, might exclude relevant evidence. (J.A. 569.) He could not use the physical analyzer to find unparsed data because “[t]here is no way to [apply the physical analyzer’s] filter and still get unparsed results.” (J.A. 569.) Because the tool “only filters parsed data . . . you don’t actually see everything.” (J.A. 578.)

Location data, he testified, is “textual.” (J.A. 591.) But “[t]ime and date stamps . . . need to be further parsed” and there are different ways for different software to “store GPS data.” (J.A. 591–92.) Applications and websites typically store location data in text, but location data embedded in files are sometimes not parsed by the physical tool. (J.A. 591–92.)

The Supervisor explained that “[u]nparsed app data could only be identified by an examiner through a manual review of the phone and actual forensic analysis.” (J.A. 398.) The 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.” (J.A. 398.) A warrant “that specifies [‘]all location data stored on the phone or within any application within the phone . . . [’] should involve manual

review.” (J.A. 398.) The Supervisor noted: “Without manual verification, an examiner would not be able to accurately state that all location data, especially within apps, was reviewed for relevance.” (J.A. 398.)

The Supervisor explained that “[p]ictures are constantly being generated by apps while the iPhone is in use” in addition to user generated photos. (J.A. 399.) “[U]sing [the] Physical Analyzer’s filters to display pictures within a specific timeframe” has limitations because it may not “accurately [determine 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.” (J.A. 399.)

- c. The Examiner conducted a second search aimed at uncovering unidentified or unparsed relevant location and date data in the device’s applications, starting with photos.

After reviewing the Search Authorization, the Examiner believed he “was allowed to look for location data in any application on the phone.” (J.A. 553.) He continued to intend to use the physical analyzer to find files with location data for December 23, 2018. (J.A. 562.) He intended to “go through the applications that were installed on the phone, see which were in fact parsed by the physical analyzer and which were not, and then attempt, at least to examine those for any data that was readable to [him].” (J.A. 568.)

Knowing that photographs commonly store location data, the Examiner went to the “images” category in the physical analyzer. (J.A. 560.) “[T]raining and experience” supported the Examiner’s belief that location data are “often [a] part of photographs.” (J.A. 560.) Photographs often have “embed[ded] lat-long coordinates” “in . . . the [EXIF] data.” (J.A. 560.)

In the left pane of the viewer, the Examiner selected the “images category.” (J.A. 389, 561.) The right pane of the viewer defaulted to “thumbnail view, similar to [W]indows” containing “row after row after row of little thumbnail views of the individual pictures.” (J.A. 561.)

- d. At the start of his confirmatory search, after sorting by size for efficiency and to sort out images that would likely not have location data, an image of child pornography appeared on the Examiner’s screen.

Knowing that cell phones often contain “tens of thousands of images on nearly any device” and because “photos taken right on that device” itself would be larger than “internet [and other generated] . . . images” on the device, the Examiner “sort[ed] them [by size] so [he could] look at the larger ones first.” (J.A. 389, 561.) He did so with one click, switching from “thumbnail view” to “table view.” (J.A. 389, 561.) The amount of images seen in table view depends on “screen resolution, how big your monitor is, [and] how you have the tool adjusted.” (J.A. 582–83.)

When in table view, he intended to “sort for all photos that contain GPS and then . . . filter that with a date.” (J.A. 389, 562.) He reasoned that after he “sorted largest to smallest” he would “begin filtering,” and as he “filtered[ed,] the larger ones w[ould] stay at the top and [he would not] have to re[-]sort every time [he] appl[ied] the filter.” (J.A. 562.)

When the Examiner placed Appellant’s 200,000 photos in “table view for the columns” for sorting and filtering and “selected descending” in size from largest to smallest, he “immediately” saw an image of suspected child pornography around “the tenth picture from the top.” (J.A. 389, 392–95, 561–63.) “It was visible within [the] screen without even scrolling” and he did not manipulate the image in any way after seeing it. (J.A. 389, 392–95, 562–63, 601.)

6. After seeing the suspected child pornography image, the Examiner stopped his search, notified his Supervisor, and obtained a Search Authorization for child pornography.

When he saw the suspected child pornography, the Examiner immediately stopped the search, and notified law enforcement who requested an additional Search Authorization for Appellant’s phone. (J.A. 285–86, 389, 395, 563.) Had he not seen the image, he would have kept searching for location data. (J.A. 568.)

But the Examiner testified he “wouldn’t [have] be[en] comfortable with” continuing the search for location data “because [he] felt if [he] stumbled on something else[,] that it was going to cause complications.” (J.A. 563.) Because

of his past experience as a police officer, he felt it was better “to just stop and then let the court decide or the attorneys decide if we’re okay to go.” (J.A. 563–64.)

The Commander signed an additional Search Authorization to search Appellant’s phone and other digital devices for evidence of child pornography and related offenses. (J.A. 285–86.)

7. A later search of Appellant’s phone yielded evidence of additional misconduct.

The Defense Cyber Crime Center resumed searching Appellant’s phone and searched his other electronic devices after the Additional Search Authorization was approved. (J.A. 285–86.) The search uncovered additional misconduct including child pornography and indecent recordings. (J.A. 285–86.)

8. Appellant’s Expert Consultant testified he believed the Examiner’s second search was unreasonable.

Appellant’s Expert Consultant testified and criticized the Examiner’s second search method opining: (1) the Examiner should have used the physical analyzer to sort all data by date for December 23, 2018, instead of sorting individual file types in his second search, (J.A. 619–21, 626); (2) the Examiner should have organized photos by location data first, which would not have shown the contraband photo in plain view, (J.A. 628, 636–37); and, he claimed, (3) the Examiner’s method of sorting would not have shown the contraband on his screen in plain view and he would have had to scroll to find the image, (J.A. 638).

- C. The Military Judge denied Appellant’s Motion in a written Ruling, concluding that the Examiner’s search of Appellant’s phone was “conducted in a reasonable manner and did not exceed the scope of the [Search Authorization].”

In a written Ruling, with Findings of Fact and Conclusions of Law, the Military Judge denied Appellant’s Motion. (J.A. 673.) The Judge considered all the “evidence and arguments presented by counsel” including “the methodology proffered by the Defense expert consultant” in making his Ruling. (J.A. 674, 691.)

1. The Judge found the Examiner’s search aimed to comply with the Search Authorization when he found the child pornography.

The Military Judge found that (1) the Search Authorization permitted the Examiner “to look in any of the applications on the phone where location data from the date 23 December 2018 could be located;” (2) the Examiner’s search plan aimed to “comply with the Search Authorization” and be “efficient”; (3) after completing his review of the parsed data, “based on his training and experience,” he planned to search for unparsed location data, specifically photos he understood to contain location data; (4) after he sorted by size, one of the “first ten images, out of over 200,000,” appeared on his screen as child pornography; and (5) after viewing the image, the Examiner “immediately stopped his search,” contacted his supervisor, and received “a new Search Authorization to search the files for child pornography.” (J.A. 678–79.)

The Military Judge held: “There is 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.” (J.A. 692.)

2. The Military Judge discussed the applicable law.

The Military Judge cited Mil. R. Evid. 315(a) as the Rule governing the admissibility of search evidence obtained from Appellant’s phone. (J.A. 682.) The Military Judge also cited the application of the Fourth Amendment’s particularity requirement to electronic devices, under *Riley v. California*, 573 U.S. 373, 401–03 (2014). Citing *United States v. Richards*, 76 M.J. 365, 369–70 (C.A.A.F. 2017), the Military Judge noted “the courts have looked to what is reasonable under the circumstances” when determining whether a search was conducted within the scope of a search authorization and whether it was lawful. (J.A. 684.) The Military Judge cited Mil. R. Evid. 316(c)(5)(C) as the Rule applying to the Fourth Amendment’s plain view exception. (J.A. 683.)

3. The Military Judge concluded that the Examiner reasonably conducted a lawful search of Appellant’s phone and saw the single image of child pornography in plain view.

The Military Judge concluded the Examiner’s “search technique was reasonable, and his search methods complied with the restrictions of [the Search Authorization].” (J.A. 692.) The Military Judge pointed to the fact that the Examiner first searched “device locations” in the parsed data from Appellant’s

phone, found no relevant evidence, then searched for potentially unparsed data. (J.A. 691.) Because not all location data is necessarily captured in the “device locations” section, the Military Judge concluded that a “thorough search would require looking further than just the ‘device locations’ section.” (J.A. 691.)

The Military Judge found the Examiner formed “a plan to search the other areas of the phone . . . for potential location data . . . from 23 December 2018.” (J.A. 691.) He “opened the images category”—because “photographs are a common place to store [location] data”—switched from the thumbnail view to the table view “[i]n one mouse-click,” and sorted by size, largest to smallest because “he believed that user-taken photos might have location meta-data.” (J.A. 691.) Although the Examiner’s “plan was to next sort the images by date,” he stopped short because “[a]fter he sorted the images by size, he saw an image that he suspected to be child pornography.” (J.A. 691.)

The image was “visible within [the Examiner’s] screen without even scrolling.” (J.A. 690.) The Military Judge pointed to the fact that the image was the tenth image from the top—“not something like the 300th image out of 220,141”—as further support for the plain view exception. (J.A. 691.) Seeing the image, the Examiner “stopped his examination completely and . . . secured a [Search Authorization] to search for child pornography.” (J.A. 692.) Only then



did the Examiner begin to search for child pornography in the contents of Appellant's phone. (J.A. 692.)

On these facts, the Military Judge concluded the Examiner's search was "conducted reasonably and did not exceed the scope of the [Search Authorization]." (J.A. 692.)

The Military Judge rejected Appellant's argument that the search should have been conducted according to "the methodology proffered by [Appellant's] expert consultant" because the Examiner's search was conducted "reasonably," which is what "the Fourth Amendment [requires]." (J.A. 691.)

The Military Judge concluded Appellant's Fourth Amendment rights were not violated because the search "was conducted in a reasonable manner and within the scope of the [Search Authorization]." (J.A. 694.) During this lawful search for location data, the Examiner discovered the image of child pornography in plain view and immediately stopped the search. (J.A. 692, 694.)

D. Appellant pled not guilty to three offenses and pled guilty to the remaining offenses pursuant to a Plea Agreement, and was sentenced by the Military Judge.

Appellant pled not guilty to three offenses and guilty to all remaining Charges and Specifications pursuant to a Plea Agreement. (J.A. 697–701, 707–08.) Appellant's Plea Agreement preserved his pre-trial Motions related to the suppression of evidence obtained from the cell phone search. (J.A. 697–701.) The

Military Judge sentenced Appellant to a dishonorable discharge, reduction in paygrade to E-1, and fifty-two months confinement. (J.A. 709.)

E. The lower court affirmed the findings and sentence.

On appeal, the lower court affirmed the findings and sentence holding the Military Judge did not abuse his discretion in finding the Examiner found the contraband in plain view and did not violate Appellant's Fourth Amendment rights. *United States v. Shields*, No. 202100061, 2022 CCA LEXIS 448, at \*15–16 (N-M. Ct. Crim. App. July 27, 2022).

### **Argument**

THE MILITARY JUDGE DID NOT ABUSE HIS DISCRETION BY DENYING APPELLANT'S MOTION TO SUPPRESS. THE FORENSIC EXAMINER SEARCHED ONLY WITHIN THE SCOPE OF THE SEARCH AUTHORIZATION, CONDUCTED A REASONABLE SEARCH, FOUND AN IMAGE OF CHILD PORNOGRAPHY ON APPELLANT'S PHONE IN PLAIN VIEW, AND IMMEDIATELY STOPPED THE SEARCH.

A. The standard of review is abuse of discretion.

This Court reviews a military judge's ruling on a motion to suppress for an abuse of discretion. *United States v. Eppes*, 77 M.J. 339, 344 (C.A.A.F. 2018). An abuse of discretion occurs where the military judge's findings of fact are clearly erroneous, or where he misapprehended the law. *Id.* In reviewing a ruling on a

motion to suppress evidence, this Court “consider[s] the evidence in the light most favorable to the prevailing party.” *Id.*

B. Courts presume a search under a valid search authorization is reasonable and lawful under the Fourth Amendment.

“The Fourth Amendment protects the people against unreasonable searches and seizures and provides that warrants shall not be issued absent probable cause.” *United States v. Hoffman*, 75 M.J. 120, 123 (C.A.A.F. 2016) (citing U.S. Const. amend. IV). “The military has implemented the Fourth Amendment through [Mil. R. Evid.] 311–17.” *Id.* Mil. R. Evid. 315 allows “competent military authority to search a person or an area for specified property or evidence . . . and to seize such property or evidence” if there is probable cause “that the person, property or evidence sought is located in the place or on the person to be searched.” Mil. R. Evid. 315. “A search conducted pursuant to a warrant or search authorization is presumptively reasonable.” *Eppes*, 77 M.J. at 344.

All warrants must “particularly describ[e] the place to be searched, and the person or things to be seized.” U.S. Const. amend. IV. The warrant particularity requirement is intended to “protect against general, exploratory rummaging in a person’s belongings.” *Eppes*, 77 M.J. at 346–47 (citing *United States v. Sims*, 553 F.3d 580, 582 (7th Cir. 2009)) (citations and internal quotation marks omitted). “[I]t also serves to prevent circumvention of the requirement of probable cause by

limiting the discretion of officers executing a warrant to determine the permissible scope of their search.” *Id.*

Law enforcement must generally secure a warrant before conducting a search of data on a cell phone. *Riley*, 573 U.S. at 386. 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.” *United States v. Allen*, 53 M.J. 402, 408 (C.A.A.F. 2000).

C. Courts decline to impose *ex ante* search methodologies on search warrants or search authorizations of digital devices. The test remains reasonableness.

“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 (citing *United States v. Hill*, 459 F.3d 966, 974–77 (9th Cir. 2006)). While “warrants for computer searches must affirmatively limit the search to evidence of specific federal crimes or specific types of material,” there is also danger in “too narrowly limiting where investigators can go.” *Id.*

A search warrant should not attempt to “structure the mechanics of the search and a warrant imposing such limits would unduly restrict legitimate search objectives.” *United States v. Burgess*, 576 F.3d 1078, 1094–95 (10th Cir. 2009) (upholding warrant to search “all computer records” for drug trafficking evidence);

*see also Richards*, 76 M.J. at 365 (noting courts are “reluctan[t] to prescribe *ex ante* limitations or require particular search methods and protocols.”).

It “is unrealistic” to “prospectively restrict the scope of a search by directory, filename or extension or to attempt to structure search methods” as “illegal activity may not be advertised even in the privacy of one’s personal computer.” *Burgess*, 576 F.3d at 1093. “Keyword searches may be useful in locating suspect files, but not always.” *Id.*

Despite reluctance to prescribe search methodologies, courts still analyze the search for reasonableness. *Richards*, 76 M.J. at 370. “As always under the Fourth Amendment, the standard is reasonableness.” *Hill*, 459 F.3d at 974–77 (upholding off-site search of all defendant’s computer storage media for evidence of child pornography). Courts assess the government’s search methods after the fact “in light of the specific circumstances of each case.” *United States v. Christie*, 717 F.3d 1156, 1166 (10th Cir. 2013).

D. The Military Judge did not abuse his discretion by denying the Motion. The Examiner’s search was reasonable because (1) it was within the scope of the Search Authorization, and (2) he discovered the contraband image in plain view.

Courts determine whether a search exceeded the scope of its authorizing warrant by assessing reasonableness on a case-by-case basis. *Dalia v. United States*, 441 U.S. 238, 258 (1979). Investigators executing a warrant can look

anywhere where evidence described in the warrant might conceivably be located.

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

1. The Examiner conducted a reasonable search. He looked for unparsed location data in places the Record supports could contain that data. Nothing supports that he conducted a general search.

The majority of federal courts employ “the Fourth Amendment’s bedrock principle of reasonableness on a case-by-case basis” in that “officers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant.” *United States v. Richards*, 659 F.3d 527, 530 (6th Cir. 2011). But a digital search “may be as extensive as reasonably required to locate the items described in the warrant based on probable cause.” *Id.*

As devices and individuals have the “ability to hide, mislabel, or manipulate files” there may be “no practical substitute for actually looking in many (perhaps all)” files and locations during a search of a digital device. *Richards*, 76 M.J. at 370 (quoting *Burgess*, 576 F.3d at 1094).

“A search pursuant to a valid warrant may become an impermissible general search if [law enforcement] flagrantly disregard the limitations of the search warrant and the search unreasonably exceeded the scope of the warrant.” *United States v. Evers*, 669 F.3d 645, 652 (6th Cir. 2012) (citation and quotations omitted).

- a. A search reasonably aimed at uncovering evidence that is the subject of a warrant does not exceed the warrant's scope.

In *Richards*, a search authorization directed a forensic examiner to search all of the appellant's digital devices for "all videos, images and possible online communication" related to alleged child sexual abuse as law enforcement suspected the appellant of having an inappropriate relationship with a minor. 76 M.J. at 368. The *Richards* court upheld the search as reasonable when the examiner used a digital forensics tool to sort by file type then manually search through all photos and came upon a picture of suspected child pornography. *Id.*

The forensic tool arranged the extracted materials in folders and subfolders. *Id.* The agent started his review with "pictures" and then moved from the "attributable folder" to "folders of unattributable material" which were "unallocated or deleted material" whose "metadata" often "does not exist or is difficult to extract." *Id.* "While searching the unallocated pictures, [the agent] encountered an image that appeared to be child pornography. He stopped his search and sought an additional authorization to search for child pornography." *Id.*

The *Richards* court rejected the appellant's challenge that the warrant was overbroad, holding that authorities "were entitled to search [the appellant's] electronic media for any communication that related to his possible [crimes enumerated in the valid warrant]." *Id.* at 370. The court held that while the

“nonattributable” folder was less likely to have relevant evidence, the agent acted within the scope of the warrant because the “possibility that relevant communications could have existed” was “sufficient basis to subject those materials to an authorized and particularized search.” *Id.* at 370–71.

In *United States v. Loera*, 923 F.3d 907 (10th Cir. 2019), the court affirmed a denial of a suppression motion and held a search satisfies the Fourth Amendment when: “executing an electronic search warrant . . . [agents] discover evidence of an ongoing crime outside the scope of the warrant, so long as their search remains directed at uncovering evidence specified in that warrant.” *Id.* at 911.

The *Loera* warrant limited agents to evidence of computer fraud and one agent manually searched through all files, including photos, on several seized discs, and found child pornography. *Id.* at 912. The agent tried to use a forensic tool which would have narrowed his search, but it did not work and he resorted to manually reviewing files on the CDs. *Id.*

Affirming, the Tenth Circuit analyzed “whether the forensic steps of the search process were reasonably directed at uncovering the evidence specified in the search warrant,” and found the agent’s search reasonable. *Id.* at 912, 921–22. The court found the search reasonable despite the officer viewing the files in “thumbnail-image view to fast-track his search.” *See id.* at 912, 921–22.



Rather, the *Loera* court held that when searching digital devices where the evidence sought may be located in numerous places, the “most practical way to search [often] . . . is through an item-by-item review . . . [and t]he reasonableness of the 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.” *Id.* at 920.

In *Burgess*, a Tenth Circuit case, the search warrant authorized a search for drug-trafficking evidence and did not specify search methodology. 576 F.3d at 1083. The examiner testified he used a digital forensics tool that allows the examiner to “preview” all the image files in “thumbnail form” while he waits for the tool to create a forensic copy. *Id.* at 1084. The examiner previewed the device’s images in a “thumbnail” “gallery view” which showed several small images on his screen where he looked for pictures of narcotics. *Id.* After viewing several hundred personal photos, the examiner saw an image “depicting child sexual exploitation” and “immediately” closed the program and sought an additional warrant. *Id.* *But see Loera*, 923 F.3d at 921 (search continued after viewing child pornography reasonable as still aimed at responsive evidence).

The Tenth Circuit held the search did not exceed the warrant’s scope as the examiner did not “abandon” the search for narcotics, but kept his search in line with the content restrictions of the warrant in that he aimed to uncover narcotics evidence. *Id.* at 1093–94 (citing *United States v. Carey*, 172 F.3d 1268, 1270–83

(10th Cir. 1999) (agent exceeded scope when he looked through images and warrant limited search to content about drugs, and “plain text” file type)).<sup>1</sup>

- b. Agents exceed a warrant’s scope when they “abandon” their search to uncover evidence of crimes outside the scope of the warrant.

In *United States v. Mann*, 592 F.3d 779 (7th Cir. 2010), an examiner looking for evidence of voyeurism used a “forensic tool kit” to make a digital copy of the appellant’s devices, sort all the files by type, and organize them for the examiner to view. *Id.* at 781. The tool also flagged “known files” that were likely child pornography. *Id.* While searching through the files for voyeurism evidence, the examiner discovered child pornography, among other evidence, and then separately viewed the “known files” where he discovered “677” flagged images of child pornography. *Id.* at 781–82.

The *Mann* court held the examiner exceeded the scope when he “abandoned” his search for the evidence specified in the warrant by looking in the “known [contraband] files” which he reasonably would have known contained

---

<sup>1</sup> See also *United States v. Walser*, 275 F.3d 981, 986–87 (10th Cir. 2001) (search did not exceed warrant limited to search for content about drugs, where examiner searched audiovisual files and found child pornography); *United States v. McMahon*, 58 M.J. 362, 365–67 (C.A.A.F. 2003) (finding search did not exceed authorization’s scope for government property in the appellant’s home when agents opened binder seeking CD-ROMs and found evidence of another crime “because [a binder] was a place where CD-ROMs might reasonably be kept”).

child pornography. *Id.* at 784. But they upheld the prior search with the forensic toolkit, where he “conducted a systematic search” by sorting and organizing the files while viewing them. *Id.* at 784, 786. The Tenth Circuit explained that search was lawfully “targeted to uncovering evidence of voyeurism” and discovered “obvious” child pornography in plain view when he looked through image files using the digital tool kit. *Id.* at 786. *See also United States v. Gurczynski*, 76 M.J. 381, 384, 386–87 (C.A.A.F. 2017) (search exceeded authorization where agents conducted digital search aimed at uncovering child pornography, but warrant did not authorize that search).

- c. Like *Richards*, *Loera*, and *Burgess*, the Examiner did not exceed the authorization’s scope: his search aimed to uncover responsive evidence—location data embedded in pictures—that the physical analyzer could not identify.

The agents in *Richards*, *Loera*, and *Burgess*, conducted expansive searches lawfully because they were aimed at relevant evidence. So too here. The Examiner acted within the scope of the Search Authorization, as he reasonably limited his search to parts of the phone the Authorization permitted him to search, and he reasonably believed would contain relevant evidence. (*See* J.A. 392–95, 398–400, 552–69, 678–79, 692.)

Like the agents in those cases, the Examiner did not “abandon” his search for responsive evidence. *Burgess* 576 F.3d at 1093–94. When he used a digital tool to organize images so he could search for unparsed location data, he had

“sufficient basis” based on his training, education, and experience that there was a “possibility that relevant [evidence] could have existed” in those places. *Compare Richards*, 76 M.J. at 368, 370, and *Burgess* 576 F.3d at 1093–94, with (J.A. 392–95, 398–400, 552–69).

The Examiner acted reasonably based on his knowledge that (1) “a physical analyzer can only parse so much of [a phone’s data],” (J.A. 557); (2) location and date data were often not fully parsed, (J.A. 591–92); and (3) the only way he could identify whether that unparsed data contained relevant location data for the warrant was by reviewing the data himself, (J.A. 560, 562, 591–92).

A high likelihood existed that Appellant’s iPhone photos contained relevant unparsed location data, because: (1) “[p]ictures are constantly being generated by apps while the iPhone is in use,” (J.A. 398–99); (2) photos contain “embed[ded] lat-long coordinates,” (J.A. 560); and (3) the physical analyzer often “display[s] incorrect date information” for pictures, (J.A. 399).

The Examiner acted reasonably when choosing to do manual review, because: (1) the considerable amount of data in a phone coupled with the wide scope of the warrant necessitated “manual review,” (J.A. 398); (2) only “actual forensic analysis” of “[u]nparsed app data” could identify relevant evidence, (J.A. 398); and (3) “[w]ithout manual verification, an examiner would not be able to

accurately state that all location data, especially within apps, was reviewed for relevance,” (J.A. 398).

- d. No evidence supports that the Examiner exceeded the scope of the Search Authorization in sorting by size or that he scrolled through Appellant’s images, and Appellant fails to point to any.

Unlike the agents in *Mann* or *Gurczynski*, who abandoned searches for relevant evidence and sought for evidence of other crimes not authorized by the warrant, the Examiner here stayed within the Search Authorization’s scope by targeting only relevant evidence. (J.A. 392–95, 398–400, 552–69.)

Appellant’s argument that no “realistic probability” existed that the Examiner would find responsive evidence is belied by the Record, including testimony and Affidavits from the Examiner and his Supervisor. *See* (Appellant’s Br. at 26; J.A. 392–95, 398–400, 552–69); *see also supra* Section D.1.c.

Likewise, Appellant’s argument the Examiner exceeded the warrant’s scope by “scrolling” through Appellant’s images fails because: (1) it is unsupported by the Record—the Examiner saw the child pornography on his screen “immediately” after sorting by size, (J.A. 392–95, 561–63); (2) the Examiner’s screen and tool setup made the image visible on his screen—unlike the setup used by Appellant’s expert, (J.A. 561, 582–83); and (3) the Examiner’s “actual forensic analysis” necessarily required him to look and select images on his screen to view their data for possible evidence, (J.A. 398).

Contrary to Appellant’s arguments, the Judge considered all the “evidence and arguments presented by counsel” and “the methodology proffered by the Defense expert consultant” in making his Ruling. (J.A. 674, 691; Appellant’s Br. at 31–32.) He acted within his discretion to give greater weight to the Examiner’s testimony than the Appellant’s Expert. *Cf. United State v. Mann*, 54 M.J. 164, 167 (C.A.A.F. 2000) (noting “the military judge was able to sort through the evidence, weigh it, and give it appropriate weight”).

Moreover, Appellant’s reliance on *United States v. Solomon*, 72 M.J. 176 (C.A.A.F. 2013), is inapt. (Appellant’s Br. at 31.) There, a judge abused his discretion when he admitted Mil. R. Evid. 413 evidence but “altogether failed to mention or reconcile [the appellant’s] important alibi evidence and gave little or no weight” to his previous acquittal. *Id.* at 180.

Here, in contrast, the Military Judge considered the “the Defense expert consultant[’s]” proffer and all “evidence and arguments presented by counsel” in deciding to rely on the Examiner’s consistent account of finding the child pornography “immediately” on his screen without scrolling. (J.A. 394–95, 562–63, 674, 691.) Appellant fails to show any evidence ignored by the Military Judge.

- e. Appellant misapplies *Garrison*: the Examiner conducted a search tailored to uncover relevant evidence.

“The scope of a lawful search is defined by the object of the search and the places in which there is probable cause to believe that it may be found. Just as

probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom.” *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

In *Garrison*, police officers executing a warrant mistakenly searched the wrong apartment and found narcotics in plain view. *Id.* at 81. Despite the error, the Court held the appellant’s Fourth Amendment rights were not violated because the officers reasonably believed they were searching the correct location. *Id.* at 88. In finding the search reasonable, the *Garrison* Court relied on: (1) the warrant’s validity; and, (2) the reasonable execution of the warrant, considering law enforcement’s “conduct in light of the information available to them at the time they acted.” *Id.* at 84.

Here, like the agents in *Garrison*, the Examiner reasonably relied on the “information available to [him] at the time [he] acted” when he tailored his search to find responsive evidence, unparsed location data for the subject date, in the phone’s images based on his training, education, and experience. 480 U.S. at 84; (J.A. 392–95, 398–400, 552–69). Nothing in the Record supports the notion he searched irrelevant areas of the phone akin to Appellant’s “lawnmower . . . in the upstairs bedroom” analogy or that he went into an unauthorized area like the *Garrison* officers. (Appellant’s Br. at 26.)

His argument fails.

2. The Examiner reasonably searched for unparsed location data—consistent with evidence about where that kind of data might be—when he sorted image files from largest to smallest.

“[A]n officer executing a search warrant [must] first look in the most obvious places and as it becomes necessary to progressively move from the obvious to the obscure.” *Burgess*, 576 F.3d at 1094. “[A] search protocol which structures the search by requiring an analysis of the file structure, next looking for suspicious file folders, then looking for files and types of files most likely to contain the objects of the search by doing keyword searches” aligns with the Fourth Amendment. *Id.*

“[I]n the end, there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders, and that is true whether the search is of computer files or physical files.” *Richards*, 76 M.J. at 370 (quoting *Burgess*, 576 F.3d at 1094); *see also Loera*, 923 F.3d at 920-21 (“reasonableness” of search for required information on digital devices evolves as search proceeds and searching officer learns about particular device and files on it).

- a. Courts do not require specific search protocols for digital searches.

Generally, courts do not require examiners to follow particular search protocols when searching digital devices, but look at the Fourth Amendment’s foundational requirement of a reasonable search under the circumstances based



upon a warrant supported by probable cause. *See Richards*, 76 M.J. at 369 (upholding agent’s unfiltered search through images for child abuse and finding contraband).<sup>2</sup>

In *United States v. Giberson*, 527 F.3d 882, 885 (9th Cir. 2008), the court upheld an examiner’s search using a digital forensics tool that showed all of the appellant’s images in thumbnail format while he searched for evidence the appellant produced fake identification cards. *Id.* at 882–85. There, the examiner used a “software package” that pulls computer files based on file type and organizes similar file types into separate folders. *Id.* at 885. After sorting all the files, the examiner used another tool so he could “view more thumbnail[s] of graphic images on the screen at a time, making his search more efficient.” *Id.*

---

<sup>2</sup> *See also United States v. Stabile*, 633 F.3d 219, 240 (3d Cir. 2011) (upholding unfiltered search for financial crimes evidence in appellant’s computer files where officers discovered child pornography); *United States v. Williams*, 592 F.3d 511, 521–24 (4th Cir. 2010) (upholding unfiltered search where officer discovered child pornography during warrant-authorized search of appellant’s computer for evidence of “making threats and computer harassment”); *United States v. Mann*, 592 F.3d 779 (7th Cir. 2010) (search through files for voyeurism uncovered child pornography) *United States v. Miranda*, 325 F. App’x 858, 859–60 (11th Cir. 2009) (per curiam) (unpublished) (upholding unfiltered search because officer had “lawful right to view each file to determine whether or not it was evidence of” subject crimes and discovered contraband); *United States v. Wong*, 334 F.3d 831, 834 (9th Cir. 2003) (upholding unfiltered search through computer image files where officer discovered child-pornography during warrant-authorized search of appellant’s computer for “maps”).

While scrolling through the images looking for relevant evidence, he came upon child pornography. *Id.*

That court rejected the appellant’s argument that the examiner should have more narrowly limited his search method. *Id.* at 889. The examiner’s search was reasonable, and more tailored search protocols were unnecessary because “whether deliberate or inadvertent . . . [relevant evidence] can be hidden in all manner of files” and “[t]here was no reasonable way to sort relevant and irrelevant graphics files because the fake I.D. files and the pornography files were innocuously labeled.” *Id.* at 889–90.

- b. The Examiner reasonably started the search sorting by size, as user-generated photos with location data would likely be the largest images. Evidence supported that photos taken by Appellant would likely have unparsed location data responsive to the Search Authorization. Tailoring his search, the Examiner’s search was more limited than the lawful but un-tailored searches in *Richard, Giverson, Loera, and Burgess.*

The agents in *Richards, Giberson, Loera, and Burgess*, did not tailor their searches, but conducted lawful searches, viewing image files where they reasonably expected to uncover relevant evidence. The Examiner here went further, tailoring his search to target user-generated images that were likely to contain embedded location data that the tool did not identify and parse; and, thus the location data could only be found through “actual forensic analysis.” (J.A. 392–95, 398–400, 552–69.)

The Examiner reasonably chose to first sort images by size because: (1) he had to find relevant evidence in the 215,767 images identified on Appellant’s phone, (J.A. 388); (2) sorting by size would bring user-generated images to the top which were more likely to contain location data, (J.A. 561); (3) this method would send irrelevant internet generated images, which would not contain location data, to the bottom, (J.A. 561); and (4) he sorted by size first to save time because then the larger, relevant images “will stay at the top and [he would not] have to resort every time [he] appl[ied] [a new] filter” for location data or date data. (J.A. 562.)

The Examiner’s next steps of sorting images for “location” data and then “date” data were logically aimed at narrowing the images down to those that would most likely contain unparsed location data and date data which he would then review to determine if they were relevant to the warrant. (J.A. 562.) Importantly, he did not reach these steps because he “immediately” saw child pornography on his screen after sorting by size. (J.A. 389, 392–95, 561–63.)

Appellant’s argument that the Examiner violated the Fourth Amendment by claiming the Examiner had no “reasonable basis” for his method and “[s]orting the images by size did nothing to advance [his] search” fails. (Appellant’s Br. at 24, 26.) Under Appellant’s proposed regime, forensic examiners would only be able to use digital tools to search in certain ways—despite that those digital tools frequently fail to parse all information on digital devices; Appellant would thus

seem to further prohibit any “actual forensic analysis” beyond the limited use of, for example, the “filter by date” operation in the digital tool. (J.A. 398.)

But that approach is inconsistent with at least eight federal circuits and this Court, which all permit human forensic analysis of digital files when aimed at uncovering relevant evidence.<sup>3</sup>

That argument is unsupported by the law or the Record.

---

<sup>3</sup> See *United States v. Ulbricht*, 858 F.3d 71, 103 (2d Cir. 2017) (upholding digital search where agents “open[ed] or cursorily read[] the first few pages of files to determine their precise contents to determine what was relevant”); *United States v. Stabile*, 633 F.3d 219, 237, 240 (3d Cir. 2011) (permitting “further investigation” of files involving manual review because evidence “could be hidden within”); *United States v. Williams*, 592 F.3d 511, 521–23 (4th Cir. 2010) (authorizing digital device search for evidence of crime necessarily included “at least a cursory review of each file on the computer” to “determine whether any one falls within the terms of the warrant” “albeit only momentarily”); *United States v. Richards*, 659 F.3d 527, 540–41 (6th Cir. 2011) (holding investigators can “open the various types of files located in the computer's hard drive in order to determine whether they contain [relevant] evidence”); *United States v. Mann*, 592 F.3d 779 (7th Cir. 2010) (allowing manual review of files sorted by digital tool); *United States v. Wong*, 334 F.3d 831, 834 (9th Cir. 2003) (upholding manual review of multiple digital devices in search for data for “maps and writings” related to a specific location); *United States v. Burgess*, 576 F.3d 1078, 1094–95 (10th Cir. 2009) (upholding preview of all image files as “thorough search” for relevant evidence of drug trafficking); *United States v. Miranda*, 325 F. App'x 858, 859–60 (11th Cir. 2009) (per curiam) (unpublished) (upholding unfiltered search because officer had “lawful right to view each file to determine whether or not it was evidence of” subject crimes); *United States v. Richards*, 76 M.J. 365, 370–71 (C.A.A.F. 2017) (upholding search of individual files in “unallocated space” when looking through an images file folder).

- c. The Examiner reasonably began searching in “obvious” places and moved to “obscure” places when looking for location data. Appellant’s argument to the contrary fails.

As the Tenth Circuit discussed in *Loera* and *Burgess*, the Examiner’s search method complied with the Fourth Amendment when he went from the “obvious to the obscure” by first looking for parsed location data for the subject date using the physical analyzer. (J.A. 557, 559.) Only then, after failing to find parsed location data, did he proceed to the next most likely place for relevant evidence.

That next most likely place was places that were likely to contain unparsed location data, including large images taken by Appellant with the phone, which might have embedded location data that could not be parsed by the physical analyzer. *See Burgess*, 576 F.3d at 1094; (J.A. 392–95, 398–400, 552–69, 578, 591–593.)

Contrary to Appellant’s argument, but as in *Loera*, the Search Authorization did not limit the type of file to be searched, but only limited the Examiner to search for “all location data stored on the phone or within any application within the phone for 23Dec18.” (J.A. 53; Appellant’s Br. at 24–25.) The Examiner reasonably relied on his training, education, and experience to conclude the small number of results in the “device locations” category likely meant the tool had not “parse[d] the entire device” for location data and dates. (J.A. 557, 559–60, 566.)

The Examiner searched in an authorized location for relevant evidence, and Appellant’s argument to the contrary fails. (Appellant’s Br. at 25.)

3. The Military Judge’s Findings of Fact were supported by the Record. Appellant fails to show his Findings were clearly erroneous.

“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) (citation and quotations omitted). “This standard requires more than just [this Court’s] disagreement with the military judge's decision.” *United States v. Bess*, 75 M.J. 70, 73 (C.A.A.F. 2016).

- a. The Examiner’s search did not amount to a general search prohibited under the Fourth Amendment, and Appellant fails to show the Examiner “rummaged through unauthorized areas of the cell phone.”

The Fourth Amendment was a “response to the reviled ‘general warrants’ and ‘writs of assistance’ of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.” *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018).

The Search Authorization permitted the Examiner to search “all location data stored on the phone or within any application within the phone for 23Dec18,” (J.A. 53); and he had a reasonable belief that large images could contain relevant

unparsed data, (J.A. J.A. 392–95, 398–400, 552–69, 578, 591–593). No evidence supports the Examiner’s search ever devolved into “an unrestrained search for evidence of criminal activity.” *Carpenter*, 138 S. Ct. at 2213; (Appellant’s Br. at 27, 38, 40).

Appellant fails to show the Military Judge’s Finding that the Examiner “was [not] rummaging through unauthorized areas of the iPhone” was clearly erroneous; instead, he merely disagrees with the Military Judge’s Finding. (Appellant’s Br. at 27); *Bess*, 75 M.J. at 73.

Instead, like the agents in *Loera*, *Burgess*, and *Richards* lawfully searched through large quantities of image files when they believed they could find relevant evidence, so too here.

- b. Appellant fails to show the Examiner did not intend to “next sort the images by date” or did not see the contraband while sorting the images. He also fails to show how the Examiner went outside “the scope of the CASS.”

The Examiner testified that before he could conduct any further sorting or analysis, and “immediately” after he sorted by size, child pornography appeared on his screen. (Appellant’s Br. at 28–29; J.A. 392–95, 561–63.) Regardless of the order of his next steps, which he was never able to take, he aimed to conduct forensic analysis in a location he reasonably believed would contain unparsed location data. Nothing in the Record supports Appellant’s unfounded speculation

that the Examiner was rummaging through Appellant’s thousands of images; rather he only saw one page of thumbnail-sized images midway through his sorting process. (Appellant’s Br. at 27–28; J.A. 389, 561.)

Appellant fails to show there is “no evidence” to support the Judge’s Findings or that “the entire evidence” leaves this Court “with the definite and firm conviction that a mistake has been committed.” *Criswell*, 78 M.J. at 141. Thus, Appellant fails to show the Military Judge’s Findings of Fact were clearly erroneous.

E. The Military Judge did not abuse his discretion by finding the contraband images admissible under the plain view doctrine.

1. The plain view doctrine permits the admissibility of evidence of additional illegality discovered during a lawful search.

Evidence may be seized when “[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.” Mil. R. Evid. 316(c)(5)(C).

“Law enforcement officials conducting a lawful search may seize items in plain view if [the officials] are acting within the scope of their authority, and . . . they have probable cause to believe the item is contraband or evidence of a crime.” *United States v. McMahon*, 58 MJ 362, 367 (C.A.A.F. 2003) (citation and internal quotation marks omitted).



“[I]n order for the 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.” *Richards*, 76 M.J. at 371 (citing *Horton v. California*, 496 U.S. 128, 136–37 (1990)). The extension of the original search justification applies only where it is immediately apparent law enforcement have evidence before them, and “may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges.” *Horton*, 496 U.S. at 135.

2. The contraband was lawfully discovered in plain view because the Examiner (1) was acting under a valid Search Authorization, (2) immediately saw the image and stopped his search, and (3) was lawfully in the location where he saw the image because he believed he would find relevant evidence.

In *Richards*, agents investigating the appellant for child sex abuse had an authorization to search his computer for related “images and possible online communication.” 76 M.J. at 367. While searching through the extracted data sorted by a digital tool into “attributable” and “unattributable” folders for images, an agent saw a child pornography image. *Id.* at 368.

The court held that “discovery of the child pornography images within the folder of unallocated materials” was consistent with “the plain view exception to the Fourth Amendment” because the agent was lawfully searching through the files

based on a valid warrant until he came upon what “appeared to be” child pornography. *Id.* at 371.

Here, like the judge in *Richards* did not abuse his discretion when finding plain view applied in a similar scenario, this Military Judge did not abuse his discretion in finding the plain view doctrine compels admission of the child pornography image. This is true for at least three reasons.

First, the Examiner acted under a valid Search Authorization when he looked through Appellant’s photos. (J.A. 53.) Appellant does not challenge the Search Authorization’s validity here, and did not challenge it at the lower court. (*See* Appellant’s Br. At 24, Oct. 18, 2021.)

Second, after sorting by size in the physical analyzer’s table view, the Examiner “immediately noticed” the child pornography image on his screen without scrolling. (J.A. 394–95, 562–63.)

Third, the Forensic Examiner had lawful access to the object itself through complying with the Search Authorization. (*Id.*) As the Military Judge correctly ruled, the resulting child pornography image was in plain view and is admissible. (*See* J.A. 691–92, 694.)

Appellant’s argument that the Examiner was not in a lawful place to view the child pornography fails because the Examiner’s search aligned with the Search Authorization. (Appellant’s Br. at 36); *see supra* Sections D.1.b–d, 2.b–c.

The Military Judge did not abuse his discretion denying Appellant’s Motion to suppress the child pornography image: (1) the Examiner conducted his search in accordance with a valid search authorization; (2) the search was reasonable under the circumstances; and, (3) the contraband was in plain view. (J.A. 53, 394–95, 562–63.)

3. Appellant’s arguments that the Military Judge misunderstood the law or should be afforded less deference are inapt because he applied the correct law to facts supported by the Record. He found the Examiner did not scroll through images because the Record supports that conclusion.

This Court does “not expect record dissertations but, rather, a clear signal that the military judge applied the right law. While not required, where the military judge places on the record his analysis and application of the law to the facts, deference is clearly warranted.” *United States v. Flesher*, 73 M.J. 303, 311–12 (C.A.A.F. 2014) (quoting *United States v. Downing*, 56 M.J. 419, 422 (C.A.A.F. 2002)).

In *Flesher*, a judge received less deference when he, among other things, failed to address the *Houser* factors in a *Daubert* hearing, provide any findings of fact, or apply the law to the facts. 73 M.J. at 312.

Here, unlike *Flesher*, this Judge’s Ruling deserves deference because he applied the correct law to the facts and concluded the Examiner found the child pornography on his screen in plain view without scrolling. (J.A. 674, 690–92;

Appellant’s Br. at 32–34.) The Judge was within his discretion in relying on the Examiner’s testimony on how he discovered the child pornography over Mr. Peden’s speculative testimony as the Examiner explained the amount of images visible in physical analyzer depends on the user’s screen size, which he explained his displayed at least ten rows. (J.A. 561, 582–83; Appellant’s Br. at 33–34.)

The Military Judge’s Ruling deserves deference and he did not abuse his discretion.

F. Even assuming the Military Judge abused his discretion, Mil. R. Evid. 311(a)(3) does not support exclusion.

1. Exclusion of evidence is required only when it would deter future unlawful searches that were the result of deliberate police misconduct.

“Evidence derivative of an unlawful search, seizure, or interrogation is commonly referred to as the ‘fruit of the poisonous tree’ and is generally not admissible at trial.” *United States v. Conklin*, 63 M.J. 333, 334 (C.A.A.F. 2006) (citing *Wong Sun v. United States*, 371 U.S. 471, 488 (1963)).

The Military Rules of Evidence generally prohibit admission of evidence obtained as a result of an unlawful search or seizure if “exclusion of the evidence results in appreciable deterrence of future unlawful searches or seizures and the benefits of such deterrence outweigh the costs to the justice system.” Mil. R. Evid. 311(a). It is “designed to safeguard Fourth Amendment rights generally through

its deterrent effect, rather than a personal constitutional right of the party aggrieved.” *United States v. Leon*, 468 U.S. 897, 906 (1984).

To warrant exclusion, “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.” *Herring v. United States*, 555 U.S. 135, 144 (2009). “When the police exhibit deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to outweigh the resulting costs.” *United States v. Davis*, 564 U.S. 229, 238 (2011) (citing *Herring*, 555 U.S. at 144) (internal quotations omitted).

When police conduct “involves only simple, ‘isolated’ negligence . . . the ‘deterrence rationale loses much of its force,’ and exclusion cannot ‘pay its way.’” *Davis*, 564 U.S. at 238–39 (internal quotations and citations omitted). Society must swallow the “bitter pill” of exclusion only as a last resort. *Id.* at 237.

2. There is no evidence law enforcement deliberately disregarded Appellant’s rights or that exclusion would deter improper conduct, so the exclusionary rule does not apply.

In *Eppes*, agents exceeded the search authorization when they searched the appellant’s bags despite only being authorized to search his person. 77 M.J. at 347. There, the affidavit included probable cause grounds to search the appellant’s bags, but the judge did not include it in the authorization likely as a result of a

“scrivener’s error.” *Id.* While ultimately relying on the inevitable discovery doctrine, the *Eppes* court held there was “no valid policy reason for applying the exclusionary rule” as “the Fourth Amendment violation was likely not the result of deliberate misconduct in need of deterrence [and] any marginal deterrent benefit to be gained is far outweighed by the heavy costs exclusion would have—namely placing the Government in a worse position than it would have been had the illegality not occurred.” *Id.* at 349.

Here, the exclusionary rule does not apply for at least three reasons. First, there is no evidence law enforcement deliberately disregarded Appellant’s Fourth Amendment rights. Here, like the scrivener’s error in *Eppes*—which did not reflect a deliberate disregard for the appellant’s rights—the Examiner’s search was at worst isolated negligence not warranting exclusion. *Davis*, 564 U.S. at 238–39. The Examiner’s search protocols were consistent with his training, education, and experience in law enforcement. (J.A. 552–69, 578, 591–593.) His supervisor agreed his search methods were sound, and they both believed the search abided by the terms of the Search Authorization. (J.A. 392–95, 398–400.) Appellant’s contention that the Examiner’s search for relevant evidence somehow amounts to a “grossly negligent disregard” of the Fourth Amendment warranting exclusion is unsupported by the law or Record. *See Davis*, 564 U.S. at 238–39; *supra* Sections D.1.b–d, 2.b–c; (Appellant’s Br. at 37–40).

Second, no evidence supports that exclusion would deter future misconduct. *See* Mil. R. Evid. 311(a)(3). Here, like in *Eppes*, there is “no valid policy reason for applying the exclusionary rule” because the Examiner conducted a search in line with this Court’s law and the majority of federal circuits for how to conduct a reasonable search under the Fourth Amendment. 77 M.J. at 349; *see supra* Section D.2.d. Thus, his organization’s policies were lawful, and any exclusion lacks deterrent value. *Leon*, 468 U.S. at 906. Appellant’s argument the Examiner’s organization engaged in “systemic negligence” by conducting forensic analysis fails. (Appellant’s Br. at 38–39.)

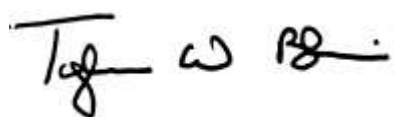
Lastly, any negligence does not warrant the high price to the justice system by excluding evidence. *See* Mil. R. Evid. 311(a)(3). Unlike in *Eppes*, where the agents clearly exceeded the authorization’s scope, nothing shows the Examiner’s actions were “sufficiently culpable” to warrant the high “price paid by the justice system”—excluding evidence of Appellant’s indecent recordings and possession of child pornography. *Herring*, 555 U.S. at 144; (J.A. 19–20).

As the Military Judge found, the Examiner’s search did not aim to violate Appellant’s rights, his conduct was reasonable in conforming his search to a valid search authorization, and therefore the exclusionary rule does not apply. (*See* J.A. 693–94.)

When “considering the evidence in the light most favorable to the prevailing party,” the Military Judge did not abuse his discretion by finding the Examiner did not violate Appellant’s Fourth Amendment rights. *Eppes*, 77 M.J. at 344.

### Conclusion

The United States respectfully requests this Court affirm the lower court’s decision.



TYLER W. BLAIR  
Captain, U.S. Marine Corps  
Appellate Government Counsel  
Navy-Marine Corps Appellate  
Review Activity  
Bldg. 58, Suite B01  
1254 Charles Morris Street SE  
Washington Navy Yard, DC 20374  
(202) 685-7433  
Bar no. 37601



GREGORY A. RUSTICO  
Lieutenant, JAGC, U.S. Navy  
Senior Appellate Counsel  
Navy-Marine Corps Appellate  
Review Activity  
Bldg. 58, Suite B01  
1254 Charles Morris Street SE  
Washington Navy Yard, DC 20374  
(202) 685-7686  
Bar no. 37338



JOSEPH M. JENNINGS  
Colonel, U.S. Marine Corps  
Director, Appellate Government  
Navy-Marine Corps Appellate  
Review Activity  
Bldg. 58, Suite B01  
1254 Charles Morris Street SE  
Washington Navy Yard, DC 20374  
(202) 685-7427, fax (202) 685-7687  
Bar no. 37744



BRIAN K. KELLER  
Deputy Director  
Appellate Government  
Navy-Marine Corps Appellate  
Review Activity  
Bldg. 58, Suite B01  
1254 Charles Morris Street SE  
Washington Navy Yard, DC 20374  
(202) 685-7682, fax (202) 685-7687  
Bar no. 31714

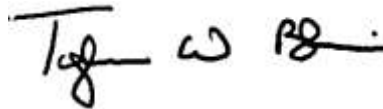


### **Certificate of Compliance**

1. This brief complies with the type-volume limitation of Rule 24(c) because this brief contains 10120 words.
2. This brief complies with the typeface and type style requirements of Rule 37 because this brief was prepared in a proportional typeface using Microsoft Word Version 2016 with 14-point, Times New Roman font.

### **Certificate of Filing and Service**

I certify that I delivered the foregoing to the Court and served a copy on opposing counsel on February 3, 2023.

A handwritten signature in black ink, appearing to read "Tyler W. Blair". The signature is written in a cursive style with a horizontal line above the first name.

TYLER W. BLAIR  
Captain, U.S. Marine Corps  
Appellate Government Counsel

[United States v. Miranda](#)

United States Court of Appeals for the Eleventh Circuit

May 6, 2009, Decided; May 6, 2009, Filed

No. 08-10987 Non-Argument Calendar

**Reporter**

325 Fed. Appx. 858 \*; 2009 U.S. App. LEXIS 9833 \*\*

UNITED STATES OF AMERICA,  
Plaintiff-Appellee, versus DAVID  
MIRANDA, Defendant-Appellant.

**Notice:** PLEASE REFER TO FEDERAL  
RULES OF APPELLATE PROCEDURE  
RULE 32.1 GOVERNING THE  
CITATION TO UNPUBLISHED  
OPINIONS.

**Subsequent History:** US Supreme Court  
certiorari denied by [Miranda v. United  
States, 2009 U.S. LEXIS 8639 \(U.S., Nov.  
30, 2009\)](#)

**Prior History:** [\*\*1] Appeal from the  
United States District Court for the Middle  
District of Florida. D. C. Docket No. 06-  
00004-CR-T-26-TGW.

**Disposition:** AFFIRMED.

**Counsel:** For David Miranda, Appellant:  
Craig L. Crawford, Federal Public  
Defender, Federal Public Defender's Office,  
ORLANDO, FL; Donna Lee Elm, Federal  
Public Defender, TAMPA, FL; Walter Ruiz,  
AFPD, Federal Public Defender,  
Clearwater, FL.

For United States of America, Appellee:  
Patricia D. Barksdale, JACKSONVILLE,  
FL; Linda Julin McNamara, U.S. Attorney's  
Office, TAMPA, FL.

**Judges:** Before TJOFLAT, DUBINA and  
BLACK, Circuit Judges.

**Opinion**

---

[\*859] PER CURIAM:

David Miranda appeals his convictions for possession of child pornography, in violation of [18 U.S.C. § 2252A\(a\)\(5\)\(B\), \(b\)\(2\)](#). The district court granted Miranda's motion to suppress evidence pertaining to child pornography as to his computer tower but denied it with regard to his laptop computer, external hard drive, and uninstalled hard drive.

We review "a district court's denial of a motion to suppress [as] a mixed question of law and fact." [United States v. Smith, 459 F.3d 1276, 1290 \(11th Cir. 2006\)](#). We review the district court's findings of fact for clear error, construing the facts in the light most favorable to the prevailing party [\*\*2] below, and its application of the law *de novo*. *Id.* The evidence brought forth at trial can be considered in determining whether the denial of a motion to suppress constitutes reversible error. [United States v. Newsome, 475 F.3d 1221, 1224 \(11th Cir.\)](#), *cert. denied, 128 S. Ct. 218, 169 L. Ed. 2d*

168 (2007).

I.

On appeal, Miranda argues the police violated the [Fourth Amendment's](#) Warrant Clause by searching his computer for information outside the scope of the warrant, which was limited to searching for evidence of counterfeit software. He relies on *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999), to contend that the pornographic images on his computer were in closed files, and thus, were not within plain view. Further, Miranda asserts: (1) the police had a warrant to search for something other than child pornography; [\*860] (2) the searching officer noticed files with sexually suggestive names, unrelated to the reason for initiating the search; and (3) the officer abandoned his original search to open additional files, without obtaining a second search warrant, based on a reasonable suspicion that the additional files might contain child pornography.

Pursuant to the [Fourth Amendment](#), search warrants must "particularly [\*\*3] describe the place to be searched, and the persons or things to be seized" in order to "protect individuals from being subjected to general, exploratory searches." [United States v. Khanani](#), 502 F.3d 1281, 1289 (11th Cir. 2007) (internal quotations omitted). However, the particularity requirement of the [Fourth Amendment](#) must be applied with a practical margin of flexibility, taking into account the nature of the items to be seized and the complexity of the case under investigation. See [United States v. Wuagneux](#), 683 F.2d 1343, 1349 (11th Cir.

[1982](#)). When a warrant authorizes the seizure of documents, "an officer acting pursuant to such a warrant is entitled to examine any document he discovers," in order to "to perceive the relevance of the documents to the crime." [United States v. Slocum](#), 708 F.2d 587, 604 (11th Cir. 1983). Moreover, "[i]n searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." [Andresen v. Maryland](#), 427 U.S. 463, 96 S. Ct. 2737, 2749 n. 11, 49 L. Ed. 2d 627 (1976).

"The 'plain view' doctrine permits a warrantless seizure where (1) an officer is lawfully located [\*\*4] in the place from which the seized object could be plainly viewed and must have a lawful right of access to the object itself; and (2) the incriminating character of the item is immediately apparent." [Smith](#), 459 F.3d at 1290 (citing [Horton v. California](#), 496 U.S. 128, 110 S. Ct. 2301, 2308, 110 L. Ed. 2d 112 (1990)). "An example of the applicability of the 'plain view' doctrine is the situation in which the police have a warrant to search a given area for specified objects, and in the course of the search come across some other article of incriminating character." *Id.* (internal quotations omitted) (quoting [Horton](#), 110 S. Ct. at 2307). Of course, the officers "must have probable cause to believe the object in plain view is contraband." *Id.*

In this case, the searching officer was searching Miranda's hard drives pursuant to

a warrant. In doing so, the officer had a lawful right to view each file to determine whether or not it was evidence of counterfeiting crimes. See [Slocum, 708 F.2d at 604](#). The child pornography files were intermingled with counterfeiting files, so they were in plain view. Once the officer saw child pornography on Miranda's hard drives, its incriminating character was immediately apparent, so the officer [\*\*5] could seize the files. See [Smith, 459 F.3d at 1290](#). This is distinguishable from the child pornography found on Miranda's computer tower, which the district court suppressed because it was found during a search conducted solely for the purpose of finding child pornography, outside the scope of the counterfeiting warrant. For these reasons, the district court did not err in denying Miranda's motion to suppress the child pornography found on his laptop computer, external hard drive, and uninstalled hard drive.

## II.

Miranda also argues the district court erred in refusing to exclude timestamp evidence obtained from the external hard drive and uninstalled hard drive. Specifically, he argues this evidence was "fruit of the poisonous tree" because the [\*861] information originated from the computer tower's internal timing mechanism, and evidence pertaining to the computer tower was suppressed by the district court.

In addition to the illegally obtained evidence, a court may suppress incriminating evidence that was derived from that primary evidence as "fruit of the

poisonous tree." [United States v. Terzado-Madruga, 897 F.2d 1099, 1112-13 \(11th Cir. 1990\)](#). When determining whether evidence is "fruit [\*\*6] of the poisonous tree" and therefore must be excluded, the relevant question is "whether, granting establishment of the primary illegality, the evidence to which instant objection is made has been come at by exploitation of that illegality or instead by means sufficiently distinguishable to be purged of the primary taint." [Wong Sun v. United States, 371 U.S. 471, 83 S. Ct. 407, 417, 9 L. Ed. 2d 441 \(1963\)](#) (internal quotations omitted). The government can establish that evidence has been "purged of the primary taint" by showing that the evidence was discovered from an independent source, would have been discovered inevitably by lawful means, or was so attenuated from the illegality "as to dissipate the taint" of the unlawful conduct. [Terzado-Madruga, 897 F.2d at 1113](#). Under the "independent source" doctrine, the challenged evidence is admissible if it was obtained from a lawful source, independent of the illegal conduct. *Id.*

Here, the district court granted Miranda's motion to suppress child pornography found on his computer tower but declined to suppress the actual computer tower, as it was lawfully seized pursuant to a search warrant. The time-stamp evidence was unrelated to the suppressed child pornography because [\*\*7] it was derived from the internal timing mechanism in the computer tower, a lawful source. For these reasons, the district court did not err by denying Miranda's motion to suppress the

time-stamp evidence.

**AFFIRMED.**

---

End of Document

[United States v. Shields](#)

United States Navy-Marine Corps Court of Criminal Appeals

June 21, 2022, Argued; July 27, 2022, Decided

No. 202100061

**Reporter**

2022 CCA LEXIS 448 \*; 2022 WL 2966378

UNITED STATES, Appellee v. Ethan R. SHIELDS, Staff Sergeant (E-6), U.S. Marine Corps, Appellant

**Notice:** THIS OPINION DOES NOT SERVE AS BINDING PRECEDENT, BUT MAY BE CITED AS PERSUASIVE AUTHORITY UNDER NMCCA RULE OF APPELLATE PROCEDURE 30.2.

**Subsequent History:** Petition for review filed by [United States v. Shields, 2022 CAAF LEXIS 659, 2022 WL 5209539 \(C.A.A.F., Sept. 15, 2022\)](#)

Review granted by [United States v. Shields, 2022 CAAF LEXIS 809 \(C.A.A.F., Nov. 10, 2022\)](#)

Motion granted by [United States v. Shields, 2022 CAAF LEXIS 925, 2022 WL 18277250 \(C.A.A.F., Dec. 9, 2022\)](#)

Motion granted by [United States v. Shields, 2023 CAAF LEXIS 35 \(C.A.A.F., Jan. 18, 2023\)](#)

**Prior History:** [\*1] 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.

**Counsel:** For Appellant: Lieutenant Commander Daniel O. Moore, JAGC, USN.

For Appellee: Major Clayton L. Wiggins, USMC; Captain Tyler W. Blair, USMC.

**Judges:** Before GASTON, HOUTZ, and MYERS Appellate Military Judges.

**Opinion**

---

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].<sup>1</sup> Appellant asserts two assignments of error: (1) the forensic search of Appellant's cellphone constituted an

---

<sup>1</sup> [10 U.S.C. §§ 880, 912a, 920c, 934.](#)

unlawful general search in violation of the [Fourth Amendment](#); and (2) the military judge abused his discretion when he denied [\*2] 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 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."<sup>2</sup>

After [\*3] 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."<sup>3</sup>

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."<sup>4</sup> As he knew based on his training and 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 [\*4] 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."<sup>5</sup> The examiner then reorganized the images into a "table view," which placed

---

<sup>3</sup> R. at 237-39; App. Ex. XXV at 87.

<sup>4</sup> *Id.* at 240.

<sup>5</sup> *Id.*

<sup>2</sup> App. Ex. XXVI at 55.

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.<sup>6</sup>

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.<sup>7</sup> 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."<sup>8</sup> His intent was to sort "for all photos that contain GPS [location data] and then . . . filter that with a date."<sup>9</sup> However, "before [he] could set a filter to only show photos with metadata that contains location data," he saw a thumbnail image of suspected child pornography.<sup>10</sup> He then stopped the search, and law enforcement requested additional authorization to search [\*5] 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](#)

---

<sup>6</sup> App. Ex. XXVI at 97.

<sup>7</sup> App. Ex. XXVI at 97; R. at 243.

<sup>8</sup> R. at 243.

<sup>9</sup> *Id.*

<sup>10</sup> App. Ex. XXVI at 97.

[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.<sup>11</sup>

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.

## II. DISCUSSION [\*6]

### 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.<sup>12</sup> A military judge abuses his discretion if the findings of fact

---

<sup>11</sup> App. Ex. LIII at 22.

<sup>12</sup> [United States v. Blackburn, 80 M.J. 205, 210-11 \(C.A.A.F. 2020\)](#).



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.<sup>13</sup> To constitute as an abuse of discretion, the decision must be "arbitrary, fanciful, clearly unreasonable or clearly erroneous."<sup>14</sup>

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 persons or things to be seized.<sup>15</sup>

A search conducted pursuant to a warrant or search authorization is presumptively reasonable.<sup>16</sup> However, search authorizations must "describe the things to be seized with sufficient particularity to prevent a general exploratory [\*7] rummaging in a person's belongings."<sup>17</sup> 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."<sup>18</sup>

Data stored within a cell phone falls within the [Fourth Amendment's](#) protections.<sup>19</sup> 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."<sup>20</sup> Given "the dangers of too narrowly limiting where investigators 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."<sup>21</sup> 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."<sup>22</sup>

Nevertheless, such searches remain subject to an "ex post reasonableness analysis" [\*8] to assess whether they have struck the appropriate balance between being

<sup>13</sup> [United States v. Ellis, 68 M.J. 341, 344 \(C.A.A.F. 2010\)](#).

<sup>14</sup> [United States v. Sullivan, 74 M.J. 448, 453 \(C.A.A.F. 2015\)](#) (citation omitted).

<sup>15</sup> [U.S. Const. amend. IV](#).

<sup>16</sup> 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, 88 S. Ct. 507, 19 L. Ed. 2d 576 \(1967\)](#)).

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

<sup>18</sup> [Maryland v. Garrison, 480 U.S. 79, 84, 107 S. Ct. 1013, 94 L. Ed. 2d 72 \(1987\)](#).

<sup>19</sup> [Riley v. California, 573 U.S. 373, 386, 134 S. Ct. 2473, 189 L. Ed. 2d 430 \(2014\)](#).

<sup>20</sup> [Richards, 76 M.J. at 369-70](#) (citation omitted).

<sup>21</sup> [Id. at 370](#) (citation omitted).

<sup>22</sup> [United States v. Allen, 53 M.J. 402, 408 \(C.A.A.F. 2000\)](#).

"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."<sup>23</sup> One aspect of this analysis examines whether the person conducting the search does so "strictly within the bounds set by the warrant."<sup>24</sup> 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."<sup>25</sup> The [Fourth Amendment](#) standard is "reasonableness"<sup>26</sup> and courts assess the government's search methods after the fact "in light of the specific circumstances of each case."<sup>27</sup>

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."<sup>28</sup> 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 [\*9] 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.<sup>29</sup> 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."<sup>30</sup>

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.<sup>31</sup> 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

---

<sup>23</sup> [Richards, 76 M.J. at 370](#) (citations omitted).

<sup>24</sup> [Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388, 394 n.7, 91 S. Ct. 1999, 29 L. Ed. 2d 619 \(1971\)](#).

<sup>25</sup> [United States v. Loera, 923 F.3d 907, 920 \(10th Cir. 2019\)](#) (quoting [United States v. Burgess, 576 F.3d 1078, 1094 \(10th Cir. 2009\)](#)).

<sup>26</sup> [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).

<sup>27</sup> [United States v. Christie, 717 F.3d 1156, 1166 \(10th Cir. 2013\)](#).

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

<sup>29</sup> [Richards, 76 M.J. at 371](#).

<sup>30</sup> [Arizona v. Hicks, 480 U.S. 321, 325, 328, 107 S. Ct. 1149, 94 L. Ed. 2d 347 \(1987\)](#) (citation and internal quotation marks omitted).

<sup>31</sup> Mil. R. Evid. 311(a).

conduct, or in some [\*10] circumstances recurring or systemic negligence.<sup>32</sup>

Thus, "[t]he extent to which the exclusionary rule is justified by these deterrence principles varies with the culpability of the law enforcement conduct."<sup>33</sup> "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 Amendment](#)."<sup>34</sup>

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 [\*11] 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.<sup>35</sup>

The military judge cited the [Fourth Amendment](#) particularity requirement's application to electronic devices, noting that "the courts have looked to what is reasonable under the circumstances" when determining whether a search was lawfully conducted within the scope of a search authorization.<sup>36</sup> 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."<sup>37</sup> The military judge found that the examiner's "plan [\*12] 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

---

<sup>32</sup> [Herring v. United States, 555 U.S. 135, 144, 129 S. Ct. 695, 172 L. Ed. 2d 496 \(2009\)](#).

<sup>33</sup> [Id. at 143](#).

<sup>34</sup> *Id.* (internal quotation and citation omitted).

---

<sup>35</sup> App. Ex. LIII at 6-7.

<sup>36</sup> *Id.* at 12, 20.

<sup>37</sup> *Id.* at 20.

examiner's] screen without even scrolling."<sup>38</sup> unreasonable or clearly erroneous.

On these facts, the military judge concluded the examiner's search was "conducted reasonably and did not exceed the scope of the [search authorization]."<sup>39</sup> 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 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."<sup>40</sup>

While we find the DC3 examiner's search methodology concerning, we find no abuse of discretion in the [\*13] 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

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] 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."<sup>41</sup> But since his intention was to "set a filter to only show photos with [\*14] metadata that contains location data,"<sup>42</sup> 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

---

<sup>38</sup> *Id.*

<sup>39</sup> *Id.*

<sup>40</sup> *Id.*

---

<sup>41</sup> R. at 243.

<sup>42</sup> *Id.*

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."<sup>43</sup> 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 [\*15] able to accurately state that all location data, especially within apps, was reviewed for relevance."<sup>44</sup>

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."<sup>45</sup>

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."<sup>46</sup>

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 [\*16] phone] where the [search authorization] did not allow him to look."<sup>47</sup> 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

---

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

<sup>46</sup> [United States v. Lee](#), 82 M.J. 591, 2022 CCA LEXIS 221, \*32 (N.M. Ct. Crim. App. 2022) (unpublished) (quoting [Garrison](#), 480 U.S. at 84).

<sup>47</sup> App. Ex. LIII at 20.

---

<sup>43</sup> App. Ex. XXVI at 91.

<sup>44</sup> App. Ex. XXVI at 100.

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.'"<sup>48</sup> The examiner's search in this case was problematic in both respects. And in another case there may be additional evidence to support a finding of not just mere negligence in this regard, but the sort [\*17] of "gross[] [or] . . . recurring or systemic negligence" that the exclusionary rule is specifically designed to deter.<sup>49</sup>

## 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 [\*18] 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 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.<sup>50</sup> Forfeiture is the failure to make a timely assertion of a right whereas waiver is the intentional relinquishment or abandonment of a known right.<sup>51</sup> "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

---

<sup>48</sup> [Loera](#), 923 F.3d at 920 (quoting [Burgess](#), 576 F.3d at 1094).

<sup>49</sup> [Herring](#), 555 U.S. at 144.

---

<sup>50</sup> [United States v. Davis](#), 79 M.J. 329, 331 (C.A.A.F. 2020).

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

disqualification."<sup>52</sup>

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 [\*19] of the military judge's relationships with the individuals involved when he agreed to waive this issue to gain 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.<sup>53</sup>

## 2. Apparent Bias

We generally do not review waived issues "because a valid waiver leaves no error for us to correct on appeal."<sup>54</sup> 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."<sup>55</sup> This includes reviewing "whether to leave an accused's waiver intact, or to correct error."<sup>56</sup> 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.<sup>57</sup> Any error is reviewed for harmlessness.<sup>58</sup> An accused has a constitutional right to an impartial judge.<sup>59</sup> However, there is a "high hurdle" an appellant must clear to prove that a military [\*20] judge was partial or appeared to be so, as the law establishes a "strong presumption" to the contrary.<sup>60</sup> 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."<sup>61</sup> 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

---

<sup>52</sup> [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)).

<sup>53</sup> See [Gladue](#), 67 M.J. at 314.

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

---

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

<sup>56</sup> *Id.*

<sup>57</sup> [United States v. Sullivan](#), 74 M.J. 448, 453 (C.A.A.F. 2015).

<sup>58</sup> [United States v. Roach](#), 69 M.J. 17, 20 (C.A.A.F. 2010) (citing [Liljeberg v. Health Services Acquisition Corp.](#), 486 U.S. 847, 108 S. Ct. 2194, 100 L. Ed. 2d 855 (1988)).

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

<sup>60</sup> [United States v. Quintanilla](#), 56 M.J. 37, 44 (C.A.A.F. 2001).

<sup>61</sup> R.C.M. 902(a).

might reasonably be questioned."<sup>62</sup>

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."<sup>63</sup> 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 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 [\*21] [military] judge."<sup>64</sup>

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."<sup>65</sup> 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."<sup>66</sup> 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."<sup>67</sup>

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 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 [\*22] 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.<sup>68</sup>

The findings and sentence are **AFFIRMED**.

---

End of Document

---

<sup>62</sup> [Hasan v. Gross](#), 71 M.J. 416, 418 (C.A.A.F. 2012).

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

<sup>64</sup> [Uribe](#), 80 M.J. at 447 (cleaned up).

<sup>65</sup> R. at 30.

<sup>66</sup> *Id.*

<sup>67</sup> *Id.* at 31 (quoting [Liljeberg v. Health Servs. Acquisition Corp.](#), 486 U.S. 847, 864, 108 S. Ct. 2194, 100 L. Ed. 2d 855 (1988)).

<sup>68</sup> [Articles 59 & 66](#), UCMJ.



[United States v. Shields](#)

United States Court of Appeals for the Armed Forces

November 10, 2022, Decided

No. 22-0279/MC.

**Reporter**

2022 CAAF LEXIS 809 \*

U.S. v. Ethan R. Shields.

---

End of Document

**Notice:** DECISION                      WITHOUT  
PUBLISHED OPINION

**Prior History:** [\*1] CCA 202100061.

[United States v. Shields, 2022 CCA LEXIS 448, 2022 WL 2966378 \(N-M.C.C.A., July 27, 2022\)](#)

**Opinion**

---

On consideration of the petition for grant of review of the decision of the United States Navy-Marine Corps Court of Criminal Appeals, it is ordered that said petition is granted on 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?](#)

Briefs will be filed under [Rule 25](#).