

**IN THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES**

UNITED STATES,
Appellant

v.

Private (E-1)
JUSTIN M. GURCZYNSKI
United States Army,
Appellee

) BRIEF ON BEHALF OF
) APPELLANT
)
) Crim. App. Dkt. No. 20160402
)
) USCA Dkt. No. _____/AR
)
) Tried at Fort Leavenworth, Kansas,
) on 25 April 2016, before a general
) court-martial, convened by the
) Commander, Headquarters, United
) States Army Combined Arms Center
) and Fort Leavenworth, Colonel
) Jeffery R. Nance, presiding.

CARLING M. DUNHAM
Captain, Judge Advocate
Appellate Counsel
Government Appellate Division
U.S. Army Legal Services Agency
9275 Gunston Road, Room 2014
Fort Belvoir, VA 22060
(703) 693-0767
carling.m.dunham.mil@mail.mil
U.S.C.A.A.F. Bar No. 36357

SAMUEL E. LANDES
Captain, Judge Advocate
Branch Chief
Government Appellate Division
U.S.C.A.A.F. Bar No. 36626

A.G. COURIE III
Lieutenant Colonel, Judge Advocate
Deputy Chief, Government
Appellate Division
U.S.C.A.A.F. Bar No. 36422

MARK H. SYDENHAM
Colonel, Judge Advocate
Chief, Government Appellate
Division
U.S.C.A.A.F. Bar No 34432

**TO THE HONORABLE JUDGES OF THE
UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES**

Index

Table of Cases, Statutes, and Other Authorities iii
Statement of Statutory Jurisdiction 1
Statement of the Case..... 1
Statement of Facts 2
Issue Presented 8

**WHETHER THE MILITARY JUDGE ERRED IN
SUPPRESSING EVIDENCE OF CHILD
PORNOGRAPHY A DIGITAL FORENSIC
EXAMINER DISCOVERED DURING A SEARCH FOR
APPELLEE’S COMMUNICATIONS WITH A CHILD
VICTIM**

Summary of Argument..... 8
Argument..... 10
Conclusion..... 37
Certificate of Filing and Service 39

Table of Cases, Statutes, and Other Authorities

United States Supreme Court

Andresen v. Maryland, 427 U.S. 463 (1976)23

Arizona v. Hicks, 480 U.S. 321 (1987)27

Coolidge v. New Hampshire, 403 U.S. 443 (1971)27

Horton v. California, 496 U.S. 126 (1990).....22-23, 27-28, 31

United States v. Herring, 555 U.S. 135 (2009)..... 35-36

United States v. Ramirez, 523 U.S. 65 (1998)9

Washington v. Chrisman, 455 U.S. 1 (1982)31

United States Court of Appeals for the Armed Forces

United States v. Kosek, 41 M.J. 60 (C.M.A. 1994).....22

United States v. Fogg, 52 M.J. 144 (C.A.A.F. 1999)22

United States v. Wicks, 73 M.J. 93 (C.A.A.F. 2014) 9, 35-36

Service Courts

United States v. Buford, AF 2016-04, 2016 CCA LEXIS 352 (A.F. Ct. Crim. App. Jun. 9, 2016).....22

United States v. Gallagher, 65 M.J. 601, 605 (N.M. Ct. Crim. App. 2007).....26

United States v. Gurczynski, ARMY 20140518, 2016 CCA LEXIS 530 (A. Ct. Crim. App. Aug. 31, 2016)1

United States v. Gurczynski, ARMY MISC 20160402, 2016 CCA LEXIS 541 (A. Ct. Crim. App. Sep. 6, 2016) 2, 13, 22, 26

<i>United States v. Maza</i> , 73 M.J. 507 (N.M. Ct. Crim. App. 2014)	22
<i>United States v. Mitchell</i> , ARMY MISC 20150776, 2016 CCA LEXIS 179 (A. Ct. Crim. App. Mar. 18, 2016)	22
<i>United States v. Osorio</i> , 66 M.J. 632 (A.F. Ct. Crim. App. 2008)	26
<i>United States v. Richards</i> , AF 38346, 2016 CCA LEXIS 285 (A.F. Ct. Crim. App. May 2, 2016)	12-13
<i>United States v. Washington</i> , ARMY M2010961, 2011 CCA LEXIS 18 (A. Ct. Crim. App. Feb. 8, 2011)	23-28
<i>United States v. Whitley</i> , NMCCA 201500060, 2016 CCA LEXIS 188 (N.M. Ct. Crim. App. Mar. 29, 2016)	14

United States Courts of Appeals

<i>United States v. Burgess</i> , 576 F.3d 1078 (10th Cir. 2009)	9, 24
<i>United States v. Carey</i> , 172 F.3d 1268 (10th Cir. 1999)	19
<i>United States v. Childers</i> , 117 Fed. Appx. 633 (10th Cir. 2004).....	28
<i>United States v. Galpin</i> , 720 F.3d 436 (2d Cir. 2013)	32-33
<i>United States v. George</i> , 975 F.2d 72 (2d Cir. 1992)	32-33
<i>United States v. Grimmett</i> , 439 F.3d 1263 (10th Cir. 2006)	18
<i>United States v. Heldt</i> , 668 F.2d 1238 (D.C. Cir. 1981).....	24
<i>United States v. Hill</i> , 459 F.3d 966 (9th Cir. 2006).....	17
<i>United States v. Mann</i> , 592 F.3d 779 (7th Cir. 2010).....	16-17
<i>United States v. Parker</i> , 549 F.3d 5 (1st Cir. 2009)	30
<i>United States v. Sells</i> , 463 F.3d 1148 (10th Cir. 2006).....	33

<i>United States v. Smith</i> , 459 F.3d 1276 (11th Cir.2006).....	23
<i>United States v. Upham</i> , 168 F.3d 532 (1st Cir. 1999).....	24
<i>United States v. Williams</i> , 592 F.3d 511 (4th Cir. 2010)	18, 28

District Courts

<i>United States v. Farlow</i> , 2009 U.S. Dist. LEXIS 112623 (D. Me. December 3, 2009)	28-30
<i>United States v. Miller</i> , 2013 U.S. Dist. LEXIS 117576 (W.D.N.Y. Aug. 16, 2013)	18
<i>United States v. Will</i> , 2015 U.S. Dist. LEXIS 79887 (D. W. Va. June 19, 2015)...	27

Other Statutes, Materials and Regulations

Article 62, UCMJ, 10 U.S.C. § 862 (2012)	1-2, 9, 26
Article 67, UCMJ, 10 U.S.C. § 867 (2012)	1
Article 107, UCMJ, 10 U.S.C. § 907 (2012)	1
Article 120, UCMJ, 10 U.S.C. § 920 (2006 & Supp. V 2012)	1
Article 134, UCMJ, 10 U.S.C. § 934 (2012)	1
Mil. R. Evid. 311.....	35-36
Mil. R. Evid. 316.....	23

Statement of Statutory Jurisdiction

The United States Army Court of Criminal Appeals (Army Court) reviewed this case pursuant to Article 62, Uniform Code of Military Justice, 10 U.S.C. §862 (2012) [hereinafter UCMJ]. The statutory basis for this Honorable Court's jurisdiction is found in Article 67(a)(2), UCMJ, which mandates review in "all cases reviewed by a Court of Criminal Appeals which the Judge Advocate General orders sent to the Court of Appeals for the Armed Forces (C.A.A.F.) for review."¹ UCMJ art. 67(a)(2).

Statement of the Case

Appellee was charged with two specifications of possession of child pornography in violation of Article 134, UCMJ.² (JA 6). On May 13, 2016, the military judge suppressed the evidence of child pornography found on Appellee's thumb drive based on an alleged violation of the Fourth Amendment. (JA 166-71). On June 22, 2016, the Government appealed the military judge's ruling under

¹ Certificate of Review, signed by the Judge Advocate General, dated November 29, 2016.

² Prior to the discovery of the child pornography on Appellee's digital media devices, he was court-martialed and convicted for two specifications of abusive sexual contact of a child between the ages of 12 and 16, two specifications of indecent liberties with a child under 16 years of age, and a false official statement for stating that he had never met DB in person, in violation of Article 120 and 107, UCMJ. *United States v. Gurczynski*, ARMY 20140518, 2016 CCA LEXIS 530, at *1 (A. Ct. Crim. App. Aug. 31, 2016) (unpublished).

The military judge sentenced him to a bad-conduct discharge, forty months confinement, total forfeitures, and a reduction to the grade of E-1. *Id.* at *1-2.

Article 62, UCMJ. On September 6, 2016, the Army Court denied the appeal. *United States v. Gurczynski*, ARMY MISC 20160402, 2016 CCA LEXIS 541 (A. Ct. Crim. App. Sep. 6, 2016) (sum. disp.). On October 6, 2016, the Government requested reconsideration en banc. The Army Court denied the Government's request for reconsideration on October 24, 2016. (JA 5). The Judge Advocate General then certified this case to this Court.

Statement of Facts

On December 19, 2012, the Criminal Investigative Command (CID) office at the Presidio of Monterey initiated an investigation into Appellee based on an allegation that he had committed an abusive sexual contact on a child, DB, who was under the age of 16. (JA 59). Appellee was interviewed and admitted to having befriended DB through the social networking website, Facebook. (JA 60). The trial counsel at the Presidio of Monterey then requested the CID office to conduct further interviews and collect digital media from Appellee's residence to find additional evidence of Appellee's offenses against DB. (JA 62).

On January 14, 2014, a United States magistrate judge issued a search warrant for Appellee's off-post residence. (JA 67). The magistrate judge incorporated the affidavit of the CID agent in the warrant. (JA 67). The affidavit requested a search warrant for the "cellular device, personal computers, and associated peripheral digital media storage devices" of Appellee. (JA 68).

The minor child alleged that Appellee had an online relationship with him four years prior to meeting in-person. (JA 70). This online relationship began when DB was in fourth grade. (JA 70). The online relationship eventually progressed to communications regarding the “child’s sexuality and the child’s readiness / willingness to lose his virginity.” (JA 70). This online relationship progressed into daily contact, using the telephone and text messaging as well. (JA 70). Appellee and DB used Facebook, mySpace, SafeBuck, TinyChat, Yahoo chat and email, AOL chat and email, and other digital media programs. (JA 70).

Friends of DB stated that he had confided in them about the relationship with Appellee and that Appellee was coming to Kansas to visit him. (JA 71). “One friend of the child described the child telling her shortly before 15 May 2015, that ‘Justin is coming to see me and said he was going to tear my ass apart.’” (JA 71).

The child’s online relationship with Appellee continued after Appellee visited him in Kansas. (JA 71). The child told investigators that his communications with Appellee ceased shortly after Appellee’s live-in boyfriend, Mr. Aaron Boyle, discovered the online relationship between Appellee and DB and questioned Appellee about the nature of the relationship and about pictures of the child found on Appellee’s computer. (JA 71). Mr. Boyle confirmed that he had discussed the nature of Appellee’s relationship with DB after “discovering

communications with, and pictures of, the child on [Appellee's] computer.” (JA 71).

The search warrant authorized CID agents to search Appellee's digital media devices for evidence of violations of the UCMJ for attempted aggravated sexual assault of a child, indecent acts with a child, attempted sexual abuse of a child, abusive sexual contact with a child, child endangerment, and other offenses related to these allegations. (JA 66, 68). The military judge found that the warrant authorized the CID agents to search Appellee's digital media devices “for evidence that [Appellee] used those devices to access on line [sic] mediums to communicate with [DB] in order to ‘engage in indecent acts with a child and to plan and execute a meeting with [DB] where [Appellee] ultimately engaged in additional indecent acts and sexual contacts with the child.’” (JA 166) (quoting from the warrant). The search warrant authorized the agents to search for evidence that he used digital media devices between September 1, 2007 and December 28, 2011 to maintain contact with DB and to discuss with DB and with others the crimes that had been committed. (JA 68).

On January 24, 2014, the CID agents executed the search warrant and seized twenty-eight digital media devices from Appellee's home, including the thumb drive and external hard drive where child pornography was found. (JA 65, 74-76).

The CID office at the Presidio of Monterey sent the evidence to the CID office at Joint Base Lewis-McChord (JBLM) for assistance in conducting the digital forensic exam. (JA 77).

The digital forensic examiner (DFE), Special Agent CJP, from the JBLM CID office testified that he received the federal search warrant along with the evidence and conducted the digital forensic exam. (JA 13, 15). While the DFE received the request from the Presidio of Monterey office and used it to inventory the evidence, the DFE testified that he based his search on the limits of the warrant. (JA 14-16). This was corroborated by his report. (JA 94). He noted that the request from the Presidio included a request to search for child pornography, but concluded, “A Federal Search Warrant, dated 14 Jan 14, [] authorized the examination; however, *limited the analysis of the media for items of evidence pertaining to the offenses under investigation . . .*” (JA 94) (emphasis added).

When the DFE examined Appellee’s thumb drive, he used software that would show him all the different files on the device. (JA 17). The software’s report revealed what appeared to the DFE to be files of child pornography. (JA 18). There were no folders on the thumb drive, so “as soon as the image loaded into [the DFE’s] software, you know, the files read through the devices, it’s right there on the screen.” (JA 18). The DFE did not have to click into any folders or files to observe the file names and an image of the files. (JA 18-20).

The forensic software the DFE used was “set up to retrieve three different views all at the same time.” (JA 18). The software displayed the file names, the file information to the right of the file names, and a picture view of the files. (JA 18-19). Based on this initial viewing of the file names and images of the files, the DFE “almost immediately” observed that the thumb drive contained child pornography. (JA 19). In this same thumb drive, along with the suspected images of child pornography, the DFE also found a photograph of Appellee and an unknown young male. (JA 111). The files of child pornography were created on or before June 12, 2010 and the image of Appellee and an unknown young male was created on March 20, 2010—both within the date range specified by the warrant. (JA 111, 68).

The DFE also noted that the thumb drive had been previously connected to Exhibit 8, which was a Western Digital Internal Hard Drive Disk. (JA 111, 106). When the DFE examined this hard drive, he found evidence that the user had sent a friend request to DB for Stickam, a live-streaming website. (JA 107). Exhibit 8 also contained evidence that Appellee had engaged in Skype chat messages with what appeared to be an underage male and engaged in a video masturbation session with him. (JA 107).

As part of his investigation, on January 1, 2015, the DFE contacted the Presidio of Monterey CID office for a photograph of the victim so he could

compare the photograph he had discovered on Appellee's digital media devices to known photographs of DB. (JA 85).

In examining the hard drive, the DFE used the limits of the search warrant to guide his search through the files. (JA 16, 94). He limited his search to areas where there would be communications between the subject and a young victim, such as programs, applications, databases, and images. (JA 21). He stated that he included images in his search because, “[f]rom [his] experience people tend to screen shot things, make copies of it and it’ll show up as an image.” (JA 22).

In this case, Appellee had a program set up on his computer to “automatically create screen shots every 30 minutes.” (JA 22, 104). In those screen shot images, the DFE found evidence of communications between the victim and Appellee. (JA 22, 104). The DFE also found chat logs that contained communications between Appellee and the victim. (JA 22-23, 104-05).

When the trial counsel asked the DFE if there were any areas that he would not look into or exclude when searching for communications with a minor, he responded, “Not much, to be honest with you. Communications are—you know, can be found pretty much anywhere.” (JA 23).

The military judge found that the Government had a “valid warrant based upon probable cause to search for communications (which could include shared photos) between [Appellee and DB].” (JA 169). The military judge acknowledged

that the “communications were alleged to have occurred via various electronic communication devices.” (JA 169). The military judge again stated that these communications could include photographs, “and even child pornography, if such child pornography were part of a communication or possible communication” to DB. (JA 170). However, the military judge held that the DD Form 2922 from the Presidio of Monterey that requested a search for child pornography improperly expanded the scope of the warrant and the resulting search. (JA 170). The military judge did not address the plain view doctrine which operates as an exception to the Fourth Amendment’s prohibition against unreasonable searches and seizures.

Issue Presented

WHETHER THE MILITARY JUDGE ERRED IN SUPPRESSING EVIDENCE OF CHILD PORNOGRAPHY A DIGITAL FORENSIC EXAMINER DISCOVERED DURING A SEARCH FOR APPELLEE’S COMMUNICATIONS WITH A CHILD VICTIM

Summary of Argument

This Court should set aside the military judge’s ruling because the child pornography was discovered while the agent was acting within the scope of the warrant. Even if, after a de novo review, this Court concludes that the child pornography was not contemplated by the warrant, this Court should set aside the military judge’s ruling because the plain view exception applies. Finally, the military judge abused his discretion in suppressing this evidence because the

deterrent effect of suppression is minimal and does not outweigh the direct harm to the justice system.

Standard of Review

Under Article 62, UCMJ, when “reviewing a military judge’s ruling on a motion to suppress, this Court reviews the military judge’s decision directly . . . [reviewing] factfinding under the clearly-erroneous standard and conclusions of law under the de novo standard.” *United States v. Wicks*, 73 M.J. 93, 98 (C.A.A.F. 2014).

Argument

A. A search for child pornography was authorized by the warrant.

“The general touchstone of reasonableness which governs Fourth Amendment analysis . . . governs the method of execution of the warrant.” *United States v. Ramirez*, 523 U.S. 65, 71 (1998). “The ultimate question of reasonableness under the Fourth Amendment is a legal conclusion that we review de novo.” *United States v. Burgess*, 576 F.3d 1078, 1087 (10th Cir. 2009). Therefore, the DFE’s understanding of the parameters of the search and his actions in executing the search should be viewed in terms of reasonableness and should be reviewed by this court de novo.

As a preliminary matter, the military judge found that there was a “valid warrant based upon probable cause to search for communications (which could

include shared photos) between the accused and the alleged child victim.” (JA 169). The military judge further stated that “the facially valid warrant particularly described the place to be searched and the things to be seized.” (JA 169).

There are four reasons the DFE acted within the scope of the valid search warrant: (1) all parties agreed that communications could be images; (2) the affidavit accompanying the search warrant indicated that there were photographs of a minor child; (3) the DFE knew he was limited by the terms of the search warrant; and (4) the DFE never abandoned the original purpose of the search warrant. In conducting the de novo review of the military judge’s legal conclusions, this Court should also consider the two clearly erroneous findings of fact by the military judge that impact the context of the DFE’s actions and findings.

1. Evidence of communications could be images.

All parties, to include the military judge, agreed that evidence of the crime—Appellee’s communications with DB—could be images. The military judge stated, “Well, if a picture is worth a thousand words, isn’t a picture sent to someone a communication?” (JA 26). The military judge continued, “Well, yeah, so if a picture’s worth a thousand words, then a video is worth 5,000 words, 10,000 words.” (JA 27). Later, the military judge noted that the way people communicate now is through pictures and videos, not just letters and phone calls. (JA 41).

2. The warrant included evidence that photographs of DB were seen on Appellee's computer.

The warrant contemplated searching for images of a minor child. (JA 71). The Presidio CID office included a picture of DB when they sent the request for forensic examination. (JA 78). When the DFE conducted his examination, he reached back to the Presidio for an additional photograph of DB so he could compare the images he had discovered on Appellee's digital media devices to known photographs of DB. (JA 85). Significantly, the military judge conceded that if the DFE had found "evidence of sending pictures back and forth between [Appellee and DB] and those pictures included naked photographs of a minor, then that would have been within the scope of the original search. . . ." (JA 35).

It was reasonable to believe that the images of the minor child could be child pornography. Appellee's boyfriend had discovered pictures of DB on Appellee's computer that prompted him to question Appellee about the nature of their relationship. (JA 71). The child, DB, told investigators that Appellee continued their online relationship even after Appellee's visit to Kansas, and it only ended when Appellee's boyfriend discovered the communications and photographs exchanged between Appellee and DB. (JA 71). As the Government argued, photographs of DB were not "just a hypothetical That was part of the basis to even get this search warrant" (JA 40). The application for the search

warrant “established probable cause that not only were there communications, but there were pictures.” (JA 40).

There is no support in the record for the military judge’s factual finding that any photos contemplated by the warrant were those that might have been exchanged between Appellee and his minor victim during the course of getting to know one another. (JA 170). The military judge acknowledged that the pictures could have been exchanged as part of Appellee’s “grooming the victim for future sexual activity.” (JA 170). Requesting and receiving child pornography *of* DB *from* DB certainly could be considered grooming for future in-person sexual activity. The nature of Appellee’s online contact with the child was sexually charged and progressed to discussing the child’s sexuality and when he was ready to lose his virginity. (JA 70-71). Appellee’s conversations with DB were sexually graphic, with Appellee telling the child that he was ““coming to see [him] and said he was going to tear [DB’s] ass apart.”” (JA 71).

Case law supports the proposition that child pornography is reasonably contemplated by a warrant authorizing a search of communications between an adult and his minor victim. In *United States v. Richards*, when the DFE came across evidence of child pornography, he was searching for evidence of communications between Appellant and the minor child, AP. *United States v. Richards*, AF 38346, 2016 CCA LEXIS 285 (A.F. Ct. Crim. App. May 2, 2016)

(unpublished). The victim, AP, “had told investigators that he had engaged in prolonged online communications with Appellant and that some of these communications were sexually explicit.” *Id.* at *60. The court found that “[u]nder these facts, it was reasonable to presume that images or videos were exchanged.” *Id.*

In this case, the warrant accurately captured the highly sexualized relationship when it stated the search was for evidence of aggravated sexual assault of a child, indecent acts with a child, attempted sexual abuse of a child, abusive sexual contact with a child, child endangerment, and other offenses related to these allegations, for a date range that spanned nearly four and a half years, beginning when the child was in fourth grade. (JA 66, 68). Significantly, both the military judge and the Army Court omitted the offense of child endangerment in the recitation of the offenses specified in the warrant. (JA 166); *Gurczynski*, 2016 CCA LEXIS, at *3. To omit child endangerment is to overlook the ongoing nature of Appellee’s crimes against DB. Additionally, the broad offense of child endangerment can provide a nexus to child pornography. *See United States v. Whitley*, NMCCA 201500060, 2016 CCA LEXIS 188, at *12 (N.M. Ct. Crim. App. Mar. 29, 2016) (unpublished).

3. The DFE knew he was limited by the terms of the search warrant.

The military judge made a clearly erroneous finding of fact when he stated that the request from the Presidio improperly expanded the scope of the warrant. (JA 170). Neither the DFE's testimony during the Article 39(a) motions hearing nor his report provide support for that finding of fact. The DFE testified that he based his search on the limits of the warrant. (JA 14-16). The testimony went as follows:

Q: Do you use those two [warrant and request] simultaneously or do you just use the search warrant?

A: No, I use both.

Q: Okay.

A: But the authorization, the search warrant actually determines the laboratory request.

Q: Okay, so you follow what the search warrant says?

A: Yes.

(JA 16).

The DFE's testimony was corroborated by his report. (JA 94). He specifically noted the request from the Presidio but then wrote, "A federal search warrant authorized the examination; however, limited the analysis of the media for items of evidence pertaining to the offense under investigation," which were the offenses of Appellee against DB. (JA 94). For each item he examined, the DFE noted whether it was pertinent to the ongoing investigation of offenses against DB or evidence of additional crimes. For example, for the DFE's search of Appellee's hard disk drive, the DFE noted that there were "screenshots and Skype chat

message pertinent to the originating office’s investigation” *and also* contained “suspected images of child pornography which may be possible *additional* victims associated with SSG Gurczynski.” (JA 95) (emphasis added).

The DD Form 2922, the forensic laboratory examination request, did not improperly expand the scope of the warrant. On the front page, it listed “abusive sexual contact with a child” as the type of offense. (JA 77). Its first mention of child pornography was on the second page, and was in the context of the investigation of the offenses against DB: “Please preview [exhibit numbers] for the presence of child pornography *or correspondence with [DB].*” (JA 78) (emphasis added). Rather than improperly expanding the scope of the warrant, the request, albeit inartfully, focused the DFE’s attention to the digital aspect of the investigation—Appellee’s sexually charged online conduct with DB, which included photographs. It is entirely reasonable to believe that Appellee, who had threatened to “tear [DB’s] ass apart,” (JA 71), had sent to or received from DB child pornography, and that such communications were stored on Appellee’s digital media devices.

As additional evidence that the request did not improperly expand the scope of the warrant, the DFE testified that he would not have been able to conduct his search in any other way. The DFE was asked, “What areas would you not look into when you’re talking about communications with a minor? [S]o what would the

search warrant have excluded in this case or prevented you from looking into?”

The DFE replied, “Not much, to be honest with you. Communications are—you know, can be found pretty much anywhere.” (JA 23).

The DFE’s testimony is similar to the detective’s testimony in *United States v. Mann*, who stated that images can be located nearly anywhere with computer searches. *United States v. Mann*, 592 F.3d 779, 782-83 (7th Cir. 2010). The detective stated that “regardless of what I found, I would search in all the files if I felt it necessary, if I felt that it contained information that was pertinent to my case or even exculpatory.” *Id.*

In *Mann*, the appellant covertly installed a video camera in the women’s locker room to capture footage of women changing their clothes. *Id.* at 780. A prosecutor obtained a search warrant to search the appellant’s residence for digital media devices. *Id.* at 781. He was charged with voyeurism under state law. *Id.*

Two months later, an investigator began his search of the appellant’s computers. *Id.* On the first computer, the investigator discovered evidence that the appellant visited a website called “Perverts Are Us,” which contained stories about child molestation. *Id.* On the laptop, the investigator discovered photographs of the high school locker room as well as images of child pornography. *Id.* The investigator also discovered that an external hard drive had been connected to the laptop. *Id.* Two months after the first search, the investigator searched the

external hard drive and found several additional images of child pornography as well as videos from the high school locker room. *Id.* In moving to suppress the evidence, the appellant alleged that the warrant lacked probable cause and the investigator had exceeded the scope of the search warrant. *Id.*

While the court found that the warrant's description of the items to be seized served as a limitation on what files could reasonably be searched, the court noted that with computer searches images can be located nearly anywhere. *Id.* at 782. Additionally, “[u]nlike a physical object that can be immediately identified as responsive to the warrant or not, computer files may be manipulated to hide their true contents.” *Id.*; see also *United States v. Hill*, 459 F.3d 966, 978 (9th Cir. 2006) (“Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer.”).

In *Mann*, the court held that this was not a prohibited general search. *Mann*, 592 F.3d at 786. In order to search the computer for images of women, the investigator could not thoroughly search the computer without “stumbling upon [the appellant’s] extensive collection of child pornography.” *Id.* at 783; see also *United States v. Williams*, 592 F.3d 511, 514 (4th Cir. 2010) (holding that that search for and seizure of the child pornography fell within the scope of the warrant

to search for evidence of computer harassment and alternatively holding search was justified under the plain view exception).

In *Burgess*, the police were looking for evidence of drug-related crimes and had a warrant that included the authority to search computer records. *Burgess*, 576 F.3d at 1083. The investigator used the same program as the DFE in this case, EnCase. *Id.* The investigator used a “preview” feature to look for photographs commonly related to drug trafficking. *Id.* at 1084. Much like this case, the images were shown in a “‘gallery view,’ an option where multiple reduced size photos are displayed on one page.” *Id.* When searching through the computer for evidence of drug-related crimes, the investigator found child pornography. *Id.*

The court stated that “‘a computer search may be as extensive as reasonably required to locate the items described in the warrant’ based on probable cause.” *Id.* at 1092 (quoting *United States v. Grimmett*, 439 F.3d 1263, 1270 (10th Cir. 2006)). The court also held that file names may alert one to contents, but it is just as possible that file names are misleading. *Id.* at 1093. The court also recognized that “image files . . . could be buried almost anywhere.” *Id.* at 1095. *See also United States v. Miller*, 2013 U.S. Dist. LEXIS 117576, at *3-4, 10 (W.D.N.Y. Aug. 16, 2013) (The warrant authorized a search of the defendant’s residence for evidence of unstamped and untaxed cigarettes. The district court held that the

police officer did not exceed the scope of the warrant when he searched a digital camera with a memory card and found images of child pornography.).

In this case, the DFE had to search the thumb drive in order to look for evidence of Appellee's communications with the minor child, which all parties agreed could have included photographs, and reasonably could have included child pornography. The DFE testified that he could not have conducted his search differently due to the concept that images could be located anywhere. He also testified that he knew he was bound by the terms of the search warrant and his analysis in his report corroborates his knowledge of his limitations.

4. The DFE never abandoned the original purpose of the search warrant.

It is also important to note that unlike the investigator in *United States v. Carey*, this DFE did not continue to open files with the expectation of finding additional child pornography. In *Carey*, after the investigator was unsuccessful in finding evidence of the sale and distribution of controlled substances, he continued to search for child pornography. *United States v. Carey*, 172 F.3d 1268, 1273 (10th Cir. 1999). The *Carey* court stated that the investigator had "temporarily abandoned that search to look for more child pornography, and only 'went back' to search for drug-related documents after conducting a five hour search of the child pornography files." *Id.*

In this case, the DFE started his search for evidence of communications between Appellee and DB on Appellee's phone. (JA 103). He found evidence that DB was a contact in his phone. (JA 103). He also found multiple chat messages which discussed DB and Appellee's attraction to underage males. (JA 103). The DFE next searched the computer hard drive. (JA 104). He found fifteen screenshots of the "friends" section of Appellee's Facebook profile, in which DB was listed, and found that Appellee had conducted a search for people named "[DB]" via Facebook. (JA 104). He also found a screenshot of a messaging program in which DB was listed as a contact. (JA 104). He discovered that DB was listed in Appellee's contacts in Skype. (JA 105). The DFE found two Skype chat messages between Appellee and DB where Appellee asked DB for his number. (JA 105). The DFE continued to look through various digital media devices for more evidence of Appellee's communications with DB, and continued to find evidence. (JA 102-11). On a different hard drive, the DFE found a Facebook chat message sent from DB to Appellee and evidence that Appellee had saved fourteen of DB's Facebook status updates. (JA 110).

The DFE examined the thumb drive last, after consistently finding evidence of Appellee's communications with DB on the other digital media devices. (JA 111). The first thing the DFE noted was that that the thumb drive had been previously connected to Exhibit 8, which was a Western Digital Internal Hard

Drive Disc. (JA 111, 106). That hard drive contained evidence that Appellee had engaged in Skype chat messages with what appeared to be an underage male and engaged in a video masturbation session with him. (JA 107).

When the DFE examined Appellee's thumb drive, there were no folders on the thumb drive, so "as soon as the image loaded into [his] software, you know, the files read through the devices, it's right there on the screen." (JA 18). The DFE did not have to click into any folders or files to observe the file names and an image of the files. (JA 18-20).

The forensic software the DFE used was "set up to retrieve three different views all at the same time." (JA 18). The software displayed the file names, the file information to the right of the file names, and a picture view of the files. (JA 18-19). Based on this first viewing of the file names and images of the files, the DFE "almost immediately" observed that the thumb drive contained child pornography. (JA 19).

The DFE searched each item with the purpose of finding evidence of communications between Appellee and DB. Part of those communications included photographs that provoked Appellee's boyfriend to confront him and resulted in the termination of Appellee's online relationship with DB. The DFE never abandoned the purpose of his search to find evidence of these sexually charged communications.

B. Even if child pornography was not contemplated by the warrant, the plain view exception applies.

The Army Court recognized that the military judge did not address the plain view exception, yet cursorily dismissed it in a footnote. *Gurczynski*, 2106 CCA LEXIS, at *6 n.3. However, the child pornography was discovered in plain view of the DFE's authorized search. Accordingly, this Court should set aside the military judge's ruling.³

1. The images of child pornography were commingled with other evidence of communications between Appellee and DB and the DFE's search meets all three prongs of the *Horton* plain view test.

Law enforcement officials conducting a lawful search may seize items in plain view if they “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. Fogg*, 52 M.J. 144, 149 (C.A.A.F. 1999); *see also* Military Rule of

³ In the alternative, this Court should remand the case to the military judge to consider the plain view exception. When a military judge has failed to consider a determinative legal principle, the appropriate remedy may be remand. *See United States v. Maza*, 73 M.J. 507, 513 (N.M. Ct. Crim. App. 2014) (“If findings are incomplete or legal issues have not been considered by the military judge, the ‘appropriate remedy . . . is a remand for clarification’ or additional findings.” (quoting *United States v. Kosek*, 41 M.J. 60, 64 (C.M.A. 1994)); *United States v. Buford*, AF 2016-04, 2016 CCA LEXIS 352, at *14 (A.F. Ct. Crim. App. Jun. 9, 2016) (unpublished) (“Consequently, this omission is so significant that we believe remand of the case is necessary to ensure the proper evaluation of this factual matter against the objective legal standard”); *United States v. Mitchell*, ARMY MISC 20150776, 2016 CCA LEXIS 179, at *4-5 (A. Ct. Crim. App. Mar. 18, 2016) (unpublished).

Evidence [Mil. R. Evid.] 316(c) (stating property may be seized if “the 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.”). “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.” *United States v. Smith*, 459 F.3d 1276, 1290 (11th Cir.2006) (quoting *Horton v. California*, 496 U.S. 128, 135 (1990)).

Although advances in technology often outpace nuances in the law, courts now recognize that the viewing of otherwise inoffensive documents may be unavoidable in searches of digital media because of the extensive comingling of documents: “[C]omputer searches are fundamentally no different than other searches involving commingled documents. When commingled records are searched, ‘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.’” *United States v. Washington*, ARMY M2010961, 2011 CCA LEXIS 18, at *9 (A. Ct. Crim. App. Feb. 8, 2011) (unpublished), *rev. denied*, *United States v. Washington*, 2011 CAAF LEXIS 345 (C.A.A.F. Apr. 22, 2011) (quoting *Andresen v. Maryland*, 427 U.S. 463, 483 n.111 (1976)). In searching comingled documents, investigators must be permitted to do a “brief perusal of

documents in plain view in order to determine whether probable cause exists for their seizure under the warrant.” *United States v. Heldt*, 668 F.2d 1238, 1267 (D.C. Cir. 1981). The Tenth Circuit Court of Appeals has held that because digital media devices have the capacity to store tremendous amounts of comingled data, there may not be a substitute for a brief, physical examination of many, if not all, of the data. *Burgess*, 576 F.3d at 1094; *see also United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) (“[A] search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for weapons or drugs.”).

Washington presents an extremely similar fact pattern in which the court found that the plain view exception applied. *Washington*, 2011 CCA LEXIS, at *12. In *Washington*, a CID agent obtained a search authorization to search the accused’s laptop and external hard drive for evidence of a rape. *Washington*, 2011 CCA LEXIS, at *2. The written authorization gave investigators authority to search the digital media for texts, documents, pictures, graphics/images, electronic mail messages, chat room databases, software, video files, peer to peer systems, file sharing, computerized logs, account names, passwords, personal notes, diaries, and other data including deleted files and folders which contained the name or image of the victim. *Id.* at *3.

The digital forensic examiner testified that he opened each file to examine it for images of the victim. *Id.* at *4. During the course of opening the image files, he observed thirty-two video files of what he believed to be child pornography. *Id.* at *4. He bookmarked those images and continued to search Appellee's digital media devices, but eventually found no images of the victim. *Id.* at *4. The agent acknowledged that some of the file names were ones that, in his experience, were associated with child pornography (e.g., "PTHC," an acronym for "Preteen Hardcore"). *Id.* at *4.

The agent testified that he "wasn't focusing on the child pornography. I was actually just focusing on the files related to the subject and the victim." *Id.* at *4. He stated that the file names were not the basis for him opening the files. *Id.* at *4. The agent testified that he had to validate the contents of the file, citing his past experience of having suspiciously-titled files, even those using the acronym PTHC, containing only adult pornography. *Id.* at *4-5.

At trial, the military judge found that the search authorization gave the agent "broad authority to search for any present or deleted files, documents or videos, pictures or codes that contained the name or image of" the victim. *Id.* at *5-6. However, much like in this case, the military judge ruled that the discovery of the file names established probable cause for an act unrelated to the victim and therefore opening the files was a warrantless search. *Id.* at *6. The military judge

also found that the plain view exception did not apply. *Id.* Upon an Article 62 appeal, the Army court vacated the military judge’s ruling by reviewing the military judge’s conclusions of law de novo and finding that the military judge was influenced by an erroneous view of the law in not applying the plain view exception. *Id.* at *9-10;⁴ *see also United States v. Gallagher*, 65 M.J. 601, 605 (N.M. Ct. Crim. App. 2007) (holding that during a search for evidence, including photos or videos, of Appellant’s sexual misconduct with a child, an unmarked briefcase containing a binder of child pornography was in plain view and was admissible).

⁴ The court in *Washington* also distinguished the Air Force case of *United States v. Osorio*. *Washington*, 2011 CCA LEXIS, at *12-15. In *Osorio*, the government had a search warrant to search for pictures taken on one specific date, February 12, 2005. *United States v. Osorio*, 66 M.J. 632 (A.F. Ct. Crim. App. 2008). The Air Force court found that the Government exceeded the scope of the search warrant once it searched for photographs taken earlier than the specified date. *Id.* at 636. The Army Court reasoned that *Osorio*’s holding was limited to the facts of that case and the very specific ways in which the agent exceeded the scope of the warrant: “First, while capable of doing so, [the agent] did not search as required by the warrant for files within the specific date. Second, she specifically searched for child pornography rather than the evidence specified in the warrant.” *Washington*, 2011 CCA LEXIS, at *12. The Army court cited *Osorio* in its opinion in this case. *Gurczynski*, 2106 CCA LEXIS, at *6 n.3. However, the holding in *Osorio* is distinguishable from this case because the Government had a search warrant to search for communications between Appellee and DB that occurred between September 1, 2007 and December 28, 2011. (JA 68). The files of child pornography were created on or before June 12, 2010 and the image of Appellee and an unknown young male was created on March 20, 2010—both within the date range specified by the warrant. (JA 111, 68). Therefore, this evidence of child pornography was discovered in plain view.

To apply the plain view exception, the searching official's conduct must: (1) not violate the Fourth Amendment in arriving at the place from which the evidence could be plainly viewed; (2) the item's incriminating character must be immediately apparent; and (3) the officer must have a lawful right of access to the object itself. *Washington*, 2011 CCA LEXIS, at *8-9 (citing *Horton*, 496 U.S. at 136-37; *Coolidge v. New Hampshire*, 403 U.S. 443 (1971); *Arizona v. Hicks*, 480 U.S. 321, 326-27 (1987) (quotations omitted)).

Civilian federal decisions are consistent with *Washington's* application of the *Horton* test. In *United States v. Will*, law enforcement obtained a warrant to search for evidence of communications between a teacher and a student once the student accused the teacher of battery in the form of kissing her during the school day. *United States v. Will*, 2015 U.S. Dist. LEXIS 79887, at *3 (D. W. Va. June 19, 2015). The student told law enforcement that the teacher had contacted her on Facebook and Twitter and the law enforcement official sought the warrant to "make [his] case for battery stronger." *Id.* at *4, 8. The warrant authorized a search of digital media devices for these communications. *Id.* at *6. During the search, law enforcement officials found evidence of child pornography unrelated to the battery of the student. *Id.* at *8.

The court applied the *Horton* test in determining that the discovery of the child pornography on the defendant's computers fell under the plain view

exception. *Id.* at *20 (citing *Horton*, 496 U.S. at 136). First, law enforcement was authorized to search the defendant’s digital media devices. Second, the child pornography was immediately apparent as incriminating and illegal. Third, that valid warrant included the authorization to “open and cursorily view each file.” *Id.* at *21 (citing *Williams*, 592 F.3d at 522).

In *United States v. Childers*, the search warrant authorized a search for evidence of fraud, social security fraud, and other property offenses. *United States v. Childers*, 117 Fed. Appx. 633, 634 (10th Cir. 2004) (unpublished). During the execution of the warrant, federal agents discovered videotapes, some with sexually suggestive titles. The agent brought a stack of the videotapes to a TV-VCR combination and played a videotape. *Id.* The “videotape depicted what appeared to be an adult male and a twelve to fourteen year old boy engaged in sex.” *Id.* at 635. The agent then fast-forwarded to another part of the videotape and identified the adult male as the Appellant. *Id.* The court held that the agent did not exceed the scope the search warrant when he briefly viewed the videotape because he was authorized to cursorily review evidence to determine if it was evidence sought by the warrant. *Id.* The court held that a reasonable officer could conclude that the videotape contained evidence of social security fraud. *Id.*

In *United States v. Farlow*, a detective, posing as an underage boy, “received sexually suggestive emails . . . that included explicit sexual advances and a request

for an in-person meeting.” *United States v. Farlow*, 2009 U.S. Dist. LEXIS 112623, at *2 (D. Me. December 3, 2009). In at least one of these emails, the defendant sent a non-pornographic digital photograph of a bodybuilder, claiming it was of him. *Id.* at *3. The “potential crimes for which the warrant was authorized [were] the dissemination of indecent material to minors and endangering the welfare of child.” *Id.* at *13. The warrant authorized the search of digital media devices and computer records or data that were evidence of the crimes of dissemination of indecent material to minors or endangering the welfare of child, including but not limited to records of Internet use, electronic communications (such as email and email attachments), records or data pertaining to online chat room communications, text messages, word processing documents, software or programs for file sharing or peer-to-peer networks, etc. *Id.* at *4-5.

The detective used EnCase software to conduct his search the defendant’s computer. *Id.* at *10. When the detective conducted the search for the image of the bodybuilder that the defendant had sent, digital images of child pornography appeared on the screen. *Id.* at *6. The defendant alleged that the search exceeded the scope of the warrant. *Id.* at *6.

The detective testified that “the only reasonable way for an examiner to locate most of the copies of a particular image is to do it visually.” *Id.* at *23. The court held that when the investigator “visually tripped over evidence of the

commission of other crimes in plain view, he was not required to ignore it.” *Id.* at *24 (citing *United States v. Parker*, 549 F.3d 5, 10 (1st Cir. 2009)).

In this case, the DFE’s conduct meets all three prongs of the *Horton* test. First, the Government did not violate the Fourth Amendment in arriving at the place to be searched. The Government had a valid warrant to search Appellee’s digital media devices, including his thumb drive. (JA 169). The Government thus “arrived” at the “place” to be searched, i.e., opened the thumb drive, pursuant to the valid warrant. The software the DFE used showed all of the file names and images of the files. (JA 18-20). The thumb drive had no subfolders. (JA 18-20). Thus, the DFE lawfully gained the vantage point from which he saw the files in plain view.

Second, the child pornography’s incriminating nature was immediately apparent to the DFE. Based on his experience, the DFE immediately saw that the thumb drive contained images of child pornography. (JA 19).

Third, the DFE had a lawful right to “seize” the files. Unlike in physical-world seizure cases, the DFE here merely noted the existence of the child pornography and continued with his search for communications. There was no barrier between the DFE and the child pornography for the DFE to breach, and so there was no additional justification needed to see it and note its existence. *Cf. Washington v. Chrisman*, 455 U.S. 1 (1982) (considering under the “lawful access”

prong whether a police officer, who saw contraband in a dorm room from his position in the hallway, had a lawful right to enter the dorm room). Here, the thumb drive had no subfolders, (JA 18-19), so the DFE noted the child pornography's existence and continued with his search for communications.

Thus, each of the *Horton* conditions for the plain view exception was met, and continued to be met as the DFE continued his search for communications. The first condition was met when the Government obtained the valid warrant to search the thumb drive. That condition never changed. When the software opened all of the files at once and displayed their name and image, the child pornography's incriminating nature was immediately apparent; this continued to be the case as the DFE continued looking through the files for communications and saw more child pornography. None of the child pornography was protected by any sort of barrier, such as a subfolder, so, at all times following the opening of the drive pursuant to the warrant, the DFE had lawful access to the child pornography. Accordingly, the plain view exception applied, and this Court should set aside the military judge's ruling.

2. If this Court determines that the valid and particularized warrant was improperly expanded, then this Court should remand the case to the military judge to do a severability analysis.

The usual cause for employing the doctrine of severability of warrant is that the warrant lacked probable cause for some offenses alleged. *United States v.*

Galpin, 720 F.3d 436, 448 (2d Cir. 2013). “When a warrant is severable, the portion of the warrant that is ‘constitutionally infirm’ . . . is separated from the remainder and evidence seized pursuant to that portion is suppressed; evidence seized under the valid portion may be admitted.” *Id.* at 448 (citing *United States v. George*, 975 F.2d 72, 79 (2d Cir. 1992)). This doctrine gives weight to the balancing test discussed *infra*, where the judicial system “recognize[s] that the social gains of deterring unconstitutional police conduct by suppressing all evidence seized pursuant to a partially invalid warrant often are outweighed by the social costs occasioned by such an across the board ruling.” *George*, 975 F.2d at 79. Striking this balances acknowledges that “Fourth Amendment guarantees are adequately protected by suppressing only those items whose seizure is justified solely on the basis of the constitutionally infirm portion of the warrant” *Id.*

In *Galpin*, both the district court and the Second Circuit Court of Appeals found that the warrant was “facially overbroad” in that it “generally authorized officers to search [the Appellant’s] physical property and electronic equipment for evidence of violations of ‘NYS Penal Law and or Federal Statutes.’” *Galpin*, 720 F.3d at 447-48. The only crime that was specified in the warrant was a failure to comply with sex offender registration. *Id.* at 448. The Government conceded that there was no probable cause to believe that the appellant possessed or produced

child pornography even though the warrant itself authorized a search for images depicting child sexual activity. *Id.* at 448.

However, determining that the warrant was facially overbroad and lacked probable cause for an offense was only the first step in the court's analysis. *Id.* at 448. The court analyzed whether the warrant was (1) severable, meaning whether it "was possible to carve out the portions of the warrant that authorized a search for evidence of a registration offense from the constitutionally infirm remainder," and then (2) "whether the challenged evidence was in plain view when it was seized." *Id.* at 448. The court held that the proper remedy was to remand to the district court in order to conduct this two-step analysis.⁵ *Id.* at 448.

⁵ The court specifically laid out a "step-by-step methodology" to severability of the warrant. *Id.* First, the court must separate the warrant into "its constituent clauses." *Id.* Second, the court must examine each individual clause to determine whether it is sufficiently particularized and is supported by probable cause. *Id.* at 448-49. Third, the court must be able to determine whether valid parts of the warrant are distinguishable from the non-valid parts, meaning categories of items to be properly seized are not linked to the language of other categories and "each valid category [must] retain[] its significance when isolated from the warrant as a whole." *Id.* (citing *United States v. Sells*, 463 F.3d 1148, 1158 (10th Cir. 2006)). In other words, in order for severability to be a valid solution, the "court must be able to excise from the warrant those clauses that fail the particularity or probable cause requirements in a manner that leaves behind a coherent, constitutionally compliant redacted warrant." *Id.* The court must also determine that the valid portions are not only "an insignificant or tangential part of the warrant." *Id.* (citing *George*, 975 F.2d at 80).

In this case, the military judge found that the warrant was valid and particularized. (JA 169). The warrant established probable cause to search Appellee’s digital media devices “for evidence of communications between [Appellee and DB] wherein [Appellee] coaxed the alleged victim into participating in sexual acts/contacts.” (JA 170). The military judge confirmed that communications could “arguably and logically include pictures and even child pornography, if such child pornography were part of a communication or possible communication to [DB].” (JA 170). However, the military judge held that the warrant did not establish probable cause for child pornography apart from DB and that it was the request from the CID office at the Presidio of Monterey that “improperly expanded the scope of [the federal] warrant.” (JA 170).

If this Court agrees that the facially valid warrant was expanded, contrary to the DFE’s testimony, then this Court should remand the case back to the military judge for him to do a severability analysis and then apply plain view analysis. Considering that the military judge has already found that the warrant was based on probable cause of the offenses alleged—attempted aggravated sexual assault of a child, indecent acts with a child, attempted sexual abuse of a child, abusive sexual contact with a child, child endangerment—then his severability analysis will be simple. He can reaffirm the valid warrant, sever what he believes is an improper expansion, and then determine whether the child pornography was

discovered in plain view while the DFE was searching for evidence of communications between Appellee and DB.

C. The military judge abused his discretion in suppressing this evidence because the deterrent effect of suppression is minimal and does not outweigh the direct harm to the justice system.

The exclusionary rule is a judicially-created rule for Fourth Amendment violations and suppression is not automatic. *Wicks*, 73 M.J. at 103. “The exclusionary rule ‘applies only where it results in appreciable deterrence’ for future Fourth Amendment violations and where the ‘benefits of deterrence must outweigh the costs.’” *Id.* at 104 (quoting *United States v. Herring*, 555 U.S. 135, 141 (2009)). Moreover, the Supreme Court stated, “exclusion ‘has always been our last resort, not our first impulse.’” *Herring*, 555 U.S. at 140. Accordingly, the “rule’s costly toll upon truth-seeking and law enforcement objectives presents a high obstacle for those urging its application.” *Id.* at 141.

Here, despite “repeated holdings” by the Supreme Court establishing this balancing test, *id.* at 147, this Court applying the balancing test in *Wicks*, and recent modifications to Mil. R. Evid. 311, the military judge did not even address the balancing test in his ruling.⁶ (JA 166-71). *Herring* and *Wicks* are binding

⁶ Military Rule of Evidence 311(a) was modified to expressly include this balancing test and authorizes the exclusion of evidence only if three criteria have been met: 1) the filing of a timely motion to suppress; 2) a finding that the accused has a reasonable expectation of privacy; and 3) “exclusion of the evidence results in appreciable deterrence of future unlawful searches or seizures and the benefits

precedent and the military judge abused his discretion in failing to adhere to their holdings. Accordingly, this Court should grant the military judge's erroneous ruling no deference.

Applying the balancing test to this case, the deterrent effect of suppression is low because law enforcement did not engage in "deliberate, reckless, or grossly negligent" conduct. *Herring*, 555 U.S. at 143 (stating "an assessment of the flagrancy of the police misconduct constitutes an important step in the calculus"). Here, law enforcement did not engage in wanton misconduct. They did not provide false information to the federal magistrate to obtain a search warrant. (JA 68-73). Moreover, the scope of the DFE's search did not exceed the warrant, which makes this case distinguishable from *Wicks*. In *Wicks*, the Government's search included reviewing "tens of thousands of text images" and it far exceeded the private search of a "few texts, photographs, and one video" by a third party. *Wicks*, 73 M.J. at 104. Here, the DFE had to search the thumb drive pursuant to the search warrant to identify any potential communications between DB and Appellee as discussed *supra*. Finally, the toll upon truth-seeking and law enforcement objectives is high because this is the only evidence showing


of such deterrence outweigh the costs to the justice system." Mil. R. Evid. 311(a)(3). Since the effective date of the amendment was May 20, 2016, it did not apply to Appellee's court-martial, but the change to the rule only reflected the precedent established by case law.


Appellee's possession of images depicting the sexual exploitation and abuse of children.


Conclusion


This Court should set aside the military judge's ruling because the child pornography was discovered while the agent was acting within the scope of the warrant. Even if, after a de novo review, this Court concludes that the child pornography was not contemplated by the warrant, this Court should set aside the military judge's ruling because the plain view exception applies. Finally, the military judge abused his discretion in suppressing this evidence because the deterrent effect of suppression is minimal and does not outweigh the direct harm to the justice system.

Wherefore, the United States respectfully requests that this Honorable Court set aside the military judge's ruling to suppress evidence from Appellee's thumb drive.


for CARLING M. DUNHAM
Captain, U.S. Army
Appellate Counsel
Government Appellate Division
U.S.C.A.A.F. Bar No. 36357


SAMUEL E. LANDES
Captain, U.S. Army
Branch Chief, Government
Appellate Division
U.S.C.A.A.F. Bar No. 36626


A.G. COURIE III
Lieutenant Colonel, Judge Advocate
Deputy Chief, Government
Appellate Division
U.S.C.A.A.F. Bar No. 36422


MARK H. SYDENHAM
Colonel, Judge Advocate
Chief, Government Appellate
Division
U.S.C.A.A.F. Bar No 34432

CERTIFICATE OF COMPLIANCE WITH RULE 24(d)

1. This brief complies with the type-volume limitation of Rule 24(c) because:

This brief contains 9,959 words.

2. This brief complies with the typeface and type style requirements of Rule 37 because:

This brief has been typewritten in 14-point font with proportional, Times New Roman typeface using Microsoft Word Version 2013.

A handwritten signature in black ink, appearing to read 'S. Landes', is positioned above the printed name.

SAMUEL E. LANDES
Captain, Judge Advocate
Attorney for Appellant
December 21, 2016

CERTIFICATE OF FILING AND SERVICE

I certify that the foregoing brief in support of certification, *United States v. Gurczynski*, Crim. App. Misc. Dkt. No. 20160402, USCA Dkt. No. _____/AR, was electronically filed with the Court (efiling@armfor.uscourts.gov) on December 21, _____ 2016 and contemporaneously served electronically on appellate defense counsel.



DANIEL L. MANN
Lead Paralegal Specialist
Office of The Judge Advocate
General, United States Army
9275 Gunston Road
Fort Belvoir, VA 22060-5546
(703) 693-0822