

# UNITED STATES ARMY COURT OF CRIMINAL APPEALS

Before  
BERGER, MULLIGAN, BURTON  
Appellate Military Judges

**UNITED STATES, Appellee**  
**v.**  
**Sergeant First Class JAMES E. HOPKINS**  
**United States Army, Appellant**

ARMY 20140913

Headquarters, U.S. Army Fires Center of Excellence and Fort Sill (trial)  
Headquarters, U.S. Army Combined Arms Center and  
Fort Leavenworth (*DuBay* hearing)  
Jeffery R. Nance, Military Judge (arraignment)  
Charles L. Pritchard, Jr., Military Judge (trial)  
J. Harper Cook, Military Judge (*DuBay* hearing)  
Colonel David E. Mendelson, Staff Judge Advocate

For Appellant: Captain Heather L. Tregle, JA; Captain Joshua G. Grubaugh, JA (on brief); Captain Katherine L. DePaul, JA; William E. Cassara, Esquire (on supplemental brief and supplemental reply brief following a *DuBay* Hearing); Lieutenant Colonel Christopher D. Carrier, JA; William E. Cassara, Esquire (on brief in response to specified issues upon reconsideration).

For Appellee: Major Daniel D. Derner, JA (on brief); Colonel Mark H. Sydenham, JA; Lieutenant Colonel A.G. Courie III, JA; Major Melissa Dasgupta Smith, JA; Captain Jennifer A. Donahue, JA (on supplemental brief following a *DuBay* Hearing); Lieutenant Colonel Eric K. Stafford, JA; Captain Austin L. Fenwick, JA; Captain KJ Harris, JA; Captain Joshua Banister, JA (on brief in response to specified issues upon reconsideration); Lieutenant Colonel Eric K. Stafford, JA, Captain Austin L. Fenwick, JA (on reply brief in response to specified issues upon reconsideration).

25 May 2018

-----  
MEMORANDUM OPINION UPON RECONSIDERATION AFTER REMAND  
-----

*This opinion is issued as an unpublished opinion and, as such, does not serve as precedent.*

BURTON, Senior Judge:

The government charged appellant with committing various forms of sexual misconduct against his two step-daughters, ZJEH and CBV, spanning from 2008 to 2013. A military judge sitting as a general court-martial convicted appellant,

contrary to his pleas, of rape of a child, sexual assault, indecent act, sexual assault of a child, two specifications of sexual abuse of a child, wrongfully providing alcohol to a minor, and obstructing justice in violation of Articles 120, 120b, and 134, Uniform Code of Military Justice (UCMJ), 10 U.S.C. §§ 920, 920b, 934. The military judge found appellant not guilty, in accordance with his pleas, of one specification each of producing and possessing child pornography in violation of Article 134, UCMJ. The military judge sentenced appellant to a dishonorable discharge, confinement for forty-two years, and reduction to the grade of E-1. The convening authority approved forty-one years and ten months confinement but otherwise approved the findings and sentence as adjudged.

This case is before us on remand to address whether appellant was denied effective assistance of counsel and to “complete [our] Article 66(c), UCMJ, review.” *United States v. Hopkins*, ARMY 20140913 (C.A.A.F. 5 May 2016) (order). In our view, “completing” our statutory obligation requires a plenary review. *See United States v. Swift*, 76 M.J. 210, 216 (C.A.A.F. 2017). We issued a decision in the case addressing ineffective assistance of counsel and *United States v. Hills*, 75 M.J. 350 (C.A.A.F. 2016), propensity error. *United States v. Hopkins*, ARMY 20140913, 2017 CCA Lexis 431 (Army Ct. Crim. App. 26 June 2017) (summ. disp. on remand). Appellant asks us to reconsider this decision with respect to our analysis of appellant’s ineffective assistance of counsel claim, to evaluate the case pursuant to our superior court’s decision in *United States v. Hukill*, 76 M.J. 219 (C.A.A.F. 2017), and to address whether the search and seizure of items at appellant’s off-post residence was supported by probable cause. We fully adopt our previous decision with respect to appellant’s ineffective assistance of counsel claim, grant relief with respect to several specifications affected by the *Hills* and *Hukill* error, and determine the search of appellant’s residence complied with the Fourth Amendment.

## BACKGROUND

The crimes appellant was convicted of committing against his two step-daughters included: digitally penetrating both girls’ genitalia on separate occasions<sup>1</sup>; plying ZJEH and her friend JA with alcohol<sup>2</sup> as a means of facilitating

---

<sup>1</sup> In Charge I, Specification 1, appellant was charged with rape of a child by digitally penetrating ZJEH’s genital opening with his finger when she was approximately ten to eleven years old. In Charge I, Specification 2, appellant was charged with sexual assault against CBV by digitally penetrating her vulva when she was seventeen.

<sup>2</sup> In Charge III, Specification 3, appellant was charged with wrongfully providing alcohol to both JA and ZJEH when they were respectively fifteen and fourteen years old.

another digital penetration of ZJEH's vulva with his finger<sup>3</sup>; committing lewd acts against both ZJEH and her friend JA<sup>4</sup>; and surreptitiously video recording each of his step-daughters naked in the bathroom<sup>5</sup>.

The allegations against appellant arose approximately six months after appellant moved out of his marital home and filed for divorce against the girls' mother, BL. In June 2013, BL moved into appellant's new residence in an attempt to reconcile. While BL was alone at the residence she found pictures on appellant's Dell computer of appellant molesting her daughter ZJEH while ZJEH appeared to be asleep.<sup>6</sup> BL left the residence to confront appellant in person, but failed to secure the computer. While on the way to see appellant, she called him on the phone and confronted him. BL testified appellant stated "he didn't remember doing it, that he must have been drunk." She later returned to the residence to secure the computer and appellant was sitting on the front porch. He informed her "he had gotten rid of the computer, that it was destroyed as well as the SIM card." She entered the residence and the computer was gone.<sup>7</sup>

---

<sup>3</sup> In Charge II, Specification 1, appellant was charged with sexual assault of a child against ZJEH by digitally penetrating her vulva with his finger when she was approximately fourteen years old.

<sup>4</sup> In Charge II, Specification 2, appellant was charged with sexual abuse of a child by asking ZJEH, who was approximately fourteen years old, to take nude photographs of herself and provide them to him. In Charge II, Specification 3, appellant was charged with sexual abuse of a child by telling JA, who was approximately fifteen years old, she was jail bait and stating the two of them could have sexual intercourse together.

<sup>5</sup> Appellant separately video-recorded CBV and ZJEH naked in the bathroom. In Charge I, Specification 3, appellant was charged with an indecent act by video recording the genitalia, breasts, and buttocks of CBV. The recordings also formed the basis for Charge III, Specifications 1 and 2, where appellant was respectively charged with producing and possessing child pornography resulting from three video-recordings of CBV and one video-recording of ZJEH. Appellant was acquitted of the child pornography charges.

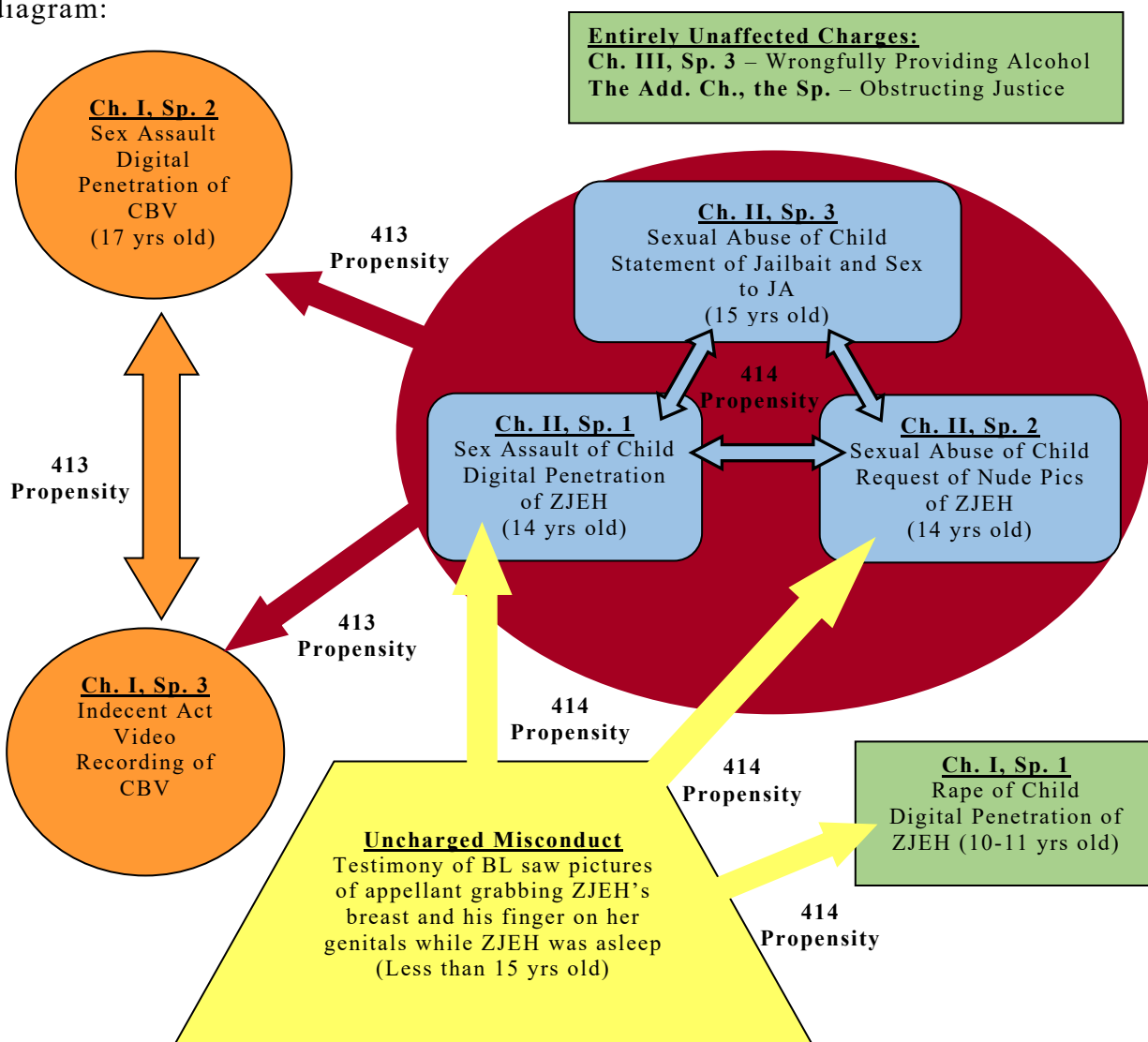
<sup>6</sup> The government used BL's testimony regarding the existence of these photographs as uncharged Military Rule of Evidence [Mil. R. Evid.] 413 misconduct.

<sup>7</sup> In the Specification of The Additional Charge appellant was charged with obstructing justice by destroying a DELL computer.

## LAW AND ANALYSIS

A. *The Erroneous Use of Propensity Evidence*

It is constitutional error to allow evidence of charged offenses to establish an appellant's propensity to commit other charged offenses. *See United States v. Guardado*, 77 M.J. 90, 93 (C.A.A.F. 2017); *Hukill*, 76 M.J. at 220; *Hills*, 75 M.J. at 352. Here, the military judge granted the government's motion to use *uncharged* and *charged* misconduct as propensity evidence. The *uncharged* misconduct ruling was, and remains, uncontested by the parties. The defense counsel at trial preserved the issue as to the *charged* misconduct and appellant asserts error on appeal. The military judge detailed which offenses could be used as propensity evidence for other specific offenses. The military judge's ruling is represented in the following diagram:



Of considerable note, Specification 1 of Charge I, the digital penetration of ZJEH's genital opening when she was approximately ten or eleven years old could not be used for any propensity purposes and remained unaffected by propensity evidence from any other charged offense, although it was affected by the unchallenged and uncharged propensity evidence. Furthermore, Specification 3 of Charge III, wrongfully providing alcohol to ZJEH and JA, and the Specification of The Additional Charge, obstructing justice, were entirely unaffected by any propensity ruling.

The error, here, was preserved and is of constitutional dimensions. *Hukill*, 76 M.J. at 221. The only remaining question is whether the error was harmless beyond a reasonable doubt with respect to each of the affected specifications. *Id.* An error "is not harmless beyond a reasonable doubt when there is a reasonable possibility that the error complained of might have contributed to the conviction." *Id.* (internal citations omitted).

In *Guardado*, the Court of Appeals for the Armed Forces (CAAF) did "not disturb [this court's] finding that [the victim]'s testimony was credible" yet found "the lack of supporting evidence ma[de] it difficult to be certain that [MSG Guardado] was convicted [] on the strength of the evidence alone." 77 M.J. at 94. The evidence against MSG Guardado consisted solely of the testimony of his accusers. *Id.* The court was not convinced that the erroneous propensity instruction played no role in MSG Guardado's conviction and was unable to conclude the erroneous instruction was harmless. *Id.* at 95.

In *Hukill*, the CAAF assessed prejudice by looking at the underlying evidence supporting the government's charge. 76 M.J. at 223. The Court found "the government's case was based entirely on the testimony of the victims and the alleged confession from [SPC] Hukill to his fiancée that he had been unfaithful, all of which [SPC] Hukill denied. No other evidence was offered." *Id.* On these facts, the CAAF found, "the Government failed to prove there was no reasonable possibility that the error contributed to the verdict." *Id.*

Similarly, in *United States v. Hills*, there was "no eyewitness testimony other than the allegations of the accuser" and "there was no conclusive physical evidence." 75 M.J. at 358. As such, the CAAF held there was no way to know whether the erroneous instructions "tipped the balance in the members' ultimate determination." *Id.*

In contrast, our superior court has found no prejudice for a *Hills* error and summarily affirmed convictions where evidence included independent eyewitness testimony and incriminating admissions by an appellant. *See United States v. Moore*, 77 M.J. 198 (C.A.A.F. 2018); *United States v. Luna*, 77 M.J. 198 (C.A.A.F. 2018).

Here, our 26 June 2017 decision rested almost exclusively on the compelling and detailed nature of the testimony of appellant's accusers. For each of the affected charges, we relied heavily on the military judge finding ZJEH to be a credible witness with respect to the unaffected charge of Specification 1 of Charge I and that uncharged propensity evidence was properly admitted against appellant.

Yet, the credibility of the accusers in *Guardado* was not enough to render the erroneous propensity evidence harmless. 77 M.J. at 94. Here, the uncharged propensity evidence itself consisted solely of the testimony of BL, appellant's ex-wife, who did not witness the actual uncharged acts, but rather testified she saw evidence of the acts on appellant's computer. The digital evidence itself of the uncharged acts was never entered into evidence, as it was never found. We are mindful that this testimony is similar in nature to the alleged confession SPC Hukill made to his fiancée about being unfaithful. *Hukill*, 76 M.J. at 223. In both cases, the evidence consisted solely of testimony without any supporting physical evidence, and in both instances each appellant took the stand and disavowed not only the accusations, but the averred admissions.

As such we are not convinced the erroneous use of propensity evidence played no role in appellant's convictions with respect to Specification 2 of Charge I and Charge II and its specifications. We provide appropriate relief in our decretal paragraph below. Specification 1 of Charge I, Specification 3 of Charge III and the Specification of The Additional Charge were entirely unaffected by an improper use of propensity evidence.

Here, the sole specification affected by the *Hills* error that was supported by physical or documentary evidence was Specification 3 of Charge I. This specification was supported by the digital evidence of the videos contained on Pros. Ex. 13. This is the type of evidence where we could rest assured that an erroneous propensity instruction did not contribute to the verdict. However, appellant additionally challenges the search and seizure that recovered this evidence.

#### *B. The Video Evidence of Specification 3 of Charge I*

In pretrial motions practice, trial defense counsel preserved challenges to the underlying video evidence supporting Specification 3 of Charge I, asserting the search of appellant's residence was unsupported by probable cause and lacked particularity in violation of the Fourth Amendment. We hold the Federal Magistrate Judge had a substantial basis for finding probable cause and the warrant was not overbroad.

### 1. *The Fourth Amendment and Probable Cause*

The Fourth Amendment requires a search warrant be supported by probable cause. U.S. Const. amend. IV. Probable cause requires a sufficient nexus between the alleged crime and the item to be seized. *United States v. Nieto*, 76 M.J. 101, 106 (C.A.A.F. 2017) (citing *United States v. Rogers*, 67 M.J. 162, 166 (C.A.A.F. 2009); *United States v. Gallo*, 55 M.J. 418, 421 (C.A.A.F. 2001)). “The question of nexus focuses on whether there was a ‘fair probability’ that contraband or evidence of a crime will be found in a particular place.” *United States v. Clayton*, 68 M.J. 419, 424 (C.A.A.F. 2010) (quoting *United States v. Leedy*, 65 M.J. 208, 213 (C.A.A.F. 2007)). “A nexus may be inferred from the facts and circumstances of a particular case, including the type of crime, the nature of the items sought, and reasonable inferences about where evidence is likely to be kept.” *Nieto*, 76 M.J. at 106 (internal quotations omitted).

We review a military judge’s denial of a motion to suppress for an abuse of discretion and consider the evidence in the light most favorable to the prevailing party. *United States v. Eppes*, 2018 CAAF LEXIS 202, \*9 (C.A.A.F. 2018). This court gives “‘great deference’ to [a] magistrate’s probable cause determination because of ‘the Fourth Amendment’s strong preference for searches conducted pursuant to a warrant.’” *Nieto*, 76 M.J. at 105 (quoting *Illinois v. Gates*, 462 U.S. 213, 236 (1983)). This court will uphold a military judge’s ruling to deny a suppression motion where the magistrate had a substantial basis for concluding probable cause existed. *Eppes*, 2018 CAAF LEXIS 202, at \*12, \*14 (citing *Nieto*, 76 M.J. at 105). “A substantial basis exists ‘when based on the totality of the circumstances, a common-sense judgment would lead to the conclusion that there is a fair probability that evidence of a crime will be found at the identified location.’” *Id.* at \*12 (quoting *Nieto*, 76 M.J. at 105 (quoting *Gates*, 462 U.S. at 238)).

*Nieto* is a case in which the CAAF held a military magistrate did not have a substantial basis to determine probable cause existed to search a laptop. 76 M.J. at 103. In *Nieto*, law enforcement suspected SPC Nieto of using his cell phone to surreptitiously record other male soldiers while they used the toilet on a Forward Operating Base. *Id.* at 104. Two non-commissioned officers looked through SPC Nieto’s phone and did not find any photographs or videos. *Id.* at 103. During the course of the investigation “somebody” had seen a cell phone and laptop on SPC Nieto’s bunk. *Id.* Law enforcement sought a search authorization to search and seize this cell phone and laptop. *Id.* In support of the search authorization a special agent submitted a sworn statement from one of the latrine victims, an affidavit concerning the investigation, and met in-person with the magistrate. *Id.* at 104. The sworn statement and the affidavit made no mention of a laptop computer. *Id.* During the in-person meeting with the magistrate the special agent informed the magistrate of his knowledge that Soldiers “normally” store photos taken with their

phones on their laptops. *Id.* However, the agent did not provide any details about any laptop SPC Nieto may have owned. *Id.*

The CAAF held the military magistrate did not have a substantial basis to find probable cause to search SPC Nieto's laptop and the generalized profile about how soldiers "normally" store images was "technologically outdated." *Id.* at 107-08. The CAAF concluded "at a minimum—there needed to be some additional showing such as the fact that [SPC Nieto] actually downloaded images (illicit or otherwise) from his cell phone to his laptop, stored images on his laptop, or transmitted images from his laptop. And yet, there was no such showing in [SPC Nieto's] case." *Id.* at 107. The CAAF noted that even SPC Nieto's ownership of a laptop was predicated on suspect information as the agent could not explain how he learned of the laptop. *Id.* at 108, n.4. In a footnote, the CAAF warned against "providing law enforcement with broad authority to search and seize *all* of an accused's electronic devices and electronic media merely because the accused used a cell phone in furtherance of a crime," stating such a generalized proposition would "run counter to the principle that law enforcement officials must provide specific and particular information in order for a magistrate to determine [probable cause]." *Id.* at 108, n.5.

In contrast, *Eppes* is a case in which the CAAF held a civilian judge did have a substantial basis to determine evidence of fraud against the government would probably be recovered on a computer in Capt. Eppes' home. 2018 CAAF LEXIS 202, at \*14. The civilian judge authorized the search of Capt. Eppes' home and his "computer hardware, computer software and digital media (e.g., computer equipment, digital storage devices, cameras, photographs, etc.) . . ." *Id.* at \*5. The affidavit supporting the warrant asserted Capt. Eppes had submitted numerous false documents to various individuals to include false claims made to a hotel's personnel via email. *Id.* at \*14-15. The affidavit also asserted Capt. Eppes had previously engaged in similar misconduct involving fraud and Capt. Eppes was a law enforcement official. *Id.* at 15.

The CAAF held, "[t]he fact that the affidavit stated [Capt. Eppes] had used email to communicate with the hotel personnel raised a reasonable inference [Capt. Eppes] probably used a computer or other digital device or media as an instrumentality to pursue the suspected fraudulent scheme." *Id.* The CAAF held it was a reasonable inference that evidence of the criminal conduct probably resided on such devices and that because of Capt. Eppes' law enforcement background it was a reasonable inference that such devices would be found at his residence rather than a shared workspace or government computer. *Id.* The CAAF specifically cautioned, "[w]ithout some other incriminating facts, a search authority cannot reasonably infer that the average servicemember is more likely to store evidence of criminality on his home computer than on his work computer." *Id.* at 16, n.5.



*a. Ms. BL's Discovery of the Crimes and Report to Law Enforcement*

It was late June when Ms. BL discovered approximately fifteen photographs of appellant molesting her daughter, ZJEH, on appellant's computer in his new residence. After discussing the photographs with both of her daughters, Ms. BL reported appellant to the local police department on 12 July 2013. On 11 September 2013, Ms. BL gave a sworn statement to U.S. Army Criminal Investigation Command (CID) special agents, informing them the computer was a Dell tower attached to the TV in the entertainment center of appellant's living room and it may have been black and gray. She also informed them appellant told her in June he had destroyed both the computer and the SIM card to his phone when she confronted him. She stated she went into the house that night in June and the computer was gone. Reflecting on appellant's comment she indicated that appellant did not have time to destroy the items that evening, but she was certain the items were gone now in mid-September. She informed investigators that the phone appellant used when she confronted him was a black Droid, possibly a Razor, and that she gave the iPhone she used that evening back to appellant because she was no longer on his phone plan.

*b. The Information Included in the Affidavit and Warrant*

On 25 September 2013, CID sought a search warrant of appellant's off-post residence from a Federal Magistrate Judge in the Western District of Oklahoma. The affidavit supporting the warrant stated that the CID agent requesting the warrant had served since July 2012 as an agent, had participated in numerous criminal investigations, and had attended the Special Victims Unit Investigative Course and Child Abuse and Prevention Techniques Course. It stated appellant was suspected of committing sexual misconduct with minors to include producing child pornography. In pertinent part it stated:

3. On July 12, 2013, Ms. [BL] reported the above allegations to Lawton Police Department, Lawton, OK (LPD). Ms. [BL] was initially interviewed by Lawton Police and later interviewed by this office on September 11, 2013, wherein she stated sometime in late June, 2013, she was looking through old photographs on [appellant's] computer when she ran across a folder labeled "Z". Ms. [BL] stated the folder contained approximately 15 photographs of [ZJEH], who appeared to be drunk and passed out on [appellant's] couch. Ms. [BL] stated the pictures appeared to be taken from [appellant's] cell phone and she recognized his hand in them. Ms. [BL] stated some of the photographs depicted [appellant's] hand lifting [ZJEH's] shirt and fondling her breasts. Other

photographs depicted [appellant's] hand pulling [ZJEH's] shorts and underwear down, exposing her genital area. Ms. [BL] stated she left the residence to confront [appellant], but couldn't wait and decided to text him instead, asking, "What the hell is going on with pictures of [ZJEH] on your computer?" Ms. [BL] stated he told her through text message that he didn't remember taking the pictures and he must have been drunk. [Appellant] also told her that he was disgusted with himself and he didn't know why he would do that.

4. Ms. [BL] further stated she went back to [appellant's] residence to take the computer to the police but [appellant] arrived before she did and said he "destroyed" the computer and the SIM card from his phone. Ms. [BL] later asked [ZJEH] if [appellant] ever touched her inappropriately and both [ZJEH] and [CBV] disclosed to her at that time that [appellant] had molested them.

The affidavit stated that MS. BL gave her cell phone back to appellant at the end of July 2013. It summarized interviews conducted with ZJEH and CBV regarding the sexual molestation appellant committed against each of them. The summaries included details that appellant used his cell phone to text sexual comments to both ZJEH and her friend JA. Lastly, the affidavit included a statement that "[b]ased on [the agent's] training and experience as a CID Special Agent, suspects treat their child pornographic media as prized possessions and rarely delete or destroy the media."

The affidavit requested, "authorization to search appellant's residence for information related to the listed offenses, in whatever form it may be found, physical, hard copy or electronic, specifically including any digital devices and storage media found therein, as more fully described in Attachment A, incorporated herein by reference, authorization to seize any such items or information found therein and authorization for the subsequent search of seized digital devices and storage media." Attachment A consisted of three pages listing a litany of different digital devices, components, media, electronic access materials, and types of electronic evidence that could conceivably be seized and searched. The affidavit also included Attachment B, detailing the location of appellant's off-post residence.

The Federal Magistrate Judge authorized the search on 25 September 2013 incorporating the affidavit by reference. Agents executed the warrant later that day, seizing several digital storage devices. The only item of evidentiary value recovered from appellant's residence was an external hard drive. The hard drive contained

three video-recordings of CBV and one video-recording of ZJEH each naked in the bathroom.

*c. Suppression Hearing and Ruling*

Trial defense counsel sought to suppress the videos of CBV and ZJEH based on a lack of probable cause and particularity contained in the warrant and underlying affidavit. At the suppression hearing neither party introduced any testimonial evidence, thereby limiting consideration of the issues to the four-corners of the warrant, affidavit, and attachments A and B to the affidavit.

There was no indication that any of the other sworn statements or investigative files trial counsel asked the military judge to consider for purposes of determining the motion had been provided to the Federal Magistrate Judge on 25 September 2013 or that the Federal Magistrate Judge had been provided any information orally for his consideration. In addition, the military judge requested the parties submit the custodial documents regarding the evidence collected from appellant's residence for his consideration. These documents, App. Ex. XIII, show that a Dell computer and the external hard drive in question were both seized from the "entertainment center" in appellant's living room.<sup>8</sup>

---

<sup>8</sup> At the suppression hearing, the parties did not enter any evidence regarding what if anything was collected from appellant's residence or where such evidence was collected from within appellant's home until the military judge specifically asked for the custody documents regarding the items sought to be suppressed. In this case, these documents failed to address the most material piece of information from the government's perspective: the fact that the external hard drive on which the government's evidence was found was actually connected to a Dell computer found in the same location as Ms. BL's description detailed in the affidavit.

Although not presented to the military judge for his consideration on the suppression motion, at trial the agent clarified "[t]he external hard drive was sitting on top of the computer" and "it was behind the closed cabinet door, but was connected to the computer." This information was only introduced at the trial on the merits and therefore could not be considered in any analysis of whether or not the military judge abused his discretion in ruling on the motion to suppress. While this ultimately does not change the outcome in this case, there are cases where the connection of one piece of evidence to another or located nearby another that is clearly supported by probable cause will matter. It is also prudent practice to remember that application for additional warrants and search authorizations may be made once more specific information is known.

After reviewing the law and detailing his findings of fact, the military judge made the following conclusions:

It is true that the two girls did not state that they were aware of any movies or photographs being taken of them [in the bathroom] on those occasions. It is also true that Ms. [BL] stated that [appellant] told her he had destroyed the computer upon which she discovered the improper photos of [ZJEH] as well as the SIM card from his phone and that when she entered the residence after he told her those things she did not see the computer in its normal place.<sup>9</sup> Nevertheless, Ms. [BL] had seen evidence of child pornography and child molestation on the accused's computer just weeks before the warrant was issued, there was evidence of other similar acts of providing alcohol to and molesting [ZJEH] and others in the form of the statements from the girls, Ms. [BL] did not see him destroy anything, the photos were likely created by one digital device and transferred to the computer, and based, upon the experience of [the CID agent], people who produce and possess child pornography tend to save it on other media than just the hard drive of a computer.<sup>10</sup> Common sense and normal inferences provide a substantial basis to believe that the accused saved the same pictures or other similar recordings on other electronic media and that those and/or the original computer itself were still located in his residence.

The military judge determined the Federal Magistrate Judge had a substantial basis to determine probable cause to conduct the search. He further held even if there was not actual probable cause the good faith exception to the exclusionary rule was satisfied because the CID agent “had an objectively reasonable belief that [the

---

<sup>9</sup> Ms. BL's statement that the computer was not in the house after she confronted appellant was not provided in the affidavit or attachments given to the Magistrate Judge, but was included in the sworn statements provided by trial counsel for the military judge to consider on the motion to suppress.

<sup>10</sup> The actual statement in the affidavit asserts “suspects treat their [c]hild [p]ornographic media as prized possessions and rarely delete or destroy the media.” The affidavit does not actually mention saving files, copying them, or transferring them to other media.

Federal Magistrate Judge] had a ‘substantial basis’ for determining the existence of probable cause and [the agent] objectively relied in good faith on the authorization (warrant).” Having determined the basis for probable cause, the military judge did not otherwise address trial defense counsel’s arguments regarding the over-breadth of the warrant and lack of particularity.

*d. A Substantial Basis for Probable Cause to Search Appellant’s Home*

We are mindful that our review is not to determine whether probable cause existed anew, but rather we review the information presented to the magistrate to determine whether the magistrate had a substantial basis for determining probable cause. *Nieto*, 76 MJ. at 105. “In evaluating the issuing search authority’s probable cause finding, we examine: 1) the facts known to the authority when he issued the warrant and 2) the manner in which he came to know these facts.” *Eppes*, 2018 CAAF LEXIS, at \*13. “Resolution of doubtful or marginal cases should be largely determined by the preference for warrants, and close calls will be resolved in favor of sustaining the search authority’s decision.” *Id.* at \*11-12 (citations omitted).

Here, appellant avers the affidavit supporting the Federal Magistrate Judge’s search warrant for appellant’s off-post residence did not provide a sufficient nexus between the alleged crime and the items to be seized because the affidavit contained generalizations based on the agent’s training and experience. However, the plain language of *Nieto* is not quite so narrow. *Nieto* does not stand for the proposition that a generalized profile may not be used, but rather a generalized profile itself is not enough to establish the necessary link of probable cause. 76 M.J. at 106 (“A law enforcement officer’s professional experience may be useful in establishing such a nexus. However, a law enforcement officer’s generalized profile about how people normally act in certain circumstances does not, *standing alone*, provide a substantial basis to find probable cause to search and seize an item in a particular case; there must be some additional showing that the accused fit that profile or that the accused engaged in such conduct.” (emphasis added) (internal citations omitted)).

Here, the affidavit clearly establishes the requisite nexus of probable cause to find evidence of a crime on three specific devices: appellant’s computer; appellant’s phone; and the phone Ms. BL used, but gave back to appellant sometime near the end of July, 2013.<sup>11</sup> Paragraph 3 of the affidavit establishes a fair probability of

---

<sup>11</sup> It is worth noting on 11 September 2013 law enforcement asked Ms. BL for descriptions of the items and determined they were: possibly a black and gray Dell tower computer previously attached to the TV in the entertainment center of appellant’s living room; a black Droid phone, possibly a Razor; and a Verizon iPhone. Yet, none of these descriptions were provided to the Federal Magistrate

(continued . . .)

finding digital evidence on the computer relating to the approximately fifteen photographs BL stated she saw in mid-June. Further, paragraph 3 also establishes a fair probability of finding on both phones text messages and call log correspondence regarding Ms. BL's accusations to appellant upon her discovery of the photographs, along with his responses. It is also clear there was a fair probability of finding additional incriminating evidence on appellant's phone because the videos of appellant molesting ZJEH appeared to have been recorded from a phone and appellant had texted sexual comments to both ZJEH and her friend JA.

While there was probable cause to search these particular devices for evidence of a crime, the nexus between the information presented in the affidavit and the reasonable probability that the devices themselves would be found in appellant's off-post residence is a much closer call. Here paragraph 4 of the affidavit establishes appellant informed Ms. BL that he destroyed both the computer and the SIM card from his phone.<sup>12</sup> However, it is a reasonable inference that appellant made self-serving statements on the night Ms. BL confronted him and given the short period of time between appellant being alerted of the photographs' discovery and Ms. BL's return to the residence it is likely the items were still in the home that evening. The problem is the time period between this confrontation and the actual search of appellant's residence.

Although the military judge characterized Ms. BL as having seen the computer "just weeks before the warrant issued," a period of almost, if not more than, three months had elapsed. The affidavit establishes Ms. BL saw the photographs in late June 2013, yet the warrant was applied for and issued on 25 September 2013. Although we disagree with the military judge regarding his characterization of the time period, we arrive at the same result because of the profile traits of suspects who have child pornography and the persisting nature of digital evidence.

The affidavit underlying the warrant specifically referenced the CID agent's training and experience that suspects treat their child pornographic media as prized possessions and rarely delete or destroy the media. The military judge extended this

---

(. . . continued)

Judge on 25 September 2017. The failure to include such details would potentially apply to a good faith analysis. *See* Mil. R. Evid. 311(c)(3); *See also United States v. Carter*, 54 M.J. 414, 419-422 (C.A.A.F. 2001).

<sup>12</sup> The fact that Ms. BL went back into the house on the night she confronted appellant and personally saw that the computer was gone also was not provided to the Federal Magistrate Judge.

rationale determining it was a fair inference appellant saved the same pictures or other similar recordings on other electronic media and that those and/or the original computer itself were still located in appellant's residence. Such inferences, if reasonable, would correct for the staleness of the search and extend probable cause for the computer to other devices in the home, including the external hard drive on which the bathroom videos were ultimately found. It is here, this case finds itself between the circumstances of both *Nieto* and *Eppes*.

Similar to the affidavit in *Nieto*, there was no information presented in the affidavit here regarding any type of external hard drive. Indeed, law enforcement had even less knowledge about the specific device on which the incriminating evidence was found than in *Nieto*. In *Nieto*, even though law enforcement did not provide any information about a laptop SPC Nieto may have owned to the military magistrate, at least they actually knew from "somebody" that SPC Nieto previously had a phone and laptop on his bunk. 76 M.J. at 103. While knowledge of SPC Nieto's laptop was "suspect and credited to an unknown source," it still existed in some form. *Id.* at 108. Here, law enforcement had no source of information regarding the existence of the external hard drive prior to actually conducting the search. Law enforcement's knowledge about the extent and types of electronic devices appellant may have owned was speculative beyond the three items Ms. BL specifically identified: a Dell tower, a Droid phone, and an iPhone. This lack of specific knowledge is underscored by the wide net cast in the laundry list of generic terms of electronic devices in Attachment A to the affidavit for which law enforcement requested and received authority to search.<sup>13</sup>

---

<sup>13</sup> The terms used in Attachment A of "any digital devices and storage devices capable of being used to commit, further, or store evidence of the offense listed above" and "any digital devices capable of being used to facilitate the transmission, creation, display, encoding, or storage of data..." would have allowed law enforcement officers to seize a number of different smart devices in appellant's home. Yet, the request never explicitly asked for the search and seizure of the devices known to have contained evidence: the two phones and Dell computer. While the breadth of the warrant here is justified by the previous transfer of the files and the connection between appellant's behavior and the generic profile, law enforcement and magistrates would do well also to make specific requests rather than rely on laundry-list templates.

This court recently had occasion to address what constitutes a specific request for disclosure within the context of discovery. *See United States v. Ellis*, \_\_ M.J. \_\_, 2018 CCA LEXIS 155, \* 21-28 (Army Ct. Crim. App. 27 Mar. 2018) (First, the request must, on its face or by clear implication, identify the specific file, document or evidence in question. Second, unless the request concerns evidence in the

(continued . . .)

And yet, in *Eppes* our superior court upheld a similarly broad search for “computer hardware, computer software and digital media (e.g., computer equipment, digital storage devices, cameras, photographs, etc.)” for evidence of fraud against the government. *Eppes*, 2018 CAAF LEXIS 202, at \*5. This warrant was upheld because the suspect, Capt. Eppes, had used an email account to communicate from an electronic device in furtherance of his scheme and clearly created fraudulent documents on an electronic device. *Id.* at \*15. The court reasoned that because Capt. Eppes was a law enforcement agent it was likely he used a device in his home rather than a shared computer at work. *Id.* at \*15-16. It is hard to reconcile the breadth of this search, where the affidavit did not include what specific devices were used or that Capt. Eppes even owned a particular device, with the cautionary note in *Nieto* of not “providing law enforcement with broad authority to search and seize all of an accused’s electronic devices and electronic media merely because the accused used a cell phone in furtherance of a crime.” *Nieto*, 76 M.J. at 108, n.5.

However, *Eppes* does not purport to overrule *Nieto*, but instead relies on it with respect to the proposition that “a nexus may be inferred from the facts and circumstances of a particular case, including the type of crime, the nature of items sought, and reasonable inferences about where evidence is likely to be kept.” *Eppes*, 2018 CAAF LEXIS 201, at \*12-13 (citing *Nieto*, 76 M.J. at 106). The CAAF rejected the generic profile and inference in *Nieto* about how servicemembers “normally” store images as outdated. Without a link between the inference that a transfer of data between the phone and the laptop occurred to SPC Nieto’s actual behavior, probable cause to seize the laptop was lacking. 76 M.J. at 107. It was for this reason there needed to be some additional showing that SPC Nieto actually downloaded images from his phone to his laptop, stored images on his laptop, or transmitted images from his laptop. *Id.* This necessary link was present in *Eppes*.

---

(. . . continued)

possession of the trial counsel, the request must reasonably identify the location of the evidence or its custodian. Third, the specific request should include a statement of the expected materiality of the evidence to preparation of the defense's case unless the relevance is plain). While such an analysis does not dictate the constitutional requirements of the particularity clause, it provides a useful rubric for practitioners as to what should be included in both an affidavit and authorization. While there is not a direct correlation between the ability to specify and detail the items and evidence sought and whether a search for such items is supported by probable cause, the extent to which a drafter can: 1) identify the specific file, document or evidence in question; and 2) articulate the items’ materiality to the crime under investigation, certainly bears on our ability to assess whether there was a substantial basis for an issuing official to conclude probable cause existed.



In *Eppes* the CAAF made clear that “without some other incriminating facts, a search authority cannot reasonably infer that the average servicemember is more likely to store evidence of criminality on his home computer than on his work computer.” *Eppes*, 2018 CAAF LEXIS 202, \*16, n.5. The necessary link between Capt. Eppes’ known use of an electronic device as an instrumentality of the crime and the likelihood that such a device would be found in Capt. Eppes’ home was “the specialized knowledge and training about criminal investigative techniques and where individuals engaged in criminal conduct might secret the fruits and instrumentalities of their crimes” that was particularized to Capt. Eppes through his law enforcement background. *Id.* at \*15-16. It was this information specific to Capt. Eppes that created a fair inference the instrumentalities of his frauds would be found in his residence.

Unlike *Nieto* and like *Eppes*, the necessary link between a generic profile and appellant’s actual behavior is present in the facts and circumstances of this case. Here, the description of the fifteen photographs Ms. BL saw that was included in paragraph 3 of the affidavit were indicative of appellant producing and possessing child pornography. This linked appellant’s actual behavior to the generic profile in the affidavit. Furthermore, the affidavit also included information indicating appellant had already copied and transferred the files. The affidavit specifically included Ms. BL’s description that “the pictures appeared to be taken from appellant’s cell phone and she recognized his hand in them.” As Ms. BL found the pictures on appellant’s computer, appellant had necessarily transferred the files that appeared to have been taken with his phone. As a result, appellant’s behavior of producing images that appeared to be child pornography with one device and his specific transfer and storage of these images to a separate device linked his behavior with the general profile that suspects of child pornography treat their child pornographic media as prized possessions and rarely delete or destroy the media. Just as in *Eppes*, together these facts establish that the issuing magistrate judge could reasonably have inferred, given the nature of the criminal activity under investigation, that appellant was likely to still have evidence on other devices in his home.<sup>14</sup> This inference was all the more reasonable with respect to seizing the external hard drive, which as a device has the singular purpose of storing transferred information.

---

<sup>14</sup> Admittedly this inference is based on a mere fifteen months of experience of the investigating agent, where it is unknown how many and what particular types of cases the agent investigated. However, unlike the technologically outdated profile in *Nieto* concerning how servicemembers “normally” store images from their cellphones on their laptops, here we find no reason to question the premise of the profile that suspects of child pornography treat their child pornographic media as prized possessions and rarely delete or destroy the media. 76 M.J. at 107.

Lastly, the inferences that can be drawn about digital evidence are distinguishable from other types of evidence with respect to the potential staleness of probable cause. Unlike the cocaine in a suspected drug case or the knife in a suspected murder, digital evidence in a suspected child pornography case has a high degree of persistence. Unlike the contraband itself in a drug case where the cocaine is consumed upon use, each use of the files in a child pornography case does nothing to consume the contraband. Further the ease with which the contraband itself may be replicated, transferred, hidden, and stored amongst devices renders it more likely that evidence of the contraband will persist. Even the destruction of digital evidence is unlike the destruction of physical evidence in that it is often kept and is unknown to the lay user. *See generally United States v. Hill*, 750 F.3d 982, 987 n.6 (8th Cir. 2014) (“Unallocated space is space on a hard drive that contains deleted data, usually emptied from the operating system’s trash or recycle bin folder, that cannot be seen or accessed by the user without the use of forensic software. Such space is available to be written over to store new information.”) (quoting *United States v. Flyer*, 633 F.3d 911, 918 (9th Cir. 2011)); *United States v. Seiver*, 692 F.3d 774, 776 (7th Cir. 2012) (explaining that when one deletes a file, that file goes into a “trash” folder; when one empties the “trash folder” the file has not left the computer because although the “trash folder is a wastepaper basket[,] it has no drainage pipe to the outside;” the file may be “recoverable by computer experts” unless it has been overwritten) (citations omitted).

Thus, despite a nearly three month lapse in time between discovery of the apparent child pornography on appellant’s computer and the search of his home, it was a reasonable inference that evidence of child pornography would still be found because of both the profile traits of suspects who have child pornography and the persisting nature of digital evidence. Given the Fourth Amendment’s strong preference for searches conducted pursuant to a warrant and the commonsense manner in which we are required to interpret affidavits, this inference is one the issuing judge reasonably could have made. *Eppes*, 2018 CAAF LEXIS 202, \*12-13. As such, the Federal Magistrate Judge had a substantial basis for finding probable cause regarding the search of the residence and the military judge did not abuse his discretion in ruling the warrant issued for the search was supported by probable cause.

## 2. *The Particularity Requirements of the Fourth Amendment*

The Fourth Amendment states, “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularity describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. At trial, the defense suppression motion challenged the warrant in part as being overbroad. As previously noted, the warrant at issue approves a search for a three-page litany of digital devices, components, media, electronic access materials, and types of electronic evidence that could conceivably be seized and searched.

We review the issue of whether a warrant was overbroad de novo. *United States v. Maxwell*, 45 M.J. 406, 420 (C.A.A.F. 1996). The Fourth Amendment requires warrants to particularly describe the place to be searched and things to be seized so that the search will be carefully tailored to its justifications. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

The CAAF addressed the difficulties in applying Fourth Amendment search requirements to electronic devices to ensure that such searches are “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.” *United States v. Richards*, 76 M.J. 365, 370 (C.A.A.F. 2017). The CAAF asserted that “[d]espite the importance of preserving this particularity requirement, considerable support can be found in federal law for the notion of achieving a balance by not overly restricting the ability to search electronic devices.” *Id.* at 369.

The particularity requirements of the Fourth Amendment and the overbreadth of a warrant are intrinsically linked to probable cause. Probable cause determines the lawful confines of the search and in turn whether the warrant has limited its authorization to those confines. Here, although a search for appellant’s Dell tower computer, Droid phone, and iPhone were clearly supported by probable cause, they were not the only items in appellant’s residence that were likely to contain evidence of the crimes under investigation. Appellant’s specific behavior of transferring apparent child pornography that he produced from one device to another within his home combined with the investigator’s informed opinion that “suspects of child pornography treat their child pornographic media as prized possessions and rarely delete or destroy the media,” made it a reasonable inference that digital evidence of the suspected crimes would be found on other, as of yet, unidentified devices and media within appellant’s home. Probable cause supported the search of appellant’s home for other such devices and evidence contained therein, and that is exactly what the warrant authorized. We therefore do not find the warrant was overbroad and affirm Specification 3 of Charge I.

## CONCLUSION

The findings of guilty of Specification 2 of Charge I and Charge II and its specifications are set aside. The remaining findings of guilty are affirmed. The sentence is set aside. The same or a different convening authority may order a rehearing on Specification 2 of Charge I and Charge II and its specifications and the sentence. If the convening authority determines a rehearing on those charges is impracticable, the convening authority may dismiss the charges and order a rehearing on the sentence only. If the convening authority determines that a rehearing on the sentence likewise is impracticable, the convening authority may

reassess the sentence, affirming no more than a dishonorable discharge, confinement for twenty years, and reduction to the grade of E-1.<sup>15</sup>

Chief Judge BERGER and Senior Judge MULLIGAN concur.



FOR THE COURT:

A handwritten signature in black ink, reading "Malcolm H. Squires, Jr.", written in a cursive style.

MALCOLM H. SQUIRES, JR.  
Clerk of Court

---

<sup>15</sup> In any event appellant will remain convicted of rape of a child, indecent act, wrongfully providing alcohol to ZJEH and JA, and obstructing justice. In reassessing the sentence we are satisfied that the sentence adjudged, absent the propensity error, would have been at least a dishonorable discharge, confinement for twenty years, and reduction to the grade of E-1. *See United States v. Sales*, 22 M.J. 305, 308 (C.M.A. 1986) and *United States v. Winckelmann*, 73 M.J. 11, 15-16 (C.A.A.F. 2013). This reassessment being both appropriate and purging the record as it stands of error does not otherwise limit the sentence that may be adjudged at a rehearing. *See UCMJ*, art. 63.