UNITED STATES NAVY–MARINE CORPS
COURT OF CRIMINAL APPEALS

No. 201600242

UNITED STATES OF AMERICA
Appellee

v.

JOSEPH A. LANCINA
Information Systems Technician First Class (E-6), U.S. Navy
Appellant

Appeal from the United States Navy-Marine Corps Trial Judiciary

Military Judge: Captain David M. Harrison, JAGC, USN.
Convening Authority: Commander, U.S. Naval Forces Japan, Yokosuka, Japan.
Staff Judge Advocate's Recommendation: Commander Timothy D. Stone, JAGC, USN.
For Appellant: Captain Daniel Douglass, USMC.
For Appellee: Major Cory A. Carver, USMC; Lieutenant James M. Belforti, JAGC, USN.

Decided 30 June 2017

Before CAMPBELL, FULTON, and HUTCHISON, *Appellate Military Judges*

This opinion does not serve as binding precedent, but may be cited as persuasive authority under NMCCA Rule of Practice and Procedure 18.2.

CAMPBELL, Senior Judge:

A military judge sitting as a general court-martial convicted the appellant, pursuant to his conditional guilty pleas, of wrongfully possessing child pornography in violation of Article 134, Uniform Code of Military Justice (UCMJ), 10 U.S.C. § 934 (2012). The military judge sentenced the

appellant to eight years' confinement, reduction to pay grade E-1, forfeiture of all pay and allowances, and a dishonorable discharge. The convening authority approved the sentence as adjudged.[1]

The appellant's sole assignment of error avers that criminal investigators presented false information that mislead the military commander who granted authorization to search for and seize evidence related to this case, and the military judge erred in denying a motion to suppress that evidence. We find no prejudicial error and affirm.

I. BACKGROUND

In June 2014, the Information Systems Security Manager ("security manager") for the "ONENET" Navy computer network in Japan notified Naval Criminal Investigative Service (NCIS) that the appellant's assigned government computer had accessed a suspicious website, ("the website"). As part of the investigation initiated by NCIS Special Agent (SA) R, the security manager covertly cloned the hard drive of the appellant's government computer, placed the cloned copy into that computer, and provided the original hard drive to NCIS. SA R later requested that the Commander, Fleet Activities Yokosuka ("CO") sign a command authorization for search and seizure (CASS) to search the appellant and his home—including "[t]he premises and all parts therein and any other area which may be feasible to contain evidence of items that may contain child pornography, and child sexual exploitation images"[2]—and seize for further searches "[a]ny [e]lectronic [m]edia [s]torage [d]evices" including "desktop computers, laptop computers, cellular/mobile telephones, [and] tablets[.]"[3]

In January 2015, about a week after the CO signed the CASS, NCIS executed the search, in coordination with Japanese police officers. At the appellant's residence, a Filipino national, Ms. O, answered the door and explained she was the appellant's live-in fiancée. Because Ms. O was a third party residing in the home, and a Japanese permanent resident, the NCIS agents received legal advice to seek her permission for the search in order to comply with the U.S.-Japan Status of Forces Agreement.

In Tagalog, Japanese, and English, the NCIS agents explained to Ms. O that they were there to execute the command authorized search and seizure in a child pornography investigation. They read a permissive authorization for search and seizure (PASS) form to Ms. O in all three languages. She

---

[1] Pursuant to a pretrial agreement, the convening authority also suspended the execution of all confinement in excess of 60 months.

[2] Appellate Exhibit (AE) V, Encl. (3) at 2 (CASS at Attachment A).

[3] *Id.* at 3 (CASS at Attachment B).

confirmed that she understood the PASS, that she was not required to consent to or sign the PASS, and why the investigators were there before she provided verbal and written consent to execute the search. At the NCIS agents' request, Ms. O identified the appellant's personal belongings. Investigators conducted a cursory search of the appellant's laptop computer and desktop computer, which had an external hard drive. Before leaving, they explained to Ms. O what media devices they were seizing. The investigation later revealed thousands of child pornography images and videos in password-protected folders on the home laptop and hard drive. The military judge denied a pretrial motion to suppress this evidence.

II. DISCUSSION

A. Probable cause for the CASS

The Fourth Amendment provides, "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." U.S. CONST. amend. IV. Searches conducted pursuant to a warrant or authorization based on probable cause are presumptively reasonable. *United States v. Hoffmann*, 75 M.J. 120, 123 (C.A.A.F. 2016). "While he issues no warrants, the commanding officer is bound by the same rules in authorizing a search as [a Federal magistrate]; that is, probable cause to believe that the things to be seized are on or within the premises to be searched." *United States v. Stuckey*, 10 M.J. 347, 357 (C.M.A. 1981). Evidence obtained in violation of the Fourth Amendment is generally inadmissible against an accused. MILITARY RULE OF EVIDENCE (MIL. R. EVID.) 311, MANUAL FOR COURTS-MARTIAL, UNITED STATES (2016 ed.).

"We review a military judge's denial of a motion to suppress evidence for an abuse of discretion." *United States v. Nieto*, 76 M.J. 101, 105 (C.A.A.F. 2017) (citation omitted). When "a military magistrate has a substantial basis to find probable cause, a military judge [does] not abuse his discretion in denying a motion to suppress." *Id.* (citation and internal quotation marks omitted) (alteration in original). "A substantial basis" for probable cause to search an area exists where "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[.]" *Id.* (citations and internal quotation marks omitted).

In determining whether an affidavit provides a substantial basis to find probable cause, "we rely alone on information that *we know was presented to the magistrate* at the time of his determination, as reflected in the affidavit, the military judge's findings and conclusions of law, and testimony in the record of trial addressed to the suppression motion that is consistent with the military judge's findings." *United States v. Leedy*, 65 M.J. 208, 214 n.5

(C.A.A.F. 2007) (emphasis added). With no evidence that SA R orally briefed the CO beyond the contents of the affidavit, our analysis focuses on those contents. *Id*.

Before any allegedly false information that may have misled a magistrate is "set aside" from an affidavit, an accused must make "'a substantial preliminary showing that a government agent included a false statement *knowingly and intentionally or with reckless disregard* for the truth in the information presented to the authorizing officer'"—and then prove this "'by a preponderance of the evidence'" in a hearing. *United States v. Cravens*, 56 M.J. 370, 375 (C.A.A.F. 2002) (emphasis added) (quoting MIL. R. EVID. 311(g)(2)). Similarly, to receive a hearing on alleged material omissions from affidavits, the defense must demonstrate that the omissions were "*both* intentional or reckless, *and* that their hypothetical inclusion would have prevented a finding of probable cause." *United States v. Mason*, 59 M.J. 416, 422 (C.A.A.F. 2004) (emphasis in original) (citation omitted). A military judge's finding of fact that the defense did not meet its burden of showing knowing and intentional falsity or reckless disregard for the truth is binding unless clearly erroneous. *United States v. Allen*, 53 M.J. 402, 408 (C.A.A.F. 2000).

Here, the military judge found *generally* that "[t]he defense . . . failed to meet its burden on *both*" making "a preliminary showing that [SA R] made false statements knowingly and intentionally or with reckless disregard for the truth, and then . . . establish[ing] by a preponderance of the evidence the statements' knowing and intentional falsity or reckless disregard for the truth."[4] Thus, we review the suppression motion record only to ascertain whether the military judge clearly erred in his determination that the statements in the affidavit were not "false" or "mislead[ing]," or that any such statements by SA R was not made "knowingly and intentionally or with reckless disregard for the truth." *Cravens*, 56 M.J. at 375. "[W]hen there are misstatements or improperly obtained information" in an affidavit, "we sever those from the affidavit and examine the remainder to determine if probable cause still exists." *United States v. Gallo*, 55 M.J. 418, 421 (C.A.A.F. 2001) (citation omitted).

We find the totality of the facts in the affidavit, and the reasonable inferences the CO could draw from them, provided a substantial basis for the CO to conclude there was a fair probability that 1) the appellant committed the offenses alleged in the command authorization—violations of "Title 18 U.S.C. § 2252 and 2252A, relating to material involving the sexual

[4] AE XVII at 17 (emphasis added) (citation omitted).

exploitation of minors"[5]—and 2) given the nexus to the appellant's home, NCIS would find evidence of those offenses in his digital devices there.

1. Probable cause to believe the alleged crimes occurred and the appellant committed them

SA R's affidavit, attached to the authorization request, stated:

i. His 11 years of experience as an NCIS agent included his "participat[ion] in child pornography investigations which have resulted [sic] convictions" and "120 hours of advanced sex crimes investigation training[.]"[6]

ii. On the appellant's government computer hard drive, he found "two thumbnail images[7] which [each] depict an apparent female child's buttocks being spread open by an adult male hand exposing the child's anus and vagina," where "[i]n one of the two photos the child's genitals are covered with apparent semen"—and, a "pedo bear icon . . . a type of visual code that indicates the presence of child pornography."[8]

iii. The security manager had told SA R that the website the appellant accessed is a "known incest/child pornography (CP) website."[9]

iv. After creating an undercover, online profile on the website, SA R "located only one profile" for website members in Japan—"LANCE ALOT," whose listed birthday exactly matched the appellant's.[10]

v. The "LANCE ALOT" profile's "avatar photo" showed "a white male's erect penis" (the appellant is white), and "LANCE ALOT" posted that he "loves to tease and please young horny wet girls to multiple orgasms."[11]

vi. Evidence on the appellant's government computer hard drive showed that, before 21 August 2014, the appellant "had viewed 13 separate member profiles" on the website.[12] Using his own undercover, online

---

[5] AE V, Encl. (3) (Affidavit for Search Authorization of 13 Jan 2015 at 1).

[6] *Id*. at ¶ 2.

[7] The appellant incorrectly states SA R "omitted [from the affidavit] that the two images of suspected child pornography were . . . thumbnails." Appellant's Brief of 15 Nov 2016 at 5.

[8] AE V, Encl. (3) at ¶ 6e.

[9] *Id.* at ¶ 6a.

[10] *Id.* at ¶ 6f.

[11] *Id.*

[12] *Id.* at ¶¶ 6c, 6e.

> profile, SA R found 10 of the 13 profiles that the appellant had viewed on the website. One of them, Ms. A,[13] listed a birthdate indicating she was "under 18 years of age" as of 20 October 2014.[14] SA R determined that the appellant had friended two other users of the website, Ms. B and Ms. C, while, according to their listed birthdays, they were younger than 18 years old. LANCE ALOT had messaged Ms. C that she was "incredibly beautiful with a sexy and stunning body." Ms. C's profile had nude photos. SA R found "three other profiles which LANCE ALOT had communicated with where the [sic] two of the females were 17 years old and one was 16 years old."[15]

a. The thumbnail images

Thumbnail images of child pornography can provide probable cause for a search authorization.[16] But the appellant first suggests that the affidavit's details of the child pornography thumbnail images cannot provide a substantial basis for probable cause because "[t]hose two images were not associated with known child pornography in the NCMEC [National Center for Missing and Exploited Children] database, nor were the images looked at by a medical professional to determine the age of the people depicted in the pictures[,]" or by the Defense Computer Forensics Laboratory.[17] Moreover, he claims these facts were "omitted" from the affidavit.[18]

---

[13] The profile names are pseudonyms.

[14] AE V, Encl. (3) at ¶ 6f.

[15] *Id.*

[16] *See, e.g., United States v. Howe*, 545 F. App'x. 64, 65 (2d Cir. 2013) (finding that the "district court did not err in concluding that probable cause existed to seize Howe's laptop" where a police officer had "viewed . . . at least one thumbnail image that the magistrate judge determined was lascivious" in the "Sample Pictures folder on that computer") (citation and internal quotation marks omitted).

[17] Appellant's Brief at 3, 12.

[18] *Id.* at 5. Although the appellant did not expressly raise this issue at trial, we find that under either a plain error or abuse of discretion standard of review, he has failed to demonstrate any prejudice by showing how the "hypothetical inclusion" of this information "would have prevented a finding of probable cause." *Mason*, 59 M.J. at 422. NCMEC databases do not contain the entire universe of child pornography images, and non-medical professionals—particularly an investigator for previous child pornography cases like SA R—are capable of recognizing child pornography for purposes of addressing probable cause. *See* Record at 67; 102-03 ("[Trial Counsel: [W]hy, based on your training and experience . . . was [it] apparent to you that these were children? [SA R:] . . . . The labia were not very distinct, not very developed. There was no pubic hair, and the pubic hair was not shaved. It appeared to be naturally not pubic hair.").

Our superior court in *Gallo* found a substantial basis for probable cause to search for child pornography where an affiant with 26 years of experience, having "participated in numerous child pornography investigations," swore that "approximately 262 apparent child pornography photographs were found on [Gallo's] work computer" and "that several of the photographs . . . matched imported photographs seized in other Customs' cases." 55 M.J. at 420-22. The *Gallo* majority did not object to the fact that the "affidavit provided no description of the images" and "merely set out [the agent's] conclusions" that the images were "'child pornography,' 'adult pornography,' and 'apparent child pornography.'" *Id.* at 424 (Gierke and Effron, JJ., dissenting). Thus, this first argument fails.

The appellant next contends the thumbnail images cannot provide a substantial basis for probable cause because their computer location indicates they were "automatically cached from internet sites onto [the appellant's] work computer" rather than actively downloaded, meaning there was "no evidence [that the appellant] viewed or knowingly possessed" the thumbnails.[19] We also reject this argument.

Appellate courts have affirmed that the presence of child pornography thumbnail images in the internet cache can be a basis for possession of child pornography *convictions*.[20] As thumbnail images, in some circumstances, can satisfy the beyond a reasonable doubt standard, we hold that they provide substantial basis for the CO here to find probable cause to suspect that the appellant possessed child pornography. The appellant suggests that the thumbnails may have been cached without the appellant having "scrolled down to their position on the page"—*i.e.*, without the appellant having viewed them.[21] The CO did not have to make this assumption favorable to the appellant, where the evidence was equally consistent with the appellant

---

[19] Appellant's Reply Brief of 9 Mar 2017 at 2. The appellant did not claim at trial that SA R's failure to state that the thumbnail images were "not [intentionally] downloaded images" was a material omission from the affidavit, as he does now. Appellant's Brief at 12; Reply Brief at 3. But regardless of the proper standard of review, again we find that the appellant has failed to demonstrate prejudice. Since as discussed in the next paragraph, thumbnail images provide direct or circumstantial evidence of the offenses, a "hypothetical inclusion" of this information would still not have prevented the CO from finding probable cause. *Mason*, 59 M.J. at 422.

[20] *See, e.g., United States v. Tucker*, 305 F.3d 1193, 1197, 1205 (10th Cir. 2002) (upholding Tucker's conviction for possessing "thumbnail" and "larger images" of child pornography in his "[w]eb browsers' cache files," despite his argument that since "he did not voluntarily cache the files," he did not possess child pornography).

[21] Appellant's Reply Brief at 2.

having viewed the images.[22] We note that child pornography thumbnail images are created in the cache when one "use[s a] webpage"[23] that contains child pornography, or a when a user executes an internet search engine "image search" which returns child pornography.[24] Thus, the thumbnail images' presence in the appellant's cache allowed the CO to draw a reasonable inference that the appellant had accessed webpages with child pornography, or entered search terms yielding such images, providing a fair probability for probable cause that the appellant had committed child pornography offenses.

b. The "pedo bear icon" ("icon")

Facts in an affidavit "are properly viewed in context, through the professional lens in which they were presented to the magistrate." *Leedy*, 65 M.J. at 215-16 (finding the filename "14 year old Filipino girl," located alongside other filename "titles . . . identify[ing] sex acts" which an experienced investigator stated were "indicative of . . . child pornography," provided probable cause to search Leedy's computer). "A possible innocent explanation or lawful alternative may add a level of ambiguity to a fact's probative value in a probable cause determination, but it does not destroy the fact's usefulness outright and require it to be disregarded." *People v. Zuniga*, 372 P.3d 1052, 1058 (Colo. 2016).

The affidavit here informed the CO that SA R, an experienced criminal investigator, found an icon on the appellant's government computer that SA R deemed a "visual code that indicates the presence of child pornography."[25] The military judge issued findings of fact which supported this conclusion and separately rejected the appellant's contention that SA R's statement "that this image indicates child pornography is wholly misleading."[26] We do not find these findings clearly erroneous. At the suppression motion hearing, SA R testified that "Pedobear is kind of like a trail sign on the Internet, or basically it's a calling card. It kind of tends to indicate to people that know what to look for, that there is child pornography here. . . . [I]t helps kind of guide them to particular sites and files that contain child pornography,"

---

[22] *See United States v. Martin*, 426 F.3d 68, 77 (2nd Cir. 2005) (noting that merely because "an innocent explanation may be consistent with the facts alleged" in a warrant application "does not negate probable cause" to issue a search warrant) (citation and internal quotation marks omitted).

[23] Appellant's Reply Brief at 2.

[24] Record at 85.

[25] AE V, Encl. (3) at ¶ 6e.

[26] AE V at 11. *See* AE XVII at 17.

though he also agreed with the trial defense counsel's statement that the filename of the icon "was not named 'Pedo,' it wasn't named Pedobear."[27] Even though, as argued at the suppression motion hearing, most internet pictures of teddy bears may be wholly innocent—which possibly reduces the "probative value" of the icon as circumstantial evidence of child pornography possession—that does not "destroy the fact's usefulness outright and require it to be disregarded." *Zuniga*, 372 P.3d at 1058. Like the filename in *Leedy*, the context in which the icon was found,[28] and SA R's experience-based assessment of what it might mean in that context, provided a substantial basis for the CO to consider the icon as circumstantial evidence of child pornography in his probable cause determination.

c. The appellant's membership in the website and child pornography

In *United States v. Clayton*, our superior court considered whether there was a substantial basis for probable cause to search Clayton's "laptop, in [his] quarters" based on Clayton's e-mail address appearing on a membership list for an "internet group" named "Preteen-Bestiality-and-Anything-Taboo," where one member had "confessed" to "upload[ing] . . . child pornography" to the group" and at whose website the affiant found child pornography. 68 M.J. 419, 422-23 (C.A.A.F. 2010). Clayton had "requested a Digest for the [g]roup, in which he would receive daily e-mails that would contain 25 of the postings to the [g]roup sent as a single e-mail to his account." *Id.* at 422 (alterations in original, internal quotation marks omitted). However, there was neither evidence in the affidavit as to what was in the e-mail digests, nor as to whether Clayton had "accessed the website, or . . . received the digests he requested," as the affiant had not "review[ed] his e-mail accounts[.]" *Id.* at 425.

The Court of Appeals for the Armed Forces (CAAF) nevertheless upheld the magistrate's search authorization due to a "practical, commonsense understanding of the relationship between the active steps that a person might take in obtaining child pornography from a website and retaining it for an extended period of time on that person's computer." *Id.* at 424. *See also United States v. Gourde*, 440 F.3d 1065, 1072-73 (9th Cir. 2006); *United*

---

[27] Record at 68, 90.

[28] The appellant alleged at trial that the icon was "in the thumb[nail]cache on the computer." AE V at 11 (internal quotation marks omitted). The appellant now suggests it was in the "'unallocated clusters" area of the computer,"' where "files are stored after having been permanently deleted." Appellant's Reply Brief at 7 n.24. In either case, per our discussion of the thumbnail images *supra*, the location of the icon does not negate its value in finding a substantial basis for probable cause, as its presence in either place demonstrates the appellant accessed a page with the icon at some point.

States v. Martin, 426 F.3d 68 (2nd Cir. 2005); *United States v. Froman*, 355 F.3d 882 (5th Cir. 2004). It did so even without proof that Clayton possessed *any* child pornography images, from *any* source, on *any* computer. *Clayton*, 68 M.J. at 425 (noting "no evidence showed that he posted messages to the Google site, participated in discussions, or uploaded or downloaded child pornography").

In *Gourde*, membership in "lolitagurls.com" provided a substantial basis for probable cause to search Gourde's computer, even though there was no evidence that he downloaded child pornography from the website. 440 F.3d at 1067 (noting the "triad of solid facts—the site had illegal images, Gourde intended to have and wanted access to these images, and these images were almost certainly retrievable from his computer if he had ever received or downloaded them"). In *Froman*, membership in "Candyman," a web group from which an agent received "hundreds of images of child pornography," provided a sufficient basis for probable cause to search Froman's computer, even though there was no evidence he had downloaded images from the group, or automatically received e-mail updates. 355 F.3d at 890-91 (noting "it is common sense that a person who voluntarily joins a group" whose "predominant purpose" is "to engage in collection and distribution of child pornography" and "uses screen names that reflect his interest in child pornography, would download such pornography from the website and have it in his possession"). In *Martin*, membership in the web group "girls12-16," to which an investigator subscribed and received e-mails with child pornography and "child erotica," was sufficient to search Martin's computer even though the "affidavit d[id] not explicitly state that Martin accessed child pornography." 426 F.3d at 75-76 (finding a "fair probability" that "evidence of a crime would be found at Martin's home because membership in the e-group reasonably implied use of the website" and child pornography was "distributed to some of the group's members").

Here, contrary to the appellant's assertion that only "weak and circumstantial" evidence suggested he was a member of the website,[29] the CO could reasonably infer from the facts in the affidavit that the appellant was a member. SA R found one member in Japan, LANCE ALOT; "Lancina" is similar to LANCE ALOT; and LANCE ALOT's listed birthday was the same as the appellant's.

The appellant tries to distinguish his membership in *this* website from the websites or groups mentioned in the authorities *supra*, on the grounds that there was inadequate support in the affidavit for SA R's claim that "[the

[29] Appellant's Brief at 23 n.86.

website] is a known child pornography website."[30] At trial, the appellant duly alleged that this claim was a "false statement" by SA R.[31] SA R's actual claim in the affidavit was that the security manager "stated [the website] was a known incest/child pornography (CP) website."[32] The military judge disagreed, finding that SA R's "statements and conclusions about the web site in the affidavit were simply not shown to be false."[33]

In the hearing on the suppression motion, SA R conceded that the security manager "did not tell [him] that there was child pornography on that website"[34]—only that the security manager had provided him with an article about the website, from which SA R concluded the website "did, in fact, appear to be an incest, child pornography, even a child rape website, that teaches its patrons, or encourages their patrons to basically have sex with children."[35] SA R added that when he accessed the website, he "*observed* the chatroom where people were [advising] other people about how to have sex with their children."[36] SA R conceded that he could not tell whether the thumbnail images or icon on the appellant's computer had been downloaded from the website, or from any other internet location.[37]

The critical distinction highlighted by the appellant is that in *Clayton* and the federal circuit court cases it cites, a website membership was sufficient to provide probable cause to suspect downloading of child pornography because the affidavits confirmed that *actual child pornography* was on the web groups or websites. The only evidence SA R cited at the suppression hearing to prove the website was a "known" child pornography website was a newspaper article discussing the arrest of another Marine for attempting to arrange "an incestuous four-way with another man and his two preteen children" with an undercover agent who was a member of the website.[38] The article has a

---

[30] Reply Brief at 4. *See also* Appellant's Brief at 12, 15, 23 (noting that the affidavit did not mention finding any "images of child pornography from the [the] website," any proof that the thumbnail images on the appellant's computer were "downloaded images," or any "evidence of [the appellant] soliciting contraband from the website" or "actively s[eeking] out updates from the website").

[31] AE IV at 9-10.

[32] AE V, Encl. (3) at ¶ 6a.

[33] AE XVII at 18.

[34] Record at 78.

[35] *Id.* at 64. AE VI, enclosure (1) (the newspaper article).

[36] Record at 64 (emphasis added).

[37] *Id.* at 100.

[38] AE VI, Encl. (1) at 1.

screenshot of the website, where the only sexual content is a banner advertisement with an obscene cartoon soliciting users to "watch live sex shows from *18yo* teens for free."[39] The article (citing a media outlet) says the website "specializes in the promotion of incest and other taboo behaviors,"[40] but nowhere states the website was known for child pornography or published actual child pornography.

While incest is illegal in many instances, it does not inherently imply sex with an underage person, let alone the presence of child pornography. In *Hoffman,* after the appellant was "taken into custody" for soliciting "young boys for sex," a search authorization was granted based in part upon an affidavit in which the affiant asserted "'that she knew through her "training and experience that there is an intuitive relationship between acts such as enticement or child molestation and the possession of child pornography."' *Hoffmann*, 75 M.J. at 123, 127 (citation omitted). The CAAF held that, absent extreme circumstances, even the "enticement" of an *actual child* for sex is "simply not sufficient to provide a substantial basis for concluding that there was probable cause to believe [someone] *possessed child pornography*." *Id.* at 127 (citation omitted) (emphasis added). In light of *Hoffman*, we find that most of SA R's observations in the affidavit—including that others on the website advised how to have sex with children, that the appellant messaged users of the website whose birthdates suggested they were under 18, and that he told one she was "incredibly beautiful with a sexy and stunning body"[41]–even assuming *arguendo* they were enticement, do not support the conclusion that the website contained child pornography.

SA R's statement that on the website profile of Ms. C—a user with whom the appellant communicated—he found nude photos, and the age listed on Ms. C's website user profile suggested she was 17 years old,[42] is also insufficient to support SA R's characterization of the website. SA R did not describe these nude photos as child pornography in the affidavit—a description he readily applied to the thumbnail images discussed *supra.*

---

[39] *Id.*, Encl. (1) at 2 (emphasis added).

[40] *Id.*, Encl. (1) at 1.

[41] AE V, Encl. (3) at ¶ 6f.

[42] Though the appellant notes that he "could have made a request for and had sexual relations with his girl and it would not have been illegal," Appellant's Reply Brief at 6 n.19, the investigation was for violations of "Title 18 U.S.C. § 2252 and 2252A, relating to material involving the sexual exploitation of minors." AE V, Encl. (3) at 1. Under federal law, "'minor' means any person under the age of eighteen years." 18 U.S.C. § 2256(1).

Thus, we conclude that the military judge's findings of fact—that SA R's "statements and conclusions about the web site in the affidavit were simply not shown to be false," and that "[t]he defense has failed to meet its burden on . . . showing that SA R made false statements knowingly and intentionally or with reckless disregard for the truth"[43]—was clearly erroneous as to SA R's claim that the security manager "stated [the website] was a . . . known . . . []child pornography website."[44] This statement was misleading at a minimum, under *Mason*, 59 M.J. at 422, given that the article never said the website actually hosted child pornography. Moreover, SA R displayed a reckless disregard for the truth in making this assertion to the CO, given that, despite his investigative efforts, he identified no actual or apparent child pornography on the website.[45]

d. Child erotica on the website

The most significant facts about the website remaining in the affidavit, after removal of the misleading statement, are that on the profile of Ms. C—a minor user with whom the appellant communicated—SA R found "nude photos,"[46] and Ms. C's user profile on the website suggested that she was 17

---

[43] AE XVII at 17-18.

[44] AE V, Encl. (3) at ¶ 6a. The portion of the finding of fact about the website being a "known incest[] . . . site," is not clearly erroneous in light of the article and affidavit.

[45] We also reject as clearly erroneous the military judge's finding of fact that the website "appeared to be one dedicated to child pornography," AE XVII at 4. The only evidence in the record that the military judge could have used as support for this conclusion are the newspaper article and SA R's testimony. The conclusion that the website "appeared to be one dedicated to . . . incest, child rape, and generally encourages and explains grooming methods of having sex with children," is not clearly erroneous in light of the article and affidavit.

[46] Trial defense counsel argued in her motion at trial that "neither [Ms. C], nor any other of the profiles reviewed, were minors," and the "assertion that [the appellant] commented on naked photographs of [Ms. C] is . . . a complete misstatement of fact[.]" AE IV at 9-10. However, the military judge held under "Discussion and Conclusions of Law" that "[a] number of the users . . . . Lanc[e ALOT] communicated with appeared to be and were thought to be minors based on their listed birth dates, and at least one had at least one nude photo of herself on the web page." AE XVII at 14, 19. "'Where a finding of fact is included under the heading of conclusions of law it will be treated as a factual finding.'" *United States v. Betancourt*, No. 201500400, 2017 CCA LEXIS 386, at *16 n.16, unpublished op. (N-M. Ct. Crim. App. 6 Jun 2017) (quoting *Utzinger v. United States*, 432 F.2d 485, 489 (6th Cir. 1970)). As the appellant's brief "does not now challenge th[is] ruling" as clearly erroneous, "we find it to be the law of the case[.]" *United States v. Trotter*, No. 201500332, 2016 CCA LEXIS 668, at *15 n.30, unpublished op. (N-M. Ct. Crim. App. 17 Nov 2016) (citing *United States v. Savala*, 70 M.J. 70, 77 (C.A.A.F. 2011))

years old.[47] Nude photos can include "child erotica," which is defined by our court as "material that depicts young girls [or boys] as sexual objects or in a sexually suggestive way, but is not sufficiently lascivious to meet the legal definition of sexually explicit conduct[.]" *United States v. Rapp*, No. 201200303, 2013 CCA LEXIS 355, at *24 n.15, unpublished op. (N-M. Ct. Crim. App. 30 Apr. 2013) (citations and internal quotation marks omitted).

Civilian courts are split as to whether the presence of child erotica provides a substantial basis for probable cause to suspect the presence of child pornography. *Compare United States v. Ranke*, 2010 U.S. Dist. LEXIS 115352, at *16-17 (E.D. Mich. Oct. 29, 2010), *aff'd on other grounds*, 480 Fed. App'x. 798 (6th Cir. 2012) ("The government contends persuasively that 'child erotica,' including nude photographs of minors or computer-generated images of children engaged in sexual conduct, is some evidence that may properly be considered in establishing probable cause to search for child pornography), *with United States v. Edwards*, 813 F.3d 953, 961-62, 969 (10th Cir. 2015) (holding that "[n]either [Edwards'] posting of child erotica nor his comments suggesting a sexual attraction to the child in the posted images established" a substantial basis for "probable cause that [he] possessed child pornography in his home," where "the search-warrant affidavit here provided evidence only that [Edwards] possessed legal child erotica").

The Eighth Circuit Court of Appeals explained that while the presence of child erotica may not in and of itself provide sufficient probable cause to suspect the presence of child pornography, such facts "combined with the other facts included in the affidavit," may support a probable cause determination under "the totality of the circumstances." *United States v.*

(additional citation omitted). Even absent waiver, we would not deem this finding of fact clearly erroneous. *See* AE VI at 6 of 8 (printed copy of Ms. C's profile where Lance ALOT "commented on [Ms. C]'s album[:] "Incredibly Beautiful and Sexy with a Stunning Body," and the handwritten notation "= 17 y/o"); Record at 263-64 ("[SA R: T]here were certainly nude images of minors on that website. . . . [a]pparently having viewed [Ms. C's] photo album, which featured numerous photographs of herself, completely naked. He made the comment, 'You have a beautiful and stunning body.'").

[47] The appellant argues "[t]here is no independent verification of the age of any [of] the girls in these profiles." Appellant's Reply Brief at 5 n.18. Even assuming *arguendo* that the ages were inaccurate, this is not relevant to how these "girls" would have appeared to users like the appellant. *See United States v. Roeseler*, 55 M.J. 286, 291 (C.A.A.F. 2001) ("Our general rule is that an accused should be treated in accordance with the facts as he or she supposed them to be.") (citations omitted). Nor does it prevent the CO from drawing reasonable inferences about the nature of the website, based on the fact that it features people claiming to be minors, posting nude photographs.

Hansel, 524 F.3d 841, 844-46 (8th Cir. 2008) (concluding that photographs of nude girls and other girls in swimsuits described by the investigating officer as "child erotica, not child pornography" could be considered along with allegations of sexual assault and camera and computer equipment, in finding probable cause to search for child pornography). Even though the affidavit in *Hansel* "misleading[ly]" stated that the child erotica photographs themselves "indicate[d] receipt of child pornography by means of a computer," the Court held that after removal of the misleading statement, a magistrate still would have found probable cause to search for child pornography based in part on the presence of child erotica. *Id.* at 844-46.

We agree that the presence of child erotica can be, at minimum, a factor in finding a substantial basis for probable cause to suspect the appellant committed a child pornography offense under the totality of the circumstances. Even wholly "innocent behavior frequently will provide the basis for a showing of probable cause." *United States v. Sparks*, 291 F.3d 683, 685, 688 (10th Cir. 2002) (reversing the lower court's suppression of methamphetamine seized during searches authorized in part based upon Sparks' arrest for picking up a bag of white powder from the side of a road) (citation and internal quotation marks omitted). Moreover, child erotica is admissible in a prosecution for possession of child pornography as evidence "to show intent to commit the charged offense." *United States v. Griffing*, No. 38443, 2015 CCA LEXIS 101, at *34, unpublished op. (A.F. Ct. Crim. App. 23 Mar 2015) (citing *United States v. Warner*, 73 M.J. 1, 3 (C.A.A.F. 2013) and *United States v. Vosburgh*, 602 F.3d 512, 538 (3d Cir. 2010)). Finally, while legally protected in other jurisdictions,[48] military courts have upheld convictions for the possession of child erotica under Article 134, UCMJ.[49]

Here, in addition to the "nude photo" on Ms. C's account that SA R referenced in the affidavit, SA R detailed: the appellant's website message to her that she was "incredibly beautiful with a sexy and stunning body;" that the appellant used an image of an erect penis as his avatar photo on the website; and, that his website profile stated he "loves to tease and please *young* horny wet girls to multiple orgasms."[50] Such contextual evidence allowed the CO to infer that the appellant had an interest in child erotica,

---

[48] *See Vosburgh*, 602 F.3d at 538 (approving district court's instruction to jurors that child erotica is "not illegal" to possess).

[49] *See, e.g., United States v. Davenport*, No. 20150322, unpublished op., 2016 CCA LEXIS 729, at *1, *8 (A. Ct. Crim. App. 19 Dec. 2016) (affirming the appellant's conviction, "contrary to his pleas, of . . . two specifications of possession of child erotica in violation of Article 134, Uniform Code of Military Justice").

[50] AE V, Encl. (3) at ¶ 6f (emphasis added).

and that he would therefore download the nude photo content present on the website that SA R described in the affidavit.[51] *See Froman*, 355 F.3d at 890-91 (finding Froman's use of "Littlebuttsue and Littletitgirly" as "screen names" on America Online, "reflected his interest in child pornography," and therefore supported the inference that he "would download such pornography from the website and have it in his possession"); *United States v. Shields*, 458 F.3d 269 (3rd Cir. 2006) (noting that Shields' "use of the name 'LittleLolitaLove' [in] registering for multiple e-groups where" child pornography images were "available and disseminated bolster[ed] a practical, commonsense decision that Shields likely downloaded such images") (citation and internal quotation marks omitted).[52]

The thumbnail images and icon on the appellant's computer discussed *supra* also suggest that the appellant has an interest in nude photographs of minors, and therefore support an inference that the appellant *would download* nude photos of minors from the website. Thus, even after removing the misleading language in the affidavit that the security manager "stated [the website] was a . . . known . . . []child pornography website,"[53] we find that the remaining facts establishing that the website hosted nude photographs of minors, and that the appellant had a demonstrable interest in nude photographs of minors, allowed the CO to consider the appellant's membership with, and participation in, that website, as probable cause to suspect that the appellant had committed child pornography offenses.

2. The nexus between the alleged crime and the appellant's home

Probable cause to suspect that the appellant wrongfully viewed or possessed child pornography on his workplace computer does not necessarily

---

[51] The appellant argues that "there is no indication or evidence that the photo in the profile existed when [he] had accessed the profile months earlier." Appellant's Reply Brief at 6. This is irrelevant given that the question is if the *website* is a child erotica website, not whether the appellant viewed or downloaded any particular website item. *See Clayton*, 68 M.J. at 424-25 (finding "the activities of a voluntary member of the . . . web group w[ere] sufficient to support a search of his quarters," even though there was "no evidence . . . that [Clayton] posted messages to the Google site, participated in discussions, or uploaded or downloaded child pornography" from the site).

[52] We reject the appellant's critique that "membership on" the website "means that member wrongfully possesses or views child pornography" is a "false assumption[]." Appellant's Brief at 16. To use the appellant's phrasing, membership on the website means that the appellant wrongfully possesses or views child erotica, and possession or viewing of child erotica under these circumstances provides probable cause to suspect the appellant committed a child pornography offense.

[53] AE V, Encl. (3) at ¶ 6a.

provide probable cause to search his home and electronic devices there. Our superior court has advised:

> [I]n order for there to be probable cause, a sufficient nexus must be shown to exist between the alleged crime and the specific item to be seized. . . . 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. . . . 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 (citations and internal quotation marks omitted). In *Nieto*, the most recent guidance from our superior court on this issue, multiple soldiers at a forward operating base suspected Nieto used his cell phone to record them using the latrine. After seizing Nieto's phone and a laptop computer, Army Criminal Investigation Command sought a search authorization for the computer. The search request contained one agent's statement that when "[s]oldiers us[e] their cell phones to photograph things," those "phones are normally downloaded, the photos they take . . . they'll back those up to their laptops so that when they get to . . . a place where they can get Internet, they can post those or send those home to family[.]" *Id.* at 104. It also recounted another agent's "experience" that:

> [P]ersons who would use a portable digital media recorder would also transfer the media from a portable device to a computer station or storage device. Persons who view and record sexual acts often times store and catalog their images and videos on larger storage devices such as a computer or hard drive.

Id. at 105. The military judge, citing *Clayton,* denied the motion to suppress on the theory that "[i]t is . . . a normal inference to be drawn . . . that data is transferred from one digital device to another." *Id.*

The CAAF held that the military judge abused his discretion in failing to suppress the search authorization. Noting that "the affidavits" and the oral briefing "accompanying the search authorization did not reference" any actual "data transfers" from Nieto's cell phone, presented no "direct evidence that images were on the laptop," and presented no evidence that "anyone had ever seen" Nieto "download material from his cell phone to a laptop," the CAAF rejected the notion that "law enforcement" has "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." *Id.* at 107-08, 108 n.5 (emphasis in original) (internal quotation marks omitted).

Before *Nieto*, the CAAF found sufficient nexus for probable cause to search homes for child pornography in other cases where child pornography had been discovered in the workplace. There was probable cause in *Clayton* to search the appellant's quarters in Kuwait where his e-mail address was found in the records of a "website group" containing child pornography, evidence showed he had accessed his e-mail account through a computer server in Kuwait, and he lived in base housing with "wireless Internet service capability." 68 M.J. at 423. In *Gallo*, the probable cause affidavit stated that, in addition to finding child pornography on his work computer an "analysis of [Gallo]'s work computer indicated that computer files of unknown content had been downloaded or uploaded from the hard drive to a diskette, relating to files received over the internet . . . mak[ing] the files extremely portable in nature." 55 M.J. at 421. The affidavit in *Gallo* also provided an experienced agent's "pedophile profile," that "[p]edophiles collect sexually explicit or suggestive materials involving children such as . . . computer disks" and "maintain and possess their materials . . . within the privacy and security of their own homes." *Id.* at 420. In *United States v. Allen*, the affidavit stated that a government computer to which the appellant had access connected to an "on-line service" and downloaded child pornography; that Allen admitted "ha[ving] access to [that on-line] service at his residence," and that he admitted having "erotica at his residence." 53 M.J. 402, 407 (C.A.A.F. 2000).

In light of *Nieto*, we find that the thumbnail images and icon found on the appellant's government computer and his access of the website from work, alone, are insufficient to provide the nexus required to search his *home*. But SA R's affidavit offered more for the CO's consideration:

i. He had "observed activity on [the appellant's] account" on the website on "six dates which included weekend days."[54]

ii. In response to a phone call to the appellant by a Japanese investigator pretending to be "a telemarketer who was taking a survey about internet service," the appellant admitted: that he had "internet service at his residence;" that he "has had it for the last 18 months;" that he owns a wireless router, desktop computer, laptop computer, and two cell phones that "he connects to the internet;" and that he "use[d] the internet for web browsing and watching movies."[55]

iii. The seven paragraphs on "computers and child pornography" noted "[t]he computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography," that the

[54] AE V, Encl. (3) at ¶ 6f.

[55] *Id*. at ¶ 6h.

internet "afford[s] individuals several different venues for obtaining, viewing and trading child pornography," and that such "computer communications can be saved or stored" both intentionally and "unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places"—such as "temporary files or ISP client software . . . the web cache and history files,"—where "[s]uch information is often maintained for very long periods of time until overwritten by other data," even "long after . . . attempts at deleting it."[56] Thus, SA R surmised that "[a] thorough search of this media could uncover evidence of receipt, distribution and possession of child pornography."[57]

iv. The 21 paragraphs of "[o]ffender [t]ypology" regarding those who "buy, produce, trade, or sell child pornography; who molest children and/or who are involved with the use of children in sexual acts," opined that "[a]s a result of [his] training and experience, [he] learned that certain characteristics are generally found to exist in" these people, such as: they generally "collect sexually explicit material consisting of photographs," they "rarely, if ever, dispose of their sexually explicit material," they "use such photos as described above as a means of reliving fantasies or actual encounters with the depicted children," and they "engage in activity or gravitate to programs which will be of interest to the type of victims they desire to attract and will provide them with easy access to these children."[58]

v. A paragraph connecting these concepts claimed that "offenders usually maintain illegal images using their computers and that evidence could remain on computers even after a viewer deletes the images," as such deleted "files have been recovered by forensic analysts"—and, that "it is normal for offenders to save . . . child pornography media . . . on assorted pieces of digital electronic media storage devices to include . . . desktop [and] laptop computers . . . smart telephones, [and] external hard drives[.]"[59]

a. Offender typology

> [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

---

[56] *Id*. at § IV.

[57] *Id*. at § IV(g).

[58] *Id*. at § I.

[59] *Id*. at ¶ 6j.

> 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.

Nieto, 76 M.J. at 106. We find that the "offender typology" SA R's affidavit provided was inadequate to provide the CO with a substantial basis to determine that there was probable cause to search the appellant's home. As in *Nieto,* there was no evidence that the appellant "fit" most of this profile at all. There was no evidence, for instance, that the appellant would "buy, produce, trade, or sell child pornography," or that he was "involved with the use of children in sexual acts." Most of the profile's descriptions were "rambling boilerplate recitations designed to meet all law enforcement needs." *United States v. Weber*, 923 F.2d 1338, 1345 (9th Cir. 1990) ("[I]f the government presents expert opinion about the behavior of a particular class of persons, for the opinion to have any relevance, the affidavit must lay a foundation which shows that the person subject to the search is a member of the class."). As such, they provided no nexus between the appellant's activities at work and at his home.

b. Information on computers and child pornography

Based on the two thumbnail images on the appellant's government computer, the affiant demonstrated, as required by *Nieto*, that the appellant "fit" part of this profile—the appellant was linked to child pornography "images in digital form."[60] Indeed, much of the information in these paragraphs (*e.g.*, that "[s]uch information is often maintained for very long periods of time until overwritten by other data") could provide a substantial basis for probable cause to search a device for which there was proof that "images in digital form" had *already* been accessed. However, standing alone, this information still does not establish a nexus between the thumbnail images and the appellant's home.[61]

---

[60] AE V, Encl. (3) at § IV(d).

[61] SA R asserted at the suppression hearing that he "felt that, if somebody was so bold as to use their government computer to look for child pornography, possibly, or even view, on their government computer, that if that same person has got a home computer and access to the Internet, certainly that same type of behavior is going on where they are basically unimpeded by any other governmental controls; and that they would most certainly view, access, download, and keep that child pornography, or child exploitation images for long periods of time." Record at 106. However, even assuming *arguendo* that SA R's "fe[eling]" provides a substantial basis for probable cause, we do not consider this information because it is not in the affidavit presented to the CO. *Cf. United States v. Macomber*, 67 M.J. 214, 217 (C.A.A.F. 2009) ("The affidavit stated: child pornographers and persons with a sexual attraction to children almost always maintain and possess child pornography materials such

The closest this portion of the affidavit gets to that connection is the statement that "it is normal for *offenders* to save . . . child pornography media . . . on assorted pieces of digital electronic media storage devices to include . . . desktop computers, laptop computers . . . smart telephones, [and] external hard drives[.]"[62] In *Gallo*, the copying of files to removable storage provided a nexus between downloading of child pornography on his work computer and the search of Gallo's home. 55 M.J. at 421-22.

However, in *Nieto*, an affiant's assertion that "[p]ersons who view and record sexual acts often times store and catalog their images and videos on larger storage devices such as a computer or hard drive," was not enough to establish a nexus between the appellant's cell phone and other digital devices. 76 M.J. at 105. The CAAF cautioned:

> [Reliance on a] generalized observation about the ease with which [digital] media may be replicated on a multitude and array of electronic devices, would run counter to the principle that law enforcement officials must provide specific and particular information in order for a magistrate to determine that there is a fair probability that contraband or evidence of a crime will be found in a particular place.

Id. at 108 n.5 (citations and internal quotation marks omitted) (second alteration in original). There being no evidence that the appellant *actually* engaged in copying files to computer media which he could have transferred to his home, unlike in *Gallo*, we conclude that this portion of the affidavit here was too "generalized" to provide a substantial basis for probable cause to search the appellant's home for child pornography.[63]

c. Use of the website

We find a sufficient nexus between the appellant's home and child erotica, which provides probable cause to suspect the presence of child pornography, based on statements in the affidavit that he had internet access at home, that he accessed the website on weekends, and reasonable inferences therefrom.

---

as: . . . . graphic image files . . . . These materials are stored in a secure but accessible location within their immediate control, such as in the privacy and security of their own homes, most often in their personal bedrooms.").

[62] AE V, Encl. (3) at ¶ 6j (emphasis added).

[63] We also note that paragraph J, unlike the other information on child pornography and computers in the affidavit, uses the term "offender[]," linking it to the "offender typology" which we determined *supra* was irrelevant due to the fact that the affiant offered no proof the appellant ever did "buy, produce, trade, or sell child pornography" or "molest children."

In *Clayton*, the CAAF found a sufficient nexus between the appellant's membership in a child pornography web group which was linked to his e-mail address, and a search of his "laptop, in [his] quarters, and . . . workspace," based on a "practical, commonsense understanding of the relationship between the active steps that a person might take in obtaining child pornography from a website and retaining it for an extended period of time on that person's computer." 68 M.J. at 424. It did so even though the affidavit provided no specific proof that the appellant had made any downloads, or that he had accessed his e-mail account from his quarters rather than his workspace. *Id.* at 427, 427 n.1 (Ryan and Erdmann, JJ., dissenting) (noting that Clayton "could have checked his personal email at work, or at other locations," because "the Government only knew that the account had been accessed by way of a U.S. Army server in Kuwait. It had no information regarding which computer had accessed the account").

In *Allen*, the affidavit stated that a computer to which Allen had access connected to an "on-line service" and downloaded suspected child pornography; Allen admitted he "had access to the on-line service from his residence;" and, that he had "erotica at his residence." 53 M.J. at 407. The CAAF held that:

> This information reasonably shows that [Allen] accessed child pornography through his on-line server while on duty, *had access to the same service at his residence*, had erotica at his residence, and was evasive about possessing child pornography at home. Thus, [his home] computer equipment and associated materials, such as discs or printed graphics, would be or would contain evidence of this contraband material.

Id. (emphasis added). The *Allen* Court found "substantial evidence" to search the appellant's home, without direct proof of child pornography there. *Id.*

As in *Clayton* and *Allen*, the appellant had *access* to the website not only from his workplace, but also from home, as evidenced by his reported "survey" responses detailed in the affidavit. Going beyond mere access, SA R had "observed activity on [the appellant's] account" on the website on "six dates which included weekend days."[64] There is no evidence that the appellant was in any peculiar circumstance, such as being underway on a ship, in which his government computer would have been his exclusive means to access the website during the weekend. The CO did not have to rule

[64] Affidavit at ¶ 6f.

out every other location from which the appellant could have accessed the website, in order to find probable cause to search his home.[65]

Thus, based on the appellant's reported survey responses and the timing of his website use, we find that the CO could reasonably infer the appellant accessed the website from his home.[66] We need not determine whether the military judge's finding that the appellant "was active on the site on weekends when he was not at work[,]"[67] was clearly erroneous, as our focus is on the CO's determination of probable cause from the affidavit, and the CO could infer that the appellant had accessed the website while not at work from the information provided.

The appellant argues that because SA R had neither an "[I]nternet [P]rotocol (IP) address of a computer tied to downloading images of child pornography," nor "any website conversation tying [the appellant's] home to wrongful possession of child pornography,"[68] we cannot find a nexus. We disagree. The Sixth Circuit Court of Appeals has held that even where an "affidavit did not contain direct evidence the child pornography was accessed at home," the lack of "an IP address connecting the subscriber to a particular location is not dispositive" regarding "probable cause to search [the] home[.]" *United States v. Kinison*, 710 F.3d 678, 684 (6th Cir. 2013) (citing *United States v. Terry*, 522 F.3d 645, 648 (6th Cir. 2008) ("While any IP or other information that could have more specifically tied Terry's home computer to the e-mail messages would certainly have been welcome, we are satisfied that the use of Terry's personal e-mail account in the wee hours of the morning, combined with information that Terry used his home computer to access that account, established at least a 'fair probability' that the computer used to send the messages was . . . in Terry's home")).

---

[65] *See United States v. Wagers*, 452 F.3d 534, 539 (6th Cir. 2006) (noting that where investigators learned Wagers used a particular internet service provider to purchase memberships at a child pornography site, there would have been "sufficient evidence to support probable cause" to search his home for child pornography even if the "home w[as] . . . one of two locations—home and office—served" by the provider which Wagers could have used).

[66] *See United States v. Lapsins*, 570 F.3d 758, 766-67 (6th Cir. 2009) (finding probable cause to search Lapsins' home, where the affidavit documented internet account activity involving child pornography which was conducted through "a residential cable modem in the city where Lapsins lived" at a time when he was likely to have been at home, even though "there was no direct evidence" he had ever "used a home computer to access" the internet accounts).

[67] AE XVII at 5.

[68] Appellant's Brief at 17.

In *Nieto*, there was no evidence linking Nieto's phone to the laptop besides the affiant's intuition and some general assumptions about what people do with their smartphones. Here, by contrast, there was evidence in this affidavit specifically demonstrating the appellant used the website on weekends, when the CO could reasonably infer that he was at home. Under the totality of the circumstances—such as the use of the website containing child erotica at home, combined with the thumbnail images and icon on the government computer, and the information in the affidavit about how digital images once accessed on a computer are likely to be retained—we find that the CO could infer that the appellant accessed child pornography at home, and that it would be maintained on digital devices there. Thus, we find that the CO had a substantial basis to find probable cause, with a nexus sufficient to search the appellant's home and digital devices for child pornography.

B. Consent by Ms. O to the PASS

In his ruling on the motion to suppress, the military judge also held that: the "defense failed to establish" the appellant's "standing to challenge the lawful consent by Ms. [O] to permit access to the apartment under the [United States-Japan Status of Forces Agreement ("SOFA)] or Japanese law;"[69] Ms. O "knowingly and voluntarily permitted . . . access to the apartment for the purpose of executing the [CASS];"[70] and, the seized evidence was admissible under both the good faith exception of MIL. R. EVID. 311(c)(3) and the inevitable discovery exception of MIL. R. EVID. 311(c)(2).[71] The appellant argues that the military judge erred in ruling that the appellant "did not have standing to challenge [Ms. O]'s consent,"[72] and, "that Ms. O knowingly and voluntarily permitted NCIS Agents access to the apartment for the purpose of executing the command authorized search."[73]

In abuse of discretion review, we "consider the evidence in the light most favorable to the prevailing party." *United States v. Rodriguez*, 60 M.J. 239, 246 (C.A.A.F. 2004) (citation and internal quotation marks omitted). We review the military judge's "factfinding under the clearly-erroneous standard and [his] conclusions of law under the *de novo* standard." *United States v. Ayala*, 43 M.J. 296, 298 (C.A.A.F. 1995). We will find an abuse of discretion only if findings of fact are clearly erroneous or conclusions of law are incorrect. *Id.*

---

[69] AE XVII at 19 n.3.

[70] *Id.* at 21.

[71] *Id.* at 22-25.

[72] Appellant's Brief at 24.

[73] *Id.* at 25.

1. The appellant's standing to challenge an alleged SOFA violation

We note that because the CASS was supported by probable cause, Ms. O's consent had no impact on the search's validity under the Fourth Amendment, regardless of any potential SOFA and Japanese law implications of entering the apartment without her consent.

Any constitutional requirement for Ms. O's consent (or a Japanese court's authorization) to search the apartment would thus have to derive from "treaties" being "the supreme law of the land." U.S. CONST. ART. VI. Under "Agreed View" 17(b) of the United States-Japan SOFA, "when the United States authorities deem it necessary to make searches or seizures outside facilities or areas in use by the United States Armed Forces with respect to crimes allegedly committed by United States . . . personnel, they should request Japanese law enforcement agencies to make such dispositions[.]"[74] However, "United States . . . law enforcement personnel may make searches and seizures of places occupied *exclusively* by" U.S. personnel and/or dependents.[75]

"Although treaties are the supreme law of the land . . . this is not to say that individuals always may enforce this country's treaty rights by a private law action or by invoking an exclusionary rule." *United States v. Whiting*, 12 M.J. 253, 254-55 (C.M.A. 1982) (citation omitted) (declining to apply the exclusionary rule to evidence obtained where "German authorities had not been notified of the off-base search, as was required by international agreements to which the United States and Germany were parties").

The appellant cites no law or facts to support his claim that the military judge's ruling that the appellant lacked standing to challenge whether Ms. O's consented to the search is "incorrect."[76] The fact that Article 17(b) of the SOFA expressly allows searches and seizures of U.S. personnel based *solely* on a decision of U.S. authorities, *unless* non-U.S. personnel live there, strongly suggests that the exception the appellant seeks to enforce was crafted for the benefit of the Japanese state—by preserving its control, absent exigent circumstances, over when U.S. law enforcement can search personnel subject to Japanese jurisdiction. As in *Whiting*, the appellant cannot assert this right. 12 M.J. at 255 (noting that "the performance of [treaty] obligations is exclusively within the province of the Executive and Legislative Branches").

---

[74] AE V, Joint Committee Agreements, No. 17.

[75] *Id.* (emphasis added).

[76] Appellant's Brief at 24.

Even if we assume *arguendo* that this provision of the United States-Japan SOFA confers a legal right upon Ms. O, were she on trial, we would decline to find that the *appellant* may assert a right belonging to Ms. O at his court-martial. *Cf. United States v. Padilla*, 508 U.S. 77, 81-82 (1993) (noting an "established principle is that suppression of the product of a Fourth Amendment violation can be successfully urged only by those whose rights were violated by the search itself, not by those who are aggrieved solely by the introduction of damaging evidence") (citation and internal quotation marks omitted).

2. Inevitable discovery

Even if the appellant had standing to assert noncompliance with the SOFA and benefit from the exclusionary rule, the inevitable discovery doctrine nevertheless "allow[s] admission of evidence that, although obtained improperly, would have been obtained by another lawful means." *United States v. Wallace*, 66 M.J. 5, 10 (C.A.A.F. 2008) (citing *Nix v. Williams*, 467 U.S. 431, 444 (1984)); *see also* MIL. R. EVID. 311(c)(2). In *Wallace*, the CAAF held that even "had [Williams] not ultimately consented to the seizure of the computer . . . investigators would have sought and obtained a search authorization based on probable cause" for investigation of an enticement crime which would have required "sift[ing] through" computer data, and thereby would have discovered child pornography on Wallace's computer. 66 M.J. at 10. The CAAF so decided even though "the government present[ed] no evidence" it "would have obtained a warrant" had Williams refused to grant consent to search his computer." *Id.* at 11 (Baker, J., concurring in the result).

Here, the military judge found that:

i. "[The legal advisor] opined that if [Ms. O] refused entry, they would coordinate with Japanese authorities to execute the search."[77]

ii. "[I]f [Ms. O] would not provide access, then [NCIS] would have proceeded to obtain permission to enter to conduct the command authorized search from Japanese authorities."[78]

iii. "Had [Ms. O] not granted the agents access to the apartment, the agents were prepared to liaise with Japanese authorities to secure a Japanese magistrate or judicial authorization to enter the apartment

[77] AE XVII at 10.

[78] *Id.* at 11.

to conduct the command authorized search of the accused's apartment and belongings."[79]

The appellant has not argued how any of these facts are erroneous, and we find no clear error. In light of *Wallace*, we agree with the military judge that these NCIS investigators, with probable cause to suspect that evidence of an alleged computer crime existed at the appellant's residence—and who, unlike the investigators in *Wallace*, were ready and willing to obtain a search authorization from the Japanese authorities if Ms. O refused consent—would have done so, thereby obtaining the incriminating evidence on the appellant's external hard drive and laptop.

III. CONCLUSION

The findings and the sentence are affirmed.

Judge FULTON and Judge HUTCHISON concur.

For the Court

R.H. TROIDL
Clerk of Court

[79] *Id.* at 14.