IN THE UNITED STATES NAVY-MARINE CORPS
COURT OF CRIMINAL APPEALS

Before Panel No. 2

UNITED STATES, Appellant	)	ARTICLE 62 BRIEF ON BEHALF OF APPELLANT
v.	)	Case No. 201900221
Jerry E. WHITE, Aviation Electrician's Mate First Class Petty Officer (E-6) U.S. Navy Appellee	)	Tried at Naval Base San Diego, San Diego, California, on May 9 and June 11, 2019, by a General Court-Martial convened by Commander, Navy Region Southwest, CAPT J. Stephens, JAGC, U.S. Navy (arraignment), and CAPT A. Rugh, JAGC, U.S. Navy (motions), presiding.

TO THE HONORABLE JUDGES OF THE UNITED STATES
NAVY-MARINE CORPS COURT OF CRIMINAL APPEALS

Errors Assigned

I.

DID THE MILITARY JUDGE ABUSE HIS DISCRETION FINDING THE COMMAND AUTHORIZATION FOR SEARCH AND SEIZURE LACKED PROBABLE CAUSE?

II.

DID THE MILITARY JUDGE ABUSE HIS DISCRETION FINDING THE GOOD FAITH EXCEPTION DID NOT APPLY?

Statement of Statutory Jurisdiction

The United States timely appealed the Military Judge's Ruling granting the Defense's Motion to Suppress Evidence. The barred evidence is substantial proof of a material fact that Appellee possessed child pornography. This Court has jurisdiction to hear this appeal under Article 62(a)(1)(B), Uniform Code of Military Justice (UCMJ), 10 U.S.C. § 862 (2016).

Statement of the Case

The Convening Authority referred a charge to a general court-martial alleging Appellee possessed child pornography in violation of Article 134, UCMJ, 10 U.S.C. §§ 934 (2016).

On July 16, 2019 at 0900, the Military Judge emailed the parties his Ruling granting the Defense Motion to Suppress. The Military Judge suppressed all evidence, including images of child pornography, from computer hard drives recovered at Appellee's residence. (Appellate Ex. VIII ("Ruling") at 9.)

On July 18, 2019, at 1314, the United States provided written notice of appeal to the Military Judge. (Notice of Appeal, July 18, 2019.)

Statement of Facts

A. The United States charged Appellee with possessing child pornography.

The United States charged Appellee with possessing child pornography on three hard drives in violation of Article 134, UCMJ. (Charge Sheet, May 6, 2019.)

B. Appellee moved to suppress all evidence recovered from the hard drives based on a lack of probable cause for the search authorization.

Appellee submitted a Motion to suppress the evidence found on the hard drives recovered from Appellee's residence. (Appellate Ex. IV.) The United States opposed the Motion. (Appellate Ex. V.)

C. In support of the Motions, the parties presented the Military Judge with the investigative materials, the Affidavit for the search authorization, and the NCIS Agent's testimony.

In support of his Motion, Appellee presented the Military Judge with excerpts of the investigation, including the Command Authorization for Search and Seizure of Appellee's electronics and the accompanying Naval Criminal Investigative Service Agent's Affidavit. (Appellate Ex. IV, Enclosures A–D.) At the Motions hearing the United States called the NCIS agent, Special Agent M.G, who drafted the Affidavit supporting the search authorization and conducted the search of Appellee's residence. (R. 16–32.)

1. Appellee's investigation stemmed from a Homeland Security investigation into sexual exploitation of children in the Philippines.

The Department of Homeland Security began investigating an online community that sexually exploited and trafficked children to paying customers worldwide. (Appellate Ex. IV, Enclosure A ("Homeland Security Report") at 2.) During that investigation, Homeland Security identified Christopher Villanueva as

part of a child sex trafficking organization and criminal ring in Taguig City, Philippines. (Homeland Security Report at 2.)

Mr. Villanueva was the "point of contact for live streaming sex shows involving young children" for the organization. (Homeland Security Report at 2.) He used "Yahoo! Messenger" and directed the undercover agent "to send payment to a Jusan NORIEGA" for the live streaming sex shows." (Homeland Security Report at 2.) When the undercover agent indicated he would travel to the Philippines, Mr. Villanueva offered the undercover agent "lotsa [sic] of young girls for u [sic] to fuck here in house." (Homeland Security Report at 2.)

The undercover agent learned the details of the sex ring operation from Mr. Villanueva and was able to identify the children Mr. Villanueva was exploiting. (Homeland Security Report at 2.) Mr. Villanueva was using the alias "Jusan NORIEGA, among others, to collect wire transfer payment from child sex show customers." (Homeland Security Report at 2.) "NORIEGA received said payments through several money service businesses to include Western Union, XOOM, and MoneyGram." (Homeland Security Report at 2.)

The undercover agent conducted several payments to Mr. Villanueva, who provided "historical looped video recordings of him having sex with young female children." (Homeland Security Report at 3.) Based on information from those transactions, Homeland Security obtained "transactional information, funder,

sender and recipient information" from Western Union, XOOM, and MoneyGram for the accounts associated with Mr. Villanueva. (Homeland Security Report at 3.)

2. Appellee paid "Jusan NORIEGA" and ten other recipients in the Philippines using XOOM.

XOOM records from Mr. Villanueva's investigation revealed that "Jusan NORIEGA received payments from numerous international payers, including a Jerry R. WHITE [Appellee] using the email jared90t@yahoo.com." (Homeland Security Report at 4.) Based on that information, Homeland Security obtained "all account and transactional history information for [Appellee] between dates 1/01/2010 and 10/26/2016." (Homeland Security Report at 4.)

According to the XOOM records, Appellee sent "money transfers to Jusan NORIEGA and ten (10) other recipients in the Philippines." (Homeland Security Report at 4.) The investigation identified nineteen "IP addresses" that Appellee used to send the payments. (Homeland Security Report at 4.) Homeland Security noted that each of the nineteen "IP addresses is registered to KDDI," and that "KDDI is a [Japanese] telecommunications company" which provides "mobile and internet services." (Homeland Security Report at 4.)

According to XOOM records, Appellee sent $10.00 to Jusan Noriega on May 16, 2015. (Homeland Security Report at 4.) The payment was electronically marked "Taguig City, Manila, Philippines." (Homeland Security Report at 5.)

Though the payment to Noriega was immediately available for collection, the payment was not claimed. (Homeland Security Report at 5.)

Using XOOM, Appellee sent another $743.17 to the Philippines across twenty-two transactions from May 16, 2015, to May 14, 2016. (Homeland Security Report at 4.)

Homeland Security also obtained "transactional history" for Appellee's MoneyGram and Western Union account. (Homeland Security Report at 6.) Via MoneyGram, Appellee sent 167 payments to the Philippines from 2012 to 2014. (Homeland Security Report at 6.) Of these, 102 payments went to payees in Taguig, Philippines. (Homeland Security Report at 6.) Via Western Union, Appellee sent transfers to eighteen recipients over the course of roughly three years. (Homeland Security Report at 6.) Nine of the recipients were located in the Philippines. (Homeland Security Report at 6.)

Mr. Villanueva was arrested on June 10, 2015. (Homeland Security Report at 5.) A total of fourteen underage children were rescued after Mr. Villanueva's arrest. (Homeland Security Report at 2.)

3. Homeland Security identified Appellee as a sailor stationed in Japan and transferred the investigation of Appellee to NCIS.

Homeland Security identified Appellee as a Second Class Petty Officer stationed in Atsugi, Japan, since October 23, 2015. (Homeland Security Report at 5.) Homeland Security transferred the investigation into Appellee to NCIS in

February 2017, providing them a copy of their Investigation. (Appellate Ex. IV, Enclosure B ("NCIS ROI") at 1.)

4. Naval Criminal Investigative Services prepared an Affidavit, seeking a search authorization from Appellee's Command.

Special Agent M.G. requested a Command Authorization for Search and Seizure of Appellee's apartment for "Electronic Media Storage Devices." (NCIS ROI at 21–36.) In support of the application for the search authorization, Special Agent M.G. prepared an Affidavit. (R. 21; NCIS ROI at 21–36.)

The Affidavit detailed Special Agent M.G.'s background, which included fourteen years as a special agent and experience investigating child pornography, and referenced the Homeland Security Investigation, which established Noriega as a point of contact for live streaming sex shows involving juveniles. (NCIS ROI at 24.) The Affidavit explained how Homeland Security gained Noriega's personal information, how the information was used to obtain a transactional history for Noriega within XOOM, and how Appellee was identified as one of the individuals processing payments to Noriega. (NCIS ROI at 24.)

Special Agent M.G.'s Affidavit explained how Appellee used IP addresses to accomplish his ten-dollar transfer to Mr. Villanueva in May 2015, as well as the other money transfers to the Philippines:

> [Appellee] utilized Internet Protocol (IP) addresses registered to KDDI corporation in order to effect [the May 2015 money transfer to Noriega] and several others, detailed below. KDDI Corporation is a Japanese

> telecommunications operator which has its headquarters in Chiyoda, Tokyo, Japan. Of note, "au" or "au by KDDI," is a mobile phone brand widely used in Japan which is marketed by KDDI in the main islands of Japan and Okinawa. [Appellee] owns a Japanese cellular phone (050-6294-6595), which is under contract by "au."

(NCIS ROI at 26.) Special Agent M.G. detailed Appellee's 189 monetary transactions via XOOM and MoneyGram to individuals in the Philippines, including the one to Mr. Villanueva. (NCIS ROI at 26.)

Special Agent M.G. stated: "Taguig City, Philippines, the base of operations for VILLANUEVA and the location of the recipients of the vast majority of [Appellee's] monetary transfers . . . is widely known to harbor those that engage in child exploitation and trafficking." (NCIS ROI at 26–27.)

Special Agent M.G. also provided an "offender typology" of individuals who buy, produce, trade, or sell child pornography. (NCIS ROI at 27–30.) Based on his training and experience, Special Agent M.G. explained these individuals "collect sexually explicit material" and "rarely, if ever, dispose of [that] sexually explicit material." (NCIS ROI at 28.) These individuals "obtain, collect, and maintain photographs and photographic computer files of the children" and "use such photos . . . as means of reliving fantasies" or "as keepsakes." (NCIS ROI at 28.)

The Affidavit explained that "traces of the path of an electronic communication may be automatically stored in many places," and that "[i]n

addition to electronic communications, a computer user's Internet activities generally leave traces or 'footprints' in the web cache and history files of the browser used." (NCIS ROI at 35.) "Such information," the Affidavit went on, "is often maintained for very long periods of time." (NCIS ROI at 35.)

Based on information obtained in Appellee's investigation and the offender typology, Special Agent M.G. believed there was probable cause that evidence of child pornography would be present on Appellee's electronic devices in his apartment. (NCIS ROI at 36.)

Special Agent M.G. provided the Commander with "a summary of the case" in addition to the "probable cause affidavit." (R. 19.)

5. The Commander signed the authorization, and NCIS found child pornography on three hard drives in Appellee's apartment.

The Commanding Officer signed the Command Authorization for Search and Seizure on March 23, 2017. (NCIS ROI at 21.) NCIS executed the search on March 27, 2017, and seized multiple electronic devices, including the three hard drives containing child pornography. (NCIS ROI at 19.)

D. The Military Judge granted the Defense Motion to suppress.

The Military Judge granted the Defense Motion to Suppress. (Appellate Ex. VIII ("Ruling") at 9.) The Military Judge began his "Conclusions of Law" by stating:

> The government's probable cause, as summarized in [Special Agent M.G.'s] 23 March 2017 affidavit, amounts to only three assertions:
>
> > 1. That between May 2012 and May 2016, the accused effected 189 wire or electronic transfer transactions totaling almost $5,500.00 with unknown persons located in the Philippines, including in Taguig City, Philippines;
> >
> > 2. That Taguig City is widely known to harbor persons who engage in child exploitation and child sex trafficking; and
> >
> > 3. That in May 2015, the accused electronically sent $10 to an alias of, or associate of, a person subsequently arrested for child sexual exploitation in the Philippines.

(Ruling at 6.) The Military Judge stated, "[t]here was no evidence in the affidavit that the accused owned a computer, a smart phone, or a digital storage device." (Ruling at 8.) He also concluded "[t]he affidavit was wholly silent" as to whether "[it] was . . . technologically possible to record and preserve live-streamed presentations in a digital format" and whether "[it] was . . . possible to find forensic digital evidence of [live-streamed presentations] on a person's computer afterwards." (Ruling at 7–8.)

The Military Judge's principal conclusions were as follows:

> First, the affidavit failed to establish that the accused was interacting with groups or persons engaged in the production or exchange of child pornography. . . .
>
> Likewise, the affidavit failed to establish that the accused received anything—digital contraband or otherwise—in exchange for the payment made to Noriega or the payments to the other unknown persons in the Philippines. . . .

> Finally, the affidavit was silent as to the accused's technological capability to receive or store child pornography in his home in Atsugi, Japan, at the time of the search. The affidavit did identify an email address associated with the accused's XOOM account. However, there was no other evidence that the accused regularly engaged in email, text, chat, or other electronic communications with anyone. There was no evidence in the affidavit that the accused owned a computer, a smart phone, or a digital storage device. There was no evidence in the affidavit that the accused had the hardware or software to digitally record and save live-streaming presentations, and there was no evidence in the affidavit that the accused had internet access at his home in Atsugi, Japan. . . .
>
> At every step in the chain . . . the affidavit failed to provide information sufficient to establish a nexus between the crimes alleged . . . and the place to be searched. . . .
>
> For these reasons, the court further concludes that under these circumstances exclusion is appropriate.

(Ruling at 6–8.)

Argument

I.

THE MILITARY JUDGE ABUSED HIS DISCRETION. FIRST, THE MILITARY JUDGE FAILED TO MENTION OR RECONCILE CRITICAL FACTS ESSENTIAL TO THE COMMANDER'S PROBABLE CAUSE DETERMINATION. SECOND, THE MILITARY JUDGE FAILED TO GIVE "SIGNIFICANT DEFERENCE" TO THE COMMANDER'S PROBABLE CAUSE DETERMINATION AND ERRONEOUSLY CONCLUDED THAT THERE WAS NO NEXUS BETWEEN THE SUSPECTED CRIME AND APPELLEE'S RESIDENCE.

A. Standard of review.

"A military judge's decision to admit or exclude evidence is reviewed under an abuse of discretion standard." *United States v. Michael*, 66 M.J. 78, 80 (C.A.A.F. 2008) (noting standard also applied "reviewing evidentiary rulings under Article 62"); *accord United States v. Nieto*, 76 M.J. 101, 105 (C.A.A.F. 2017). Though this Court "may act only with respect to matters of law" on interlocutory review, Article 62(b), UCMJ, 10 U.S.C. § 862(b) (2016), the Court is not "bound by the military judge's factual determinations [if] they are unsupported by the record or clearly erroneous," *United States v. Gore*, 60 M.J. 178, 185 (C.A.A.F. 2004) (citing *United States v. Burris*, 21 M.J. 140, 144 (C.M.A. 1985)). Further, conclusions of law are reviewed *de novo*. *United States v. Rodriguez*, 60 M.J. 239, 246 (C.A.A.F. 2004).

B. A Commander authorizing a search needs only a substantial basis to conclude that probable cause exists. This determination is due substantial deference.

The Fourth Amendment recognizes "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. Searches "conducted pursuant to a warrant or search authorization," however, "[are] presumptively reasonable." *United States v. Eppes*, 77 M.J. 339, 344 (C.A.A.F. 2018) (citing *United States v. Wicks*, 73 M.J. 93, 99 (C.A.A.F. 2014)).

The Military Rules of Evidence require that "[a] search authorization . . . be based upon probable cause." Mil. R. Evid. 315. "To establish probable cause, a sufficient nexus must be shown to exist between the alleged criminal activity, the things to be seized, and the place to be searched." *Eppes*, 77 M.J. at 345 (citation omitted). This 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." *Id.* at 345 (quoting *Nieto*, 76 M.J. at 106).

Importantly, a commander need only have "a substantial basis for concluding that probable cause existed." *Nieto*, 76 M.J. at 105 (quoting *United States v. Rogers*, 67 M.J. 163, 164–65 (C.A.A.F. 2009)). "A substantial basis exists 'when, based on the totality of the circumstances, a common-sense

judgement would lead to the conclusion that there is a fair probability that evidence of a crime will be found at the identified location.'" *Id.* (citing *Rogers*, 67 M.J. at 165). Such determinations "made by a neutral and detached search authority are entitled to substantial deference." *Eppes*, 77 M.J. at 345; *see also United States v. Clayton*, 68 M.J. 419, 425 (C.A.A.F. 2010) (explaining that the commander authorizing a search "is not required to resolve" questions appropriately addressed to the factfinder at the court-martial or "actions that could have been taken to enhance the law enforcement investigation").

C. The Military Judge abused his discretion by failing to discuss critical facts and failing to afford deference to the Commander's finding of probable cause.

1. As in *Ramos,* the Military Judge abused his discretion failing to mention or reconcile critical facts, resulting in incorrect conclusions of law. The Military Judge failed to mention or reconcile: (a) that the Affidavit supported Appellee's ownership of a cell phone and, possibly, a computer; (b) that the Affidavit supported the ability to discover traces of internet activities and communications years after the fact; (c) that the Affidavit explained why Appellee's payment to the known trafficker in child pornography was not collected; and (d) the facts in the Homeland Security Report that supported probable cause.

"[A] military judge abuses his discretion if his findings of fact are clearly erroneous or his conclusions of law are incorrect." *United States v. Diaz*, 69 M.J. 127, 135–36 (C.A.A.F. 2010). Even without a clearly erroneous finding of fact, a military judge abuses his discretion if he "altogether fail[s] to mention or

reconcile" critical facts. *United States v. Ramos*, 76 M.J. 372, 377 (C.A.A.F. 2017) (citing *United States v. Solomon*, 72 M.J. 176, 180 (C.A.A.F. 2013)).

In *United States v. Ramos*, the military judge concluded as a matter of law that law enforcement agents were not conducting an investigation, but were focused on "force protection." 76 M.J. at 377. But the *Ramos* court found this a legally erroneous conclusion, as the judge "declined to consider, or mention in his analysis," the critical testimony of agents that they declined to provide appellant his Article 31(b) rights "because, if they had, they 'would have had to tell him what he was suspected of and then hoped he would have continued to talk.'" *Id.* The court held this was an abuse of discretion. *Id.*

Like *Ramos*, the Military Judge abused his discretion by failing to mention or reconcile four categories of evidence. First, the Military Judge erroneously found that "the affidavit was silent as to the accused's technological capability to receive or store child pornography in his home in Atsugi, Japan, at the time of the search" and that "there was no evidence in the affidavit that the accused owned a computer[] [or] a smart phone." (Ruling at 8.) The Affidavit and the supporting investigation, however, establishes that Appellee used nineteen IP addresses registered to "KDDI corporation," a Japanese telecommunications company that provides internet and mobile services. (NCIS ROI at 26; Homeland Security Report at 4.)

The Affidavit also establishes that Appellee owned a Japanese cell phone under contract with KDDI corporation. (NCIS ROI at 26.) Viewed together, this information indicated that Appellee owned a smart phone and, potentially, a computer. The Military Judge therefore failed to mention or reconcile that the Appellee not only owned a cell phone and possibly a computer, and he further failed to address Appellee's known capability to receive and store child pornography in his home.

Second, the Military Judge erroneously stated that "[t]he affidavit was wholly silent" as to whether "[it] was . . . possible to find forensic digital evidence of [live-streamed video] on a person's computer afterwards, even years later." (Ruling at 7.) The Military Judge thereby failed to consider or reconcile the Affidavit's explanation that "traces of the path of an electronic communication may be automatically stored in many places," and that "[i]n addition to electronic communications, a computer user's Internet activities generally leave traces or 'footprints' in the web cache and history files of the browser used." (NCIS ROI at 35.) "Such information," the Affidavit continued, "is often maintained for very long periods of time." (NCIS ROI at 35.)

Third, the Military Judge erroneously concluded that the search was without probable cause because "the affidavit failed to establish that the accused received anything—digital contraband or otherwise—in exchange for the payment made to

Noriega." (Ruling at 7–8.) The Military Judge failed to consider or reconcile the Affidavit's explanation that "the last payment collected by [Noriega] on "XOOM" was completed on 15MAY15, shortly before his apprehension [on 10 June 2015] in the Philippines." (NCIS ROI at 26.)

Although Noreiga did not "claim" the funds sent by Appellee, this does not "fairly impl[y] . . . the [Appellee] received nothing for his money." (Ruling at 8.) The Affidavit supports that Noriega did not collect that payment, or any other payments, before his arrest. (NCIS ROI at 26.) But it also supports that Appellee transferred funds to a known streamer of child pornography. (NCIS ROI at 26.) That transfer of funds just as fairly implies Appellee received something for his money but that Noriega was merely unable to collect due to his arrest less than a month after Appellee's completed—or attempted—purchase. At minimum, the Military Judge needed to explicitly reconcile the timing of Appellee's transfer of funds with the timing of Noriega's arrest, and address how that timing affects probable cause. Instead, the Military Judge erroneously concluded that Noriega's failure to collect meant that Appellee received nothing.

Fourth, the Military Judge failed to discuss or mention facts outside of the Affidavit that supported probable cause. The Military Judge emphasized the Affidavit's failure to discuss whether "[it] was . . . technologically possible to record and preserve live-streamed presentations in digital format" or whether "the

accused had internet access at his home in Atsugi, Japan." (Ruling at 7.) But the Homeland Security Report, which served as the backdrop for the NCIS investigation, stated the IP addresses used to send payments from the Appellee were "each . . . registered to KDDI," who "provides fixed line, mobile and internet services." (Homeland Security Report at 4.) This Report also noted that Noriega made and shared recordings of the "[streamed] live sex shows for other customers." (Homeland Security Report at 3.)

These critical facts, which directly conflict with the Military Judge's conclusions, were known to NCIS when Special Agent M.G. provided the Commander with "a summary of the case" in addition to the "probable cause affidavit," (R. 19.), and are therefore properly considered by this Court in its probable cause review. *Cf. United States v. Lancina*, No. 201600242, 2017 CCA LEXIS 436, at *5 (N-M. Ct. Crim. App. June 30, 2017) (focusing only on evidence in affidavit where "no evidence that the [agent] orally briefed the CO beyond the contents of the affidavit"); *see generally* Mil. R. Evid. 315(f)(2) (noting that search authorization may be based on "oral statements communicated to the authorizing official in person").

Like *Ramos*, the Military Judge's failure to mention or reconcile these facts—both those in the Affidavit and the Homeland Security Report—was an abuse of discretion. *Ramos*, 76 M.J. at 377.

2. The Military Judge failed to accord "substantial deference" to the Commander's probable cause determination and erred finding no nexus between the place searched and suspected crime.

"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." *Nieto*, 76 M.J. at 106 (quoting *Clayton*, 68 M.J. at 424). This nexus "need not be based on direct observation but can be inferred from the facts and circumstances of a particular case." *Clayton*, 68 M.J. at 424 (citing *United States v. Lopez*, 35 M.J. 35, 38–39 (C.M.A. 1992)).

Courts have routinely held that "[a] law enforcement officer's professional experience may be useful in establishing such a nexus." *Nieto*, 76 M.J. at 106 (citing *United States v. Leedy*, 65 M.J. 208, 215–16 (C.A.A.F. 2007)). But "a law enforcement officer's generalized profile . . . does not, standing alone, provide a substantial basis to find probable cause." *Id.* (citing *United States v. Macomber*, 67 M.J. 214, 220 (C.A.A.F. 2009)). "[T]here must [instead] be some additional showing that the accused fit [a generalized] profile or . . . engaged in such conduct." *Id.*

Probable cause determinations "are entitled to substantial deference," and reviewing "[c]ourts should not invalidate warrants by interpreting affidavits in a hypertechnical, rather than a common sense manner." *Eppes*, 77 M.J. at 345; *see also United States v. Clayton*, 68 M.J. 419, 425 (C.A.A.F. 2010) (explaining that

the commander authorizing a search "is not required to resolve" questions appropriately addressed to the factfinder at the court-martial or "actions that could have been taken to enhance the law enforcement investigation").

a. The Military Judge failed to distinguish *Clayton*, engaged in an analysis rejected by *Clayton*, and failed to afford the Commander any "substantial deference."

In *Clayton*, the court upheld a search of the appellant's quarters and personal laptop. In support of the search, the magistrate had the following information: (1) the appellant was a member of a group that shared Internet child pornography; (2) the appellant requested e-mail transmissions from the group; (3) the appellant used an e-mail account bearing his name to access group; (4) the appellant's e-mail address was accessed in Kuwait, where the appellant was located; and (5) the appellant possessed a work laptop computer. *Clayton*, 68 M.J. at 424–25. The court concluded, in view of "the ease with which computer media may be replicated on portable devices, the information . . . was sufficient to support a practical, commonsense decision by the magistrate" that contraband would be in the appellant's quarters. *Id.* at 425.

In support of that conclusion, the *Clayton* court cited a "number of courts" that had "observed that a person's voluntary participation in a website group that had as its purpose the sharing of child pornography supported a probable cause determination that child pornography would be found on the person's computer."

Id. at 24 (citing *United States v. Gourde*, 440 F.3d 1065, 1072–73 (9th Cir. 2006) (en banc); *United States v. Martin*, 426 F.3d 68, 74–75 (2d Cir. 2005); *United States v. Froman*, 355 F.3d 882, 890–91 (5th Cir. 2004); and *United States v. Hutto*, No. 02-5210, 84 F. App'x 6, 8 (10th Cir. 2003)). The *Clayton* court recognized "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 . . . on that person's computer." *Id.*

Here, Special Agent M.G. told the Commander that: (1) Appellee sent about 189 small monetary transactions to individuals in the Philippines; (2) one of those transactions was sent to an individual known to provide streaming child pornography in exchange for online payments; (3) that transaction was made from an IP address associated with a telecommunications company in Japan; (4) Appellee was located in Japan at the time of the transaction; and, (5) Appellee owned a Japanese cell phone that utilized the same telecommunications company's network. (NCIS ROI at 26.)

The Military Judge never cited or applied *Clayton,* which is binding precedent. Instead, the Military Judge asked eleven rhetorical questions regarding the "nexus" between live-streaming child sex shows and "the acquisition of digital images or videos by the accused on his computer." (Ruling at 7.) But the *Clayton* court rejected this analysis. The commander authorizing a search "is not required

to resolve" questions appropriately addressed to the factfinder at the court-martial or "actions that could have been taken to enhance the law enforcement investigation." *Clayton* 68 M.J. at 425. Here, the Military Judge's rhetorical questions demonstrate that he failed to provide "substantial deference" to the Commander and failed to acknowledge "inferences" the Commander "reasonably could have made." *Eppes*, 77 M.J. at 345.

b. Federal courts uphold probable cause determinations to search electronic devices based on IP addresses alone.

Federal courts have given particular weight to IP addresses when analyzing the requisite nexus between crime and place. The Sixth Circuit found probable cause to search an appellant's home because the affidavit documented internet activity involving child pornography that was conducted through "a residential cable modem in the city where [the appellant] lived" even though "there was no direct evidence that [the appellant] used a home computer to access [his] accounts." *United States v. Laspins*, 570 F.3d 758, 766–67 (6th Cir. 2009).

The Fifth Circuit found "a substantial basis to conclude that evidence of criminal activity would be found at [the appellant's address]" based on an affidavit that stated "child pornography . . . had been transmitted over the IP address . . . assigned to [the appellant]." *United States v. Perez*, 484 F.3d 735, 740 (5th Cir. 2007).

And the Third Circuit held that "it was fairly probable that instrumentalities or evidence of [child pornography] . . . would be found in [the appellant's] apartment" based on an affidavit that targeted "someone using a computer with an IP address . . . assigned to a Comcast account registered to [the appellant's] apartment." *United States v. Vosburg*, 602 F.3d 512, 526–27 (3rd Cir. 2010).

As in *Lapsins*, *Perez*, and *Vosburg*, Appellee's IP history established a substantial basis for probable cause to search the electronic devices in his residence. Each of Appellee's transactions with XOOM used an IP address that was assigned to KDDI, a "Japanese telecommunications operator" with whom Appellee had cellular service. (NCIS ROI at 26.)

Even more, the fact that Appellee's IP addresses were not explicitly registered to his home—as in *Lapsins*, *Perez*, and *Vosburg*—does not work against the nexus here. The IP addresses used to facilitate Appellee's electronic transfers to the Philippines were linked to Appellee's cellphone company, KDDI. (NCIS ROI at 26.) Furthermore, KDDI "provide[d] fixed line . . . and internet services." (Homeland Security Report at 4.)

The *Clayton* court endorsed the "practical, commonsense decision" that contraband would be located in the appellant's quarters given "the ease with which computer media may be replicated on portable devices." 68 M.J. at 425. So too, here: Appellee's known subscription to KDDI's internet services supports the

practical, commonsense decision that contraband would be found in his home electronics. This is particularly so where Appellee used his KDDI internet access to send funds to a known trafficker in child pornography.

The Commander had a reasonable basis to believe that Appellee possessed the means to access the Internet at home through his contracted service with KDDI. Like *Vosburg*, *Laspins*, and *Perez*, this digital footprint provides a sufficient link between Appellee's electronic transfer of funds to a known child-pornographer and his home, which would have been reasonably expected to contain internet-enabled electronics. *See Vosburg*, 602 F.3d at 526–27; *Laspins*, 570 F.3d at 766–67; *Perez*, 484 F.3d at 740; *see also Clayton* 68 M.J. at 425.

These facts, viewed in light of the Agent's experience that "people that buy . . . child pornography . . . rarely, if ever, dispose of their sexually explicit material . . . [and] rarely destroy correspondence received from other people with similar interests," formed a substantial basis for the Commander to find probable cause to search Appellee's home. *See, e.g.*, *United States v. Gallo*, 55 M.J. 418, 422 (C.A.A.F. 2001) ("[A] gap in the nexus [can] be filled in based on the affiant's experience.").

c. <u>The type of crime, and the nature of the items to be searched, distinguish *Nieto*</u>.

A nexus "can be inferred from the facts and circumstances of a particular case." *Clayton*, 68 M.J. at 424. "Determinative factors include the type of crime,

the nature of the items sought, the extent of the suspect's opportunity for concealment, and normal inferences as to where a criminal would likely hide the property." *Id.* (citations omitted).

In *Nieto*, the court held that a magistrate lacked substantial basis to authorize a search and seizure of the appellant's laptop where he relied solely on a law enforcement agent's generalized profile of how people ordinarily use electronic devices. *Nieto*, 76 M.J. at 103. Nothing provided to the magistrate included "details about any laptop that [the appellant] may have owned." *Id.* at 103–04.

The magistrate relied solely on the law enforcement officer's statement that "[s]oldiers [use] their cell phones to photograph things" and that "they'll back those up on their laptops." *Id.* at 104. Although the *Nieto* court found this insufficient, the court noted its holding did not create "a heightened standard for probable cause or requir[e] direct evidence to establish a nexus in cases where technology plays a key role." *Id.* at 107 n.3. "Rather, the traditional standard that a nexus may be inferred . . . still holds in cases involving technological devices such as cell phones and laptops." *Id.*

Appellee's case is distinguishable from *Nieto* based on the "determinative factors" described in *Clayton*. First, the crime was different. Appellee's suspected crime involved receiving, distributing, and possessing child pornography. (NCIS

ROI 25–27.) In *Nieto,* the appellant "admitted to using his cellular telephone to view and record Soldiers using the latrine." *Nieto*, 76 M.J. at 105.

Second, the nature of items sought was different. In *Nieto*, the agents only sought photos taken on the cellular phone. *Id.* Here, Special Agent M.G. had probable cause to search for three different types of evidence relevant and responsive to the authorization: (1) evidence of Appellee's use of XOOM, MoneyGram, and Western Union; (2) evidence of web-streaming applications or access to web-streaming platforms; and, (3) photos, videos, or other material of child pornography.

Finally, Special Agent M.G.'s "offender typology" for individuals engaged in child sexual exploitation was not "technologically outdated" like the agent's general profile in *Nieto*. Nor should it matter that the Affidavit did not address if Appellee received anything for his transfers. Precedent establishes that a subscription to an email digest about pre-teen bestiality may satisfy a reasonable belief that child pornography might be found on a personal laptop. *Clayton*, 68 M.J. at 424–25. So too, Appellee's electronic transfers to individuals in Taguig City—including at least one to a known child pornography trafficker—support a substantial basis to find probable cause. *Cf. Clayton*, 68 M.J. at 424–25.

II.

THE MILITARY JUDGE ABUSED HIS DISCRETION FINDING THE GOOD FAITH EXCEPTION DID NOT APPLY. THE AFFIDAVIT WAS NOT "BARE BONES." INSTEAD, IT SUBSTANTIATED APPELLEE'S CONNECTION TO A CHILD EXPLOITATION ORGANIZATION.

A. Standard of Review.

A military judge's application of the good faith exception is reviewed for abuse of discretion. *United States v. Carter*, 54 M.J. 414, 422 (C.A.A.F. 2001).

B. The good faith exception applies when a law enforcement officer reasonably believes the commander had a substantial basis to find probable cause.

The exclusionary rule is a "judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than a personal constitutional right of the party aggrieved." *United States v. Leon*, 468 U.S. 897, 906 (1984); *accord Wicks*, 73 M.J. at 103. In the absence of an allegation a commander abandoned his detached and neutral role, suppression is appropriate only if law enforcement was dishonest or reckless in preparing their affidavit or could not have harbored an objectively reasonable belief in the existence of probable cause. *Leon*, 468 U.S. at 926; *see also Davis v. United States*, 564 U.S. 229, 236–37 (2011) (stating Supreme Court "repeatedly held" exclusionary rule's "sole purpose . . . is to deter future Fourth Amendment violations").

The "good-faith" exception provides that evidence obtained as a result of an unlawful search or seizure is admissible if: (1) the search resulted from an authorization issued by a competent official; (2) that official "had a substantial basis for determining the existence of probable cause"; and, (3) "the officials seeking and executing the authorization reasonably and with good faith relied on the issuance of the [search] authorization." Mil. R. Evid. 311(c)(3)(A)–(C) (noting that "[g]ood faith is to be determined using an objective standard").

C. The Military Judge abused his discretion declining to apply the good-faith exception. The Commander was neutral and detached, had a substantial basis, requesting officials executed the authorization reasonably, and they relied on it in good faith.

1. The Commander was competent to issue authorization.

Military Rule of Evidence 315(d) authorizes a commander to issue a search authorization so long as he or she is "impartial." Mil. R. Evid. 315(d)(1). The commander must perform his function in a neutral and detached manner, and cannot "merely serve as a rubber stamp for the police." *Carter*, 54 M.J. at 419; *see also Leedy*, 65 M.J. at 217–18.

In *Leedy*, the Court of Appeals for the Armed Forces upheld a magistrate's probable cause determination and found that the magistrate had acted in a neutral and detached manner. *Id.* The *Leedy* court noted that "there [was] no evidence that the magistrate had any generalized proclivity towards simply conceding search

requests to investigators," had "closely read the affidavit," and spoke with a legal advisor before authorizing the search. *Id.*

Here, the Commander acted in neutral and detached manner. As in *Leedy*, nothing supports that the Commander "had any generalized proclivity towards simply conceding search requests to investigators." *Id.* Special Agent M.G. explained the Commander was "inquisitive about [any given] case" and typically subjected him to questions alongside his Staff Judge Advocate. (R. 22.)

The Commander was impartial and qualified as a "competent official." Mil. R. Evid. 315(d).

2. Special Agent M.G. offered a detailed Affidavit that established probable cause, recognized shortcomings in the evidence, and contained no intentional or reckless falsehoods. His confidence in the Commander's probable cause determination was objectively reasonable.

The second prong of the good faith exception requires that "the individual issuing the authorization . . . had a substantial basis for determining the existence of probable cause." Mil. R. Evid. 311(c)(3)(B). This requirement "is satisfied 'if the law enforcement official had an objectively reasonable belief that the [authorizing official] had a 'substantial basis' for determining the existence of probable cause.'" *United States v. Perkins*, 78 M.J. 381, 387 (C.A.A.F. 2019) (citing *Carter*, 54 M.J. at 422). In other words, "the affidavit must not be

intentionally or recklessly false, and it must be more than a 'bare bones' recital of conclusions." *Carter*, 54 M.J. at 421; *see also Leedy*, 65 M.J. at 212.

The Court of Appeals for the Armed Forces routinely focuses on both the degree of detail and experience represented by an officer when analyzing whether his or her affidavit is "bare bones." In *Carter*, the court concluded that an affidavit did not qualify as "bare bones," citing the fact that the agent "identified his sources of information" as well as "conflicts and gaps in the evidence." *Carter*, 54 M.J. at 422. Similarly, in *United States v. Gallo*, the court explained the good-faith exception would apply in light of the "detailed affidavit" that was "presented by an experienced law enforcement official investigating child pornography." *United States v. Gallo*, 55 M.J. 418, 422 (C.A.A.F. 2001).

Civilian courts also look to the experience of an affiant officer in determining if the good-faith exception applies. In *United States v. Schultz*, the Sixth Circuit upheld the search of a safe deposit box where an officer's training and experience was the sole evidence establishing a nexus between the appellant's deposit box with his suspected drug trafficking. *United States v. Schultz*, 14 F.3d 1093, 1098 (6th Cir. 1994). Though the court acknowledged that experience alone was not enough to establish probable cause, and that the officer's claimed nexus was "[little] more than a guess," the court still applied the good faith doctrine because, in light of the officer's experience, the warrant was not "so lacking in

indicia of probable cause as to render official belief in its existence entirely unreasonable." *Id.* at 1097–98.

Special Agent M.G. had an objectively reasonable belief in probable cause for four reasons. First, like *Carter*, his Affidavit not only set forth the details necessary for probable cause but also recognized shortcomings in the Government's evidence. Beyond the detailed description of Appellee's XOOM transactions, the Affidavit noted that "various other wire transfers believed to be associated with [Appellee] were uncovered" but "could not be definitively traced to [Appellee]." (NCIS ROI at 26.)

Second, as in *Gallo*, Special Agent M.G. based his conclusions on significant experience with child pornography cases. *Gallo*, 55 M.J. at 422; *see also Schultz*, 14 F.3d at 1097–98.

Third, Special Agent M.G.'s belief that evidence would be found at Appellee's residence was far more than the informed "guess" that qualified for the good-faith exception in *Schultz*. *Schultz*, 14 F.3d 1097–98. Special Agent M.G. clearly detailed the link between Appellee's payment, the Japanese IP provider, and his known cellular service with that same provider. This fairly linked Appellee's online behavior to his home and associated electronics. Finally, nothing in the Record indicates that the Affidavit was false, let alone intentionally

or recklessly false. As the Military Judge commented, "nothing in the [R]ecord indicates that [Special Agent M.G.] acted with malice." (Ruling at 8.)

Special Agent M.G. thus had "an objectively reasonable belief that the [Commander] had a 'substantial basis' for determining the existence of probable cause.'" *Perkins*, 78 M.J. at 387 (citing *Carter*, 54 M.J. at 422).

3. Special Agent M.G. reasonably and with good faith relied on the issuance of the search authorization.

Officials cannot "reasonably and with good faith" rely on a search authorization where: (1) they know that the magistrate "merely rubber stamped" their search request; or (2) when the warrant is "facially defective." A warrant is facially defective where it fails "to particularize the place to be searched or the things to be seized." *Carter*, 54 M.J. at 419–21.

Neither condition applies here. Nothing in the Record suggests the Commander "rubber stamped" the search authorization. (R. 19.) Special Agent M.G. explained that he "almost always . . . forward[ed] a copy of it to [the Commander] and to his SJA." (R. 22.) "They would both have a chance to take a look at it before [the Agent] sat down" with them, and both the Commander and the Staff Judge Advocate "would bounce questions off of [the Agent.]" (R. 22.)

Furthermore, the search authorization was not "facially defective." The Commander granted authority to search Appellee's residence for "[a]ny Electronic Media Storage Devices, to include but not limited to: desktop computers, laptop

computers, cellular/mobile telephones, smart telephones, and handheld devices . . . that can be used to transmit information or communicate to another person." (NCIS ROI at 22.)

This particularized the search location and limited what could be seized. These limitations were appropriate, given "the ease with which computer media may be replicated on portable devices." *See Clayton*, 68 M.J. at 424–25.

Investigating agents complied with these parameters. This demonstrates that the agents "reasonably and with good faith" relied on the issuance of the search authorization.

Conclusion

The United States respectfully requests that this Court reverse the Military Judge's Ruling.

JOSHUA C. FIVESON
Lieutenant, JAGC, U.S. Navy
Appellate Government Counsel
Navy-Marine Corps Appellate
Review Activity
Bldg. 58, Suite B01
1254 Charles Morris Street SE
Washington Navy Yard, DC 20374
(202) 685-7976, fax (202) 685-7687
Joshua.c.Fiveson@navy.mil

BRIAN L. FARRELL
Captain, U.S. Marine Corps
Senior Appellate Government Counsel
Navy-Marine Corps Appellate
Review Activity
Bldg. 58, Suite B01
1254 Charles Morris Street SE
Washington Navy Yard, DC 20374
(202) 685-7430, fax (202) 685-7687

Certificate of Filing and Service

I certify that the original and required number of copies of the foregoing were delivered to the Court, uploaded to the Court's case management system, and that a copy of the foregoing was delivered to Appellate Defense Counsel, Captain Mary C. FINNEN, U.S. Marine Corps, on August 28, 2019.

JOSHUA C. FIVESON
Lieutenant, JAGC, U.S. Navy
Appellate Government Counsel