IN THE UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES

UNITED STATES, Appellee v. Warrant Officer One (WO1) **GRAHAM H. SMITH** United States Army, Appellant	**FINAL BRIEF ON BEHALF OF APPELLANT** USCA Dkt. No. 18-0211/AR Crim. App. Dkt. No. 20160150

TO THE JUDGES OF THE UNITED STATES COURT OF APPEALS
FOR THE ARMED FORCES:

BRYAN E. DEPOWELL, ESQUIRE
Appellate Defense Counsel
Crisp and Associates Military Law
4031 North Front Street, Suite 200
Harrisburg, Pennsylvania
(717) 412-4676
USCAAF Bar No. 37000

JULIE L. BORCHERS
Major, Judge Advocate
Branch Chief
Defense Appellate Division
US Army Legal Services Agency
9275 Gunston Road
Fort Belvoir, VA 22060
703-693-0715
USCAAF Bar No. 36843

TABLE OF CONTENTS

TABLE OF AUTHORITIES

SUPREME COURT OF THE UNITED STATES

U.S. COURT OF APPEALS FOR THE ARMED FORCES/COURT OF MILITARY APPEALS

U.S. DISTRICT COURTS

U.S. CONSTITUTION

STATUTES

RULES

IN THE UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES

UNITED STATES, Appellee v. Warrant Officer One (WO1) **GRAHAM H. SMITH** United States Army, Appellant	**FINAL BRIEF ON BEHALF OF APPELLANT** USCA Dkt. No. 18-0211/AR Crim. App. Dkt. No. 20160150

TO THE JUDGES OF THE UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES:

ISSUES PRESENTED

I.

WHETHER THE MILITARY JUDGE ABUSED HER DISCRETION IN DENYING A DEFENSE MOTION TO SUPPRESS EVIDENCE OBTAINED FROM APPELLANT'S CELLULAR TELEPHONE BECAUSE ACCESS TO THE CONTENTS OF THE IPHONE WOULD NOT HAVE BEEN AVAILABLE BUT FOR THE GOVERNMENT'S ILLEGAL SEARCH AND THE GOOD FAITH DOCTRINE WOULD BE INAPPLICABLE UNDER THE CIRCUMSTANCES.

II.

WHETHER THE ARMY COURT ERRED IN DETERMINING THE INSUFFICIENT NEXUS ISSUE WAIVED BECAUSE THERE WAS NO DELIBERATE DECISION NOT TO PRESENT A GROUND FOR POTENTIAL RELIEF BUT INSTEAD ONLY A FAILURE TO SUCCINCTLY ARTICULATE THE GROUNDS UPON WHICH RELIEF WAS SOUGHT.

STATEMENT OF STATUTORY JURISDICTION

The Army Court of Criminal Appeals (Army Court) had jurisdiction over this matter pursuant to Article 66, Uniform Code of Military Justice (UCMJ), 10 U.S.C. § 866 (2012). This Honorable Court has jurisdiction over this matter under Article 67(a)(3), UCMJ, 10 U.S.C. § 867(a)(3) (2012).

STATEMENT OF THE CASE

On March 9, 2016, a military judge sitting as a general court martial convicted Warrant Officer One (WO1) Graham H. Smith [hereinafter appellant], contrary to his pleas, of two specifications of other sexual misconduct in violation of Article 120c, UCMJ, 10 U.S.C. §920c (2012). (JA 010-011). The military judge sentenced appellant to be confined for two months and to be dishonorably discharged from the service. (JA 010). On May 20, 2016, the convening authority approved the findings and sentence as adjudged. (JA 010).

On February 28, 2018, The Army Court affirmed the findings and sentence. (JA 001-009). Appellant was notified of the Army Court's decision and, in accordance with Rule 19 of this Court's Rules of Practice and Procedure, filed a Petition for Grant of Review on April 27, 2018, along with a motion to file the supplement separately under Rule 30. On April 30, 2018, this Court granted the motion extending the time to file the supplement to May 17, 2018. On July 26, 2018, this Court granted Appellant's petition for review.

STATEMENT OF FACTS

On July 15, 2014, while grocery shopping at the commissary on Fort Rucker, Alabama, JW noticed a broad, muscular, white, male wearing a t-shirt and shorts. (JA 112). She walked into the refrigerated produce area of the store and noticed this same individual out of her peripheral vision, coming up alongside her. (JA 113). JW observed the individual crouch down next to her and believed he was attempting to take a photograph under her dress using his cellular telephone. (JA 113).

JW reacted loudly, drawing attention to the area and causing WO1 Smith to hastily head for the exit. (JA 113-114). A uniformed individual entering the commissary, later identified as Master Sergeant (MSG) Mark T. Clarke, heard the commotion. Observing JW trailing WO1 Smith to the door, MSG Clarke blocked WO1 Smith's exit, seized WO1 Smith's cellular telephone by placing his hand over the phone, held onto the phone, and thereby prevented any further access to the device.[1] (JA 113).

Within minutes, military police were on the scene. (JA 153). Sergeant (SGT) Michael Durkin was the first military police officer to arrive. (JA 076). MSG Clarke gave the phone to SGT Durkin who then gave the phone to Military

[1] Master Sergeant Clarke later testified, substantially, that he relieved the man of his phone for safekeeping and preservation of evidence. (JA 148-153).

Police Investigator [hereinafter Investigator] William Kesler. (JA 076-077). At the time of the seizure, the phone was locked and military police investigators did not have access to its contents because they did not have the password. (JA 077). They also had not seen (and neither had WO1 Smith) any alleged photos. (JA 077). Based upon JW's report, Investigator Kesler contacted part-time military magistrate, Major (MAJ) Jennifer Farmer. (JA 077). Investigator Kesler sought and obtained a *verbal* search authorization for "all Apple related products capable of connecting to iCloud, desktop/laptop computers, data storage cards, external storage drives, and wireless router/storage combined devices."[2] When the search authorization was later memorialized in writing, Investigator Kesler opined the following:

> Based on the technology and capability built into Apple products, known as the iCloud, we have reason to believe any pictures taken with the iPhone have been synchronized wirelessly with the iCloud allowing them to be synchronized with all Apple linked to Smith's Apple account. In addition, those items can be accessed by the internet to be viewed and or distributed to other parties electronically. It is paramount to the resolution and for the preservation of evidence related to this investigation that Smith's residence be searched for any additional electronic devices that are able to access the internet and store data digitally.

(JA 271).

[2] *See* Search and Seizure Authorization dated 15 July 2014. (JA 271-272).

On July 16, 2014, military police investigators conducted a search of WO1 Smith's residence where they seized several additional electronic items, including two laptop computers. (JA 221). Shortly thereafter, the Fort Rucker Criminal Investigation Command (CID) office took responsibility for the investigation. Special Agent Howell applied for and received a search authorization to conduct a digital forensic examination (DFE) of WO1 Smith's previously seized electronic devices.[3] Special Agent Howell's affidavit supporting his request for a search authorization relied on the information provided by Investigator Kesler and added no new information. (JA 267). Warrant Officer One Smith's iPhone (which was still locked via a password) and the other electronic devices seized from his residence were sent to the Fort Benning CID office where Digital Forensic Examiner Special Agent Troy Pugliese conducted the DFE. (JA 165). Special Agent Pugliese, not able to open the iPhone directly, was ultimately able to gain access to the phone and its contents by searching for and obtaining a file from the laptop computer seized on July 16, 2014, during the search of WO1 Smith's residence. (JA 165). The exact name of the file was "7bce93979fefced4e4a9f790eeee497937db94c7.plist." (JA 362). Specifically, SA Pugliese searched the seized laptop for a file that the computer used to communicate with the iPhone. (JA 165). Manipulation of this file allowed him to

[3] *See* Search and Seizure Authorization dated 25 August 2014. (JA 267-274).

bypass the password function on WO1 Smith's iPhone. (JA 165). Absent this computer, CID would have been unable to unlock WO1 Smith's iPhone. (JA 165).

A search of the iPhone after the password had been bypassed revealed eight video files. (JA 285). These video files were contained only on the iPhone (not on any other computer and particularly not on the computer used to bypass the iPhone password). (JA 284-287). Aside from JW's statement regarding her observations that day, a disk containing the videos was the only other evidence offered by the government in support of the charge and its specifications. (JA 013).

STANDARD OF REVIEW

This Court reviews a military judge's evidentiary ruling on a motion to suppress for an abuse of discretion. *United States v. Rader*, 65 M.J. 30, 32 (C.A.A.F. 2007); *United States v. Khamsouk*, 57 M.J. 282, 286 (C.A.A.F. 2002). This Court reviews findings of fact under the clearly erroneous standard and conclusions of law de novo. *United States v. Rodriguez*, 60 M.J. 239, 245 (C.A.A.F. 2004). On mixed questions of law and fact, "a military judge abuses his discretion if his findings of fact are clearly erroneous or his conclusions of law are incorrect." *United States v. Ayala*, 43 M.J. 296, 298 (C.A.A.F. 1995).

SUMMARY OF ARGUMENT

The military judge abused her discretion in denying the defense motion to suppress the evidence obtained from WO1 Smith's iPhone for several reasons.

First, Investigator Kesler's initial application for a search authorization failed to provide a sufficient nexus between the items sought and the alleged wrongdoing under investigation. Speculation about habits regarding the use of cell phones and technology cannot and should not constitute evidence that can be used in support of a particularized authorization to search. Here, where the military magistrate did not have a substantial basis to find probable cause for the search authorization, this Court should apply the exclusionary rule. Additionally, the good faith exception to the exclusionary rule is applicable only when investigators act with an objectively reasonable good faith belief that their conduct is lawful. *See Davis v. United States*, 564 U.S. 229, 238 (2011)(citing *United States v. Leon*, 468 U.S. 897, 906 (1984)). Investigator Kesler's reliance on the magistrate's determination that probable cause existed, which was based on Investigator Kesler's own unsupported opinion, was not objectively reasonable.

Second, SA Agent Pugliese's actions in obtaining access to the iPhone constituted an illegal search that exceeded the scope of the authorization. Special Agent Puglese—*based on his own testimony*—exceeded the scope of what he reasonably believed he was authorized to search for. Thus, the search he conducted was unreasonable, and the military judge should have suppress the evidence obtained as the result of that search. Further, willfully exceeding the

scope of a search authorization is not objectively reasonable, and as such, the good faith doctrine is inapplicable to SA Pugliese's actions.

Finally, the Army Court erred in determining that any issues surrounding SA Pugliese's unlawful search of appellant's laptop were waived. Waiver constitutes a deliberate decision not to present a ground for relief that might be available in the law. *See United States v. Campos*, 67 M.J. 330 (C.A.A.F. 2009) (citing *United States v. Cook*, 406 F.3d 485, 487 (7th Cir. 2005)). In determining whether an issue is waived versus merely forfeited, this Court considers whether the failure to raise the objection at trial was the intentional relinquishment of a known right. *See United States v. Sweeney*, 70 M.J. 296, 304 (C.A.A.F. 2011) (citing *United States v. Harcrow*, 66 M.J. 154, 157-158 (C.A.A.F. 2008)). Here, no such deliberate relinquishment occurred. Defense counsel challenged the search of the iPhone, as well as the other seized electronic items (to include the laptop used to gain access to the iPhone), as overly broad. (JA 195-227). Although the relationship between the seized laptop and access to appellant's iPhone was not specifically articulated in the motion to suppress, this should not be considered a waiver. The government lacked probable cause to support the search and seizure of all of appellant's internet capable electronic items, which appellant specifically noted in his motion to suppress the evidence illegally obtained from his iPhone. (JA 195-227).

However, if this court finds that the issue was not properly preserved, then appellant urges that this court review for plain error.

LAW AND ARGUMENT

I.

THE MILITARY JUDGE ABUSED HER DISCRETION IN DENYING A DEFENSE MOTION TO SUPPRESS EVIDENCE OBTAINED FROM APPELLANT'S CELLULAR TELEPHONE BECAUSE ACCESS TO THE CONTENTS OF THE IPHONE WOULD NOT HAVE BEEN AVAILABLE BUT FOR THE GOVERNMENT'S ILLEGAL SEARCH AND THE GOOD FAITH DOCTRINE WOULD BE INAPPLICABLE UNDER THE CIRCUMSTANCES.

Law

The Fourth Amendment requires that "no Warrants shall issue, but upon probable cause." U.S. Const. amend IV. Probable cause relies on a "common-sense decision whether, given all the circumstances…there is a fair probability that contraband" will be found. *United States v. Leedy*, 65 M.J. 208, 213 (C.A.A.F. 2007) (quoting *Illinois v. Gates*, 462 U.S. 213, 236 (1983).

> The threshold for probable cause is subject to evolving case-law adjustments, but at its core it requires factual demonstration or reason to believe that a crime has or will be committed. As the term implies, probable cause deals with probabilities. It is not a "technical" standard, but rather is based on "factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." Probable cause requires more than a bare suspicion, but something less than a preponderance

> of the evidence…The duty of the reviewing court is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit…there is a fair probability that contraband or evidence of a crime will be found in a particular place.

Leedy, 65 M.J. at 213 (citations omitted).

"Stated differently, in 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. *United States v. Nieto*, 76 M.J. 101, 106 (C.A.A.F. 2017) (citing *United States v. Rogers*, 67 M.J. 162, 166 (C.A.A.F. 2009) and *United States v. Gallo*, 55 M.J. 418, 421 (C.A.A.F. 2001)). "The question of nexus focuses on whether there was a 'fair probability' that contraband or evidence of a crime will be found in a particular place." *United States v. Clayton*, 68 M.J. 419, 424 (C.A.A.F. 2009) (citations omitted).

Evidence obtained as the result of an unlawful search or seizure must be suppressed unless:

> (A) The search or seizure resulted from an authorization to search, seize, or apprehend issued by an individual competent to issue the authorization under Mil. R. Evid. 315(d) or from a search warrant or arrest warrant issued by a competent civilian authority;
>
> (B) The individual issuing the authorization or warrant had a substantial basis for determining the existence of probable cause; and
>
> (C) The officials seeking and executing the authorization or warrant reasonably and with good faith relied on the

> issuance of the authorization or warrant. Good faith is to be determined using an objective standard.

Mil. R. Evid. 311(c)(3).

There is a substantial basis for determining the existence of probable cause "if the law enforcement official has an objectively reasonable belief that the magistrate had a 'substantial basis' for determining the existence of probable cause." *United States v. Carter*, 54 M.J. 414, 421 (C.A.A.F. 2001) (citations omitted).

"Courts give 'great deference' to the magistrate's probable cause determination because of the Fourth Amendment's strong preference for searches conducted pursuant to a warrant." *Gates*, 462 U.S. at 236. "However, this deference is 'not boundless,' and a reviewing court may conclude that 'the magistrate's probable-cause determination reflected an improper analysis of the totality of the circumstances." *Nieto*, 76 M.J. at 105 (quoting *United States v. Leon*, 468 U.S. 897, 915 (1984). In evaluating the issuing search authority's probable cause finding, reviewing courts examine: "1) the facts known to the authority when he issued the warrant and 2) the manner in which he came to know these facts." *Leedy*, 65 M.J. at 214.

Where a military magistrate does not have a substantial basis to find probable cause, military courts ordinarily apply the exclusionary rule unless there is an applicable exception. *See* Mil. R. Evid. 311(a). The good faith exception to

the exclusionary rule is applicable when investigators "act with an objectively reasonable good faith belief that their conduct is lawful." *Davis v. United States*, 564 U.S. 229, 238 (2011)(citing *United States v. Leon*, 468 U.S. 897, 906 (1984)). The test for good faith is "whether a reasonably well-trained officer would have known that the search was illegal…in light of all the circumstances." *Herring v. United States*, 555 U.S. 135, 145 (2009) (citing *Leon*, 468 U.S. at 922, n.23). The good faith exception applies to conduct involving only "simple, isolated negligence," but not to conduct amounting to a "deliberate, reckless, or grossly negligent disregard of Fourth Amendment rights." *Davis*, 564 U.S. at 238.

This Court may not set aside the finding of the court-martial "unless the error materially prejudices the substantial rights of the accused." Article 59(a), UCMJ, 10 U.S.C. § 859(a). "A constitutional error is harmless when it appears beyond a reasonable doubt that the error complained of did not contribute to the verdict obtained." *Mitchell v. Esparza*, 540 U.S. 12, 17-18 (2003) (internal quotations marks omitted); *accord United States v. Mott*, 72 M.J. 319, 332 (C.A.A.F. 2013).

Argument

Both the initial seizure of appellant's internet capable electronic devices by Investigator Kesler and the later search of appellant's laptop where SA Pugliese manipulated a file to gain access to appellant's iPhone constitute violations of the

Fourth Amendment rendering any evidence obtained fruits of an illegal search that were improperly admitted at trial over defense objection. The good faith exception is inapplicable, and the government cannot show that these errors were harmless beyond a reasonable doubt.

1. Investigator Kesler's initial application for a search authorization failed to provide a sufficient nexus between the items sought and the alleged wrongdoing under investigation.

Appellant does not contest that Major Farmer was the part-time military magistrate at Fort Rucker when this incident occurred. By virtue of that position, she was a person competent to issue search and seizure authorizations. However, the only evidence available to Investigator Kesler at the time he sought a search authorization was the locked iPhone itself. (JA 108). Investigator Kesler had no information regarding Appellant's phone settings, whether the iPhone was synced to other devices or computers, or if the iPhone belonged to the appellant. The iPhone was locked when it was seized such that no access to the operating system or internal settings was possible. (JA 108). Nevertheless, Investigator Kesler opined that there existed "reason to believe any pictures taken with the iPhone have been synchronized wirelessly with the iCloud allowing them to be synchronized with all Apple products linked to Smith's apple account." (JA 020-021). Investigator Kesler made this assertion to Major Farmer even though he was: (1) completely unaware of the phone's settings regarding syncing with the

iCloud; (2) completely unaware if the phone had ever been synced with a computer; and (3) completely unaware if any actual photos existed on the phone. Ultimately, the only nexus linking the iPhone taken from appellant to the items seized at Investigator Kesler's request was the one created by the generalized opinion of Investigator Kesler himself. Such an opinion is more akin to a guess and, as here, absent any connection to the available evidence, cannot support even the minimum probable cause necessary to render his search constitutional.

2. Without an evidentiary nexus, Investigator Kesler's reliance on the warrant was not objectively reasonable, thus the good faith exception is inapplicable.

At the time he sought a search authorization, Investigator Kesler did not have an objective belief that the magistrate had a substantial basis for finding probable cause. The only support for the search and seizure of all appellant's internet capable devices was Investigator Kesler's own opinion regarding the syncing habits of individuals with iPhones. He was unable to access the phone due to the password protection and any objective information about the phone's settings was thus unavailable to him.

Under the these circumstances there was not sufficient probable cause to support his request. Investigator Kesler's "reason to believe" was nothing more than his own opinion. Indeed, MAJ Farmer testified that Investigator Kesler told her "the phone could also be used with the Cloud technology." (JA 024).

However, such speculation about what a phone could do is not a '"fair probability' that contraband or evidence of a crime will be found in a particular place." *Clayton*, 68 M.J. at 424 (citations omitted). Regardless of his personal experience, Investigator Kesler had no evidentiary nexus by which to connect the item he sought to seize to appellant's alleged actions in the Fort Rucker commissary.

The information Investigator Kesler provided to support the seizure of internet capable electronic devices was a speculative guess based on his own opinion rather than articulable facts from which MAJ Farmer could reasonably have believed that evidence of a crime would be found on those devices. He had no idea if the phone contained any pictures from the commissary, whether appellant synced his phone with the iCloud, if the phone had the ability to sync content automatically, or whether appellant even owned other electronic devices capable of viewing synced content. Investigator Kesler's reliance on MAJ Farmer's determination that there was probable cause is unreasonable because her determination was based on his unsupported opinion. Thus, Investigator Kesler could not have had an "objectively reasonable belief that the magistrate had a 'substantial basis' for determining the existence of probable cause." *See Carter*, 54 M.J. at 421 (citations omitted). For these reasons, the good faith exception is inapplicable and cannot save this otherwise illegal search.

3. <u>Special Agent Pugliese's actions in obtaining access to the iPhone were an illegal search that exceeded the scope of the authorization.</u>

In order to access appellant's phone, SA Pugliese had to first search for a particular file necessary to unlock the password-protected iPhone. (JA 108). He then had to isolate that file from other files on the seized laptop. (JA 108, 165, 362). Finally, SA Pugliese manipulated the file in order to gain access to the iPhone. (JA 108, 165, 362). These actions were not ancillary to the search, but were, in fact, necessary actions without which the iPhone would have remained in its locked and secured state. Considering that this search was conducted in conjunction with SA Pugliese's understanding of the scope of the authorization, (JA 109, 284, 359), he knowingly exceeded the scope of what he believed the authorization permitted.

According to his own testimony, SA Pugliese believed that he had authority to search for "pictures, video, emails, documents, and texts related to other sexual misconduct." (JA 109).[4] However, his search of the laptop for the file necessary to unlock the iPhone does not fall into any of these categories. Special Agent Pugliese's search was for something entirely different. When asked how he obtained access to the iPhone he stated, "[t]o get into that iPhone, because it was

[4] "I thought I was looking for evidence related to the offense of other sexual misconduct." (JA 157).

locked, I had to get a file off the computer that the computer uses to communicate with the phone . . . and that allows the forensic software to then actually extract data from the phone." (JA 108). Based on his own testimony, he reasonably believed that he was authorized to search for "pictures, videos, emails, documents, and texts." (JA 109). Yet, he searched for a file that would allow him access to the iPhone.

Assuming *arguendo* that the search authorization was valid, SA Pugliese's actions still exceeded the scope of the authorized search. The good faith exception is inapplicable where SA Pugliese, by his own admission, exceeded the scope of what he believed he was able to search. (JA 109, 157). The willful and purposeful actions of a government agent in exceeding the scope of a search authorization are not objectively reasonable.

Ultimately, what the Army Court considered SA Pugliese's "reliance on technological acumen[,]" (JA 009), was really an unlawful search. The Army Court's description of SA Pugliese's search of the laptop as merely using "the laptop as a 'key' to open the locked iPhone" ignores the fact that SA Pugliese was not authorized to search for the "key." (JA 009). Since his actions were not objectively reasonable, the good faith exception to the exclusionary rule is inapplicable. Based on the foregoing, the evidence seized from the iPhone though the use of the laptop should have been suppressed.

4. <u>The government cannot show that these errors were harmless beyond a reasonable doubt.</u>

An error of constitutional dimension "requires either automatic reversal or an inquiry into whether, beyond a reasonable doubt, the error did not contribute to a defendant's conviction or sentence." *See United States v. Davis*, 26 M.J. 445 (C.M.A. 1988). *See also Chapman v. California*, 386 U.S. 18 (1967); *United States v. Moore*, 1 M.J. 390 (C.M.A. 1976). The evidence offered by the government consisted primarily of eight video files. (JA 013). These video files were contained only on the iPhone. (JA 285). They were not on any other computer and were not found on the laptop used to bypass the iPhone security. (JA 286). Thus, the video files would have been unavailable to the government absent the search by SA Pugliese.

The remaining evidence, the testimony of JW, is insufficient to sustain appellant's conviction. JW was unsure if appellant actually filmed anything. (JA 124). She observed him out of her peripheral vision. (JA 122). She did not see any videos in the commissary and was unaware of the settings on WO1 Smith's iPhone. (JA 124). In fact, during the exchange she was heard telling appellant, "[I]f you didn't do anything, I'm sorry." (JA 152). Therefore, the only direct evidence offered by the government to support the alleged offenses were the illegally recovered video files. Absent this evidence, the testimony of JW would

have been insufficient to convict appellant. Thus, the government cannot show that these errors were harmless beyond a reasonable doubt.

II.

THE ARMY COURT ERRED IN DEEMING THE INSUFFICIENT NEXUS ISSUE WAIVED SINCE THERE WAS NO DELIBERATE DECISION NOT TO PRESENT A GROUND FOR POTENTIAL RELIEF BUT INSTEAD ONLY A FAILURE TO SUCCINCTLY ARTICULATE THE GROUNDS UPON WHICH RELIEF WAS SOUGHT.

Law

"Whereas forfeiture is the failure to make the timely assertion of a right, waiver is the 'intentional relinquishment or abandonment of a known right.'" *United States v. Olano*, 507 U.S. 725, 732 (1993) (internal quotations omitted) (citations omitted).

"[T]here is a presumption against the waiver of constitutional rights, and for a waiver to be effective it must be clearly established that there was an intentional relinquishment of a known right or privilege." *United States v. Harcrow*, 66 M.J. 154, 157 (C.A.A.F. 2008). "To determine whether a failure to object was waiver or mere forfeiture, we look to the state of the law at the time of trial, and we will not find waiver where subsequent case law 'opened the door for a colorable assertion of the right…where it was not previously available.'" *United States v.*

Sweeney, 70 M.J. 296, 304 (C.A.A.F. 2011) (citing *United States v. Harcrow*, 66 M.J. 154, 157-158 (C.A.A.F. 2008)).

A "forfeiture, subject to review for plain error, is basically an oversight; a waiver is a deliberate decision not to present a ground for relief that might be available in the law." *United States v. Campos*, 67 M.J. 330 (C.A.A.F. 2009) (citing *United States v. Cook*, 406 F.3d 485, 487 (7th Cir. 2005)). Plain error occurs "where (1) there was error, (2) the error was plain and obvious, and (3) the error materially prejudiced a substantial right of the accused." *Sweeney*, 70 M.J. at 304 (citations omitted). "Where, as here, the alleged error is constitutional, the prejudice prong is fulfilled where the Government cannot show that the error was harmless beyond a reasonable doubt." *Id*.

Argument

1. The insufficient nexus issue was not waived.

Although defense counsel challenged the search authorization and seizure of appellant's internet capable electronic devices by filing a motion to suppress, counsel did not specifically articulate a challenge to the way in which one of the those illegally seized devices, appellant's laptop, was used, to unlock appellant's iPhone. This, however, should not be considered waiver and thus fatal to further review. The government lacked probable cause to support the search and seizure of all of appellant's internet capable electronic items, which appellant specifically

noted in his motion to suppress the evidence illegally obtained from his iPhone. (JA 195-227).

Not only did appellant not intentionally relinquish his right to challenge the manner in which his illegally seized electronic devices were used during the DFE, this court reached its decision in *United States v. Nieto* well after the trial in this case concluded. In *Nieto*, this Court articulated that probable cause sufficient to support a search authorization must demonstrate a "particularized nexus" between the alleged crime and the item sought. *See Nieto*, 76 M.J. at 107. Mere speculation pertaining to general behavior is wholly insufficient. *Id*.

Here, just as in *Nieto*, the information provided by investigators to the military magistrate was not based on a "firm factual foundation" linking appellant's alleged misconduct involving an iPhone in the Fort Rucker commissary to his ownership of a laptop capable of communicating with that phone later seized from his residence. *Id*. Further, had the military judge properly excluded the evidence obtained from the illegally seized laptop, there would have been no need for appellant to articulate to the court how the digital forensic examiner's use of the laptop was also illegal. Thus, because this court has now articulated in *Nieto* the requirement for a particularized nexus between the alleged crime and the items sought—which was not articulated in this case and where appellant also moved to suppress—appellant would urge that this

court "not find waiver where subsequent case law 'opened the door for a colorable assertion of the right…where it was not previously available.'" S*weeney*, 70 M.J. at 304 (citations omitted).

2. <u>Even if this court determines that appellant forfeited the right to challenge the search of his laptop and use of his laptop to unlock his phone, this court should still review for plain error.</u>

a. There was plain and obvious error.

As discussed above, Investigator Kesler's initial application for a search authorization failed to provide a sufficient nexus between the items sought and the alleged wrongdoing under investigation. Further, without any evidentiary nexus, his reliance on the warrant authorized by the military magistrate was not objectively reasonable and the good faith exception is inapplicable. Additionally, SA Pugliese's actions in obtaining access to the iPhone though appellant's laptop constituted an illegal search that exceeded the scope of the authorization.

Although the relationship between the seized laptop and access to appellant's iPhone was not specifically articulated in the defense motion to suppress, the defense did challenge the search authorization as overly broad. Further, SA Pugliese, by his own admission, exceeded the scope of the authorized search. (JA 109, 157). Defense counsel's failure to specifically identify this way in which this search of appellant's laptop exceeded the scope of an already overly

broad search authorization was not the intentional relinquishment of a known right but rather an oversight made clear by this court's subsequent decision in *Nieto*.

b. The error materially prejudiced appellant's substantial rights.

"Where, as here, the alleged error is constitutional, the prejudice prong is fulfilled where the Government cannot show that the error was harmless beyond a reasonable doubt." *Sweeney*, 70 M.J. at 304. Again, absent the evidence obtained in violation of appellant's Fourth Amendment rights, the only other evidence offered by the government was JW's testimony. Because of her admitted uncertainly about appellant's actions, it alone is insufficient to show that the error was harmless beyond a reasonable doubt.

3. If the court finds that the insufficient nexus issue was waived then, appellant urges this court to consider whether trial defense counsel were ineffective.

If this Court were to find that the suppression issue was not properly preserved, then appellant urges this court to analyze the issue under a doctrine of forfeiture rather than waiver. Alternatively, if this Court believes the issue was waived, then this Court should review the defense counsel's failure to preserve the issue as one of ineffective assistance of counsel under *Strickland v. Washington*, 466 U.S. 668, 687 (1984).

CONCLUSION

At the time he sought a search authorization for all of WO1 Smith's internet capable electronic devices, Investigator Kesler did not know the settings for WO1 Smith's iPhone or whether the phone was set to sync with the iCloud. He had no idea if WO1 Smith was aware of the iCloud. He had no idea what additional electronic devices appellant owned, which of those might be capable of communicating with an iPhone, or if the locked iPhone was ever linked with or synced to any other device. Investigator Kesler did not even know if the locked iPhone contained evidence of any crime. In spite of this, Investigator Kesler offered the military magistrate a guess; his opinion about the way people might use their phones based on the internet and technology.

As this court has since made clear, such speculation about what a phone could do is not a "fair probability that contraband or evidence of a crime will be found in a particular place." *Clayton*, 68 M.J. at 424. *See also Nieto*, 76 M.J. at 107 (holding that probable cause sufficient to support a search authorization must demonstrate a "particularized nexus" between the alleged crime and the item sought). Mere speculation pertaining to general behavior is insufficient. Further, where the military magistrate's determination was based on Investigator Kesler's speculation, Investigator Kesler could not have had an "objectively reasonable

belief that the magistrate had a 'substantial basis' for determining the existence of probable cause." *Carter*, 54 M.J. at 421 (citations omitted).

After law enforcement officials obtained appellant's iPhone and other internet capable devices, those devices were forensically examined by CID. By his own admission, SA Pugliese, the DEF examiner, believed he had permission to search for evidence related to "the offense of other sexual misconduct." (JA 157). He then conducted a search for something completely different, a file needed to bypass the password protection of the iPhone. Again, although he objectively knew this was not evidence he was authorized to seek, he nonetheless conducted the search thereby purposefully exceeding the scope of the search authorization.

Finally, while defense counsel challenged the search authorization and seizure of all of appellant's internet capable electronic devices, he did not specifically articulate a challenge to the way in which one of those illegally seized devices, appellant's laptop, was used to unlock appellant's iPhone. However, the government lacked probable cause to support the seizure and search of all of appellant's internet capable electronic items, which appellant specifically noted in his motion to suppress the evidence illegally obtained from his iPhone. (JA 195-227). Additionally, because this court has now articulated in *Nieto* the requirement for a particularized nexus between the alleged crime and

the items sough, appellant would urge that this court "not find waiver where subsequent case law 'opened the door for a colorable assertion of the righter…where it was not previously available.'" *Sweeney*, 70 M.J. at 304 (citations omitted).

WHEREFORE, appellant respectfully requests this Honorable Court set aside the findings of guilty and the sentence.

BRYAN E. DEPOWELL, ESQUIRE
Civilian Appellate Defense Counsel
Crisp and Associates Military Law
4031 North Front Street, Suite 200
Harrisburg, Pennsylvania
(717) 412-4676
USCAAF Bar No. 37000

JULIE L. BORCHERS
Major, Judge Advocate
Branch Chief, Defense Appellate Division
US Army Legal Services Agency
9275 Gunston Road
Fort Belvoir, VA 22060
703-693-0715
USCAAF Bar No. 36843

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Rule 24(c) because it contains 5,766 words.

This brief complies with the typeface and type style requirements of Rule 37 because it has been prepared in Times New Roman font, using 14-point type with one-inch margins.

CERTIFICATE OF FILING AND SERVICE

I certify that a copy of the foregoing was electronically delivered to the Court and the Government Appellate Division on September 24, 2018.

JULIE L. BORCHERS
Major, Judge Advocate
Branch Chief, Defense Appellate Division
USCAAF Bar No. 36843
US Army Legal Services Agency
9275 Gunston Road
Fort Belvoir, VA 22060
703-693-0715
USCAAF Bar No. 36843