

IN THE UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES

UNITED STATES,

Appellee

v.

Private First Class (E-3)

JEFFREY G. EUGENE

United States Army,

Appellant

**FINAL BRIEF ON BEHALF OF
APPELLANT**

USCA Dkt. No. 18-0209/AR

Crim. App. Dkt. No. 20160438

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

BENJAMIN A. ACCINELLI
Captain, Judge Advocate
Appellate Defense Counsel
Defense Appellate Division
U.S. Army Legal Services Agency
9275 Gunston Road
Fort Belvoir, Virginia 22060
(703) 693-0682
USCAAF Bar No. 36899

DANIEL C. KIM
Captain, Judge Advocate
Appellate Defense Counsel
Defense Appellate Division
USCAAF Bar No. 36754

JULIE L. BORCHERS
Major, Judge Advocate
Branch Chief
Defense Appellate Division
USCAAF Bar No. 36843

CHRISTOPHER D. CARRIER
Lieutenant Colonel, Judge Advocate
Chief, Capital and Complex Litigation
Defense Appellate Division
USCAAF Bar No. 32172

ELIZABETH G. MAROTTA
Colonel, Judge Advocate
Division Chief
Defense Appellate Division
USCAAF Bar No. 34037

INDEX

ISSUES PRESENTED1

STATEMENT OF STATUTORY JURISDICTION.....2

STATEMENT OF THE CASE2

STATEMENT OF FACTS3

STANDARD OF REVIEW.....9

SUMMARY OF ARGUMENT10

WHETHER APPELLANT’S REQUEST TO CRIMINAL INVESTIGATION COMMAND [CID] THAT HIS CELL PHONE BE RETURNED WAS A WITHDRAWAL OF THE THIRD PARTY CONSENT TO SEARCH GIVEN BY APPELLANT’S WIFE IN APPELLANT’S ABSENCE.11

1. Appellant could revoke the third party consent to search and seize his cell phone originally provided to law enforcement by his wife.11

2. Even if appellant could not revoke the previously given consent to seize his cell phone he could still revoke consent to search the cell phone.....14

3. Appellant revoked his consent to search *and* seizure following his interview with SA Nations by asking for the return of his cell phone.16

4. Once appellant withdrew his consent, CID needed a search authorization or warrant to lawfully search his cell phone.21

5. The military judge’s error in denying the defense motion to suppress materially prejudiced the substantial rights of appellant.23

WHETHER THE ARMY COURT ERRED IN DETERMINING THE APPLICABILITY OF THE INEVITABLE DISCOVERY DOCTRINE

WHERE (1) THE CID AGENTS FAILED TO TAKE ANY STEPS TO OBTAIN A WARRANT AND (2) THE CASE TOOK A “DEAD-END” UNTIL THE WARRANTLESS SEARCH.24

1. Criminal Investigation Command agents failed to take any steps to obtain a search warrant or authorization despite their own internal procedure and guidance.26

2. The investigation took a “dead-end” and the CID agents did not have any parallel investigation that would have inevitably led them to the digital evidence on the cell phone.29

3. The military judge should have applied the exclusionary rule to suppress the evidence obtained through the DFE of appellant’s cell phone.....30

CONCLUSION33

TABLE OF AUTHORITIES

SUPREME COURT OF THE UNITED STATES

<i>Florida v. Jimeno</i> , 500 U.S. 248 (1991)	17, 18
<i>Georgia v. Randolph</i> , 547 U.S. 103 (2006)	12
<i>Mitchell v. Esparza</i> , 540 U.S. 12 (2003)	23
<i>Nix v. Williams</i> , 467 U.S. 431 (1984)	24
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014)	16, 22
<i>United States v. Herring</i> , 555 U.S. 135 (2009)	31
<i>United States v. Matlock</i> , 415 U.S. 164 (1974)	11

COURT OF APPEALS FOR THE ARMED FORCES

<i>United States v. Ayala</i> , 43 M.J. 296 (C.A.A.F. 1995)	10
<i>United States v. Dease</i> , 71 M.J. 116 (C.A.A.F. 2012).....	11, 15
<i>United States v. Hoffman</i> , 75 M.J. 120 (C.A.A.F. 2016).....	12, 13
<i>United States v. Keefauver</i> , 74 M.J. 230 (C.A.A.F. 2015)	25
<i>United States v. Khamsouk</i> , 57 M.J. 282 (C.A.A.F. 2002).....	9
<i>United States v. Kozak</i> , 12 M.J. 389 (C.M.A. 1982)	25
<i>United States v. Maxwell</i> , 45 M.J. 406 (C.A.A.F. 1996).....	25
<i>United States v. Mott</i> , 72 M.J. 319 (C.A.A.F. 2013)	23
<i>United States v. Owens</i> , 51 M.J. 204 (C.A.A.F. 1999).....	24, 25, 26
<i>United States v. Rader</i> , 65 M.J. 30 (C.A.A.F. 2007).....	9
<i>United States v. Rodriguez</i> , 60 M.J. 239 (C.A.A.F. 2004)	10
<i>United States v. Wallace</i> , 66 M.J. 5 (C.A.A.F. 2008).....	passim
<i>United States v. Wicks</i> , 73 M.J. 93 (C.A.A.F. 2014)	15, 25, 30, 31

SERVICE COURTS OF CRIMINAL APPEALS

<i>United States v. Eugene</i> , ARMY 20160438, 2018 CCA LEXIS 106 (A. Ct. Crim. App. February 28, 2018) (mem. op.)	9, 12
<i>United States v. Lutcza</i> , 76 M.J. 698 (A.F. Ct. Crim. App. 2017).....	14

RULES

Mil R. Evid. 314.....	11, 14
Mil. R. Evid. 316.....	14

UNITED STATES CODE

Article 59(a)23

FEDERAL COURTS

United States v. Allen, 159 F.3d 832 (4th Cir. 1998).....30
United States v. Gray, 369 F. 3d 1024 (8th Cir. 2004).....18
United States v. Romero, 692 F. 2d 699 (10th Cir. 1982)25
United States v. Souza, 223 F.3d 1197 (10th Cir. 2000)25

TREATISES

Wayne R. LaFave, SEARCH AND SEIZURE § 8.2(f) 133 (5th ed. 2012).....11

IN THE UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES

UNITED STATES,

Appellee

v.

Private First Class (E-3)
JEFFREY G. EUGENE
United States Army,

Appellant

**FINAL BRIEF ON BEHALF OF
APPELLANT**

USCA Dkt. No. 18-0209/AR

Crim. App. Dkt. No. 20160438

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

ISSUES PRESENTED

I.

**WHETHER APPELLANT’S REQUEST TO
CRIMINAL INVESTIGATION COMMAND [CID]
THAT HIS CELL PHONE BE RETURNED WAS A
WITHDRAWAL OF THE THIRD PARTY
CONSENT TO SEARCH GIVEN BY APPELLANT’S
WIFE IN APPELLANT’S ABSENCE.**

II.

**WHETHER THE ARMY COURT ERRED IN
DETERMINING THE APPLICABILITY OF THE
INEVITABLE DISCOVERY DOCTRINE WHERE
(1) THE CID AGENTS FAILED TO TAKE ANY
STEPS TO OBTAIN A WARRANT AND (2) THE
CASE TOOK A “DEAD-END” UNTIL THE
WARRANTLESS SEARCH.**

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 April 15, 2016, the general court-martial convening authority referred to trial, by general court-martial, two specifications of attempted viewing of child pornography and four specifications of attempted sexual abuse of a child in violation of Article 80, UCMJ, 10 U.S.C. § 880 (2012) which had been preferred against Private First Class (PFC) Jeffery G. Eugene [hereinafter appellant] on March 3, 2016. (JA 018-020).

On May 18, 2016, appellant's trial defense counsel filed a motion to suppress evidence obtained from a digital forensic search of appellant's iPhone 6 [hereinafter cell phone]. (JA 215). On May 25, 2016, a military judge conducted a hearing with respect to the motion to suppress and on May 27, 2016, issued a written ruling denying the defense motion to suppress. (JA 245).

On June 15-16, 2016, appellant was tried at Wheeler Army Airfield, Hawaii, by a military judge-alone general court-martial. Contrary to his pleas, appellant was convicted of the two specifications of attempted viewing of child pornography

and the four specifications of attempted sexual abuse of a child in violation of Article 80, UCMJ, 10 U.S.C. § 880 (2012). The military judge sentenced appellant to be reduced to the grade of E-1, to be confined for 26 months, and to be dishonorably discharged from the service. On October 4, 2016, the convening authority approved the sentence as adjudged.

The Army Court heard argument on January 11, 2018. On February 28, 2018, the Army Court affirmed the findings of guilty and the sentence. Appellant was subsequently notified of the Army Court's decision and, in accordance with Rule 19 of this Court's Rules of Practice and Procedure, appellate defense counsel filed a Petition for Grant of Review on April 27, 2018. On April 30, 2018, this Court granted appellate defense counsel's Motion for Leave to File the Supplement Separately from Petition and on May 17, 2018, the supplement was filed. On June 18, 2018, this Court granted appellant's petition for review.

STATEMENT OF FACTS

On June 1, 2015, appellant went to a field exercise with his unit on Schofield Barracks, Hawaii. (JA 245). He was not allowed to take his cell phone to the field exercise because "an order was given from the battalion commander that [soldiers] couldn't take [their] phones to the field" (JA 128). Appellant gave his cell phone to his wife, Mrs. Briana Eugene. (JA 245).

Later that day, appellant's wife accessed appellant's cell phone, specifically a messaging application called "Kik." (JA 242). In it, she later testified, she saw messages and picture exchanges between appellant and females whom she suspected were under the age of eighteen. (JA 245). Appellant's wife was upset by the content and contacted appellant's platoon sergeant. (JA 246). After sending the platoon sergeant some of the pictures and messages she had seen, she was told to go to the military police station. (JA 246). None of the messages or pictures that appellant's wife saw or sent to the platoon sergeant formed the basis for the charges against appellant. (JA 176-77).

On June 2, 2015, appellant's wife went to the Schofield Barracks Criminal Investigation Command (CID) office, met with Special Agent (SA) Nations, and told him about the content she had seen on appellant's cell phone. (JA 242). She signed a form titled "Consent to Search" and gave consent for CID to search appellant's "APPLE IPHONE." (JA 213).

The "Consent to Search" form did not contain any language that authorized CID to seize the cell phone itself. Instead, the form authorized CID to search for and then seize a specific type of digital content:

I am authorizing the above search(es) for the following general types of property which may be removed by the authorized law enforcement personnel and retained as evidence under the provisions of Army Regulation 195-5, or other applicable laws or regulations: Text, graphics, electronics, mail messages, and other data including

deleted files/folders, containing material related to the sexual exploitation of minors, and/or material depicting apparent or purported minors engaged in sexually explicit conduct.

(JA 213).

Appellant's wife then provided a written sworn statement to SA Nations regarding the images she had viewed on appellant's cell phone. (JA 242). When SA Nations obtained appellant's wife's consent to search the cell phone, he knew that the cell phone belonged to appellant. (JA 246).

On June 2, 2015, after obtaining appellant's wife's consent to search appellant's cell phone, SA Nations put the cell phone on airplane mode pursuant to "standard procedure for CID." (R. at 78). He then conducted a "logical extraction" using CID's "Cellbrite examination device." (JA 091). However, he "did not find anything related to the Kik Messenger Application." (JA 095). The government conceded in the Government Response to Defense Motion to Suppress Evidence that the initial logical extraction "revealed nothing relevant." (JA 237).

On June 5, 2015, appellant went to CID and provided a written sworn statement to SA Nations. In his sworn statement, appellant stated that he had not given anyone authority to access his cell phone. (JA 210). As the military judge found, "[f]ollowing the interview, [appellant] asked SA Nations if he could have his cell phone back. Special Agent Nations refused to return the cell phone to the accused." (JA 247).

Six days later, on June 11, 2015, a “Forensic Laboratory Examination” request was submitted to the digital forensic examiner at the Schofield Barracks CID Office. (JA 194, 224). Some time prior to 12:50 p.m. on June 15, 2015, someone reviewing SA Nation’s investigation file annotated in his Case Activity Summary, “consulting DFE [digital forensic examination] cell, you need to obtain a federal search warrant to get the content associated with the offense.” (JA 244).

On June 15, 2015, SA Nations briefed the trial counsel “on all aspects of this investigation.” (JA 114, 244). When asked by the military judge during the suppression hearing on May 25, 2016, if he was “ever advised to get a search authorization” by the trial counsel, SA Nations responded: “I don’t remember if it was ever brought up.” (JA 122). When the military judge asked again, “You’re not sure if you ever spoke to him about that issue?” SA Nations answered, “Correct.” (JA 123).

On June 15, 2015, SA Nations wrote in the Case Activity Summary in response to the previously annotated instruction to obtain a warrant, “Acknowledged, will submit for IG, as well as coordinate with SAUSA for federal search warrant.” (JA 244). No federal search warrant was ever obtained.

On June 16, 2015, appellant’s investigation was reassigned from SA Nations to SA Tsuno. (JA 096, 244). On the same day, SA Tsuno wrote the following in the Case Activity Summary:

Case file reassigned to SA Tsuno. SA Nations briefed SA Tsuno on the investigation. The investigation requires the following actions:

Draft of DoD IG Subpoena request.

Obtain consent from PFC Eugene to search his cell phone.

(JA 244) (emphasis added).

Sometime after SA Tsuno took over the investigation, he unsuccessfully searched through appellant's cell phone for a lead: "[w]e put the cell phone on a network, and then we went on Kik Messenger app, and basically we looked at each e-mail that PFC Eugene was conversing with." (R. at 202). Special Agent Tsuno then contacted the people whom "PFC Eugene was conversing with." (JA 185). However, the "case took a dead-end" when no one was willing to cooperate. (JA 190). At that point, SA Tsuno talked to his "team chief" and someone named "Zac," and they agreed that they "were going to wait for the DFE examination [sic] to be completed." (JA 190).

"After approximately 5 months in the DFE queue," appellant's cell phone was searched sometime in early November 2015 by SA Ralston, a digital forensic examiner at the Schofield Barracks CID office. (JA 229). Special Agent Ralston was "asked to search for text based communication, images, videos pertaining to possible CP[,] . . . Kik messaging traffic and communications with videos and images." (JA 194). Special Agent Ralston searched appellant's cell phone by conducting a "file system extraction." (JA 195). At the end of this search, SA

Ralston extracted “chat logs . . . from the Kik Messaging artifacts from [appellant’s cell] phone.” (JA 200).

On November 9, 2015, SA Ralston wrote the final report of the forensic examination of appellant’s cell phone. (JA 224). In the report he wrote, “A Consent to Search was authored on 2 Jun 15, by Mrs. Briana N. EUGENE . . . which authorized the exam.” (JA 224).

After the defense had filed its Motion to Suppress Evidence alleging a Fourth Amendment violation, but prior to the suppression hearing, SA Nations conducted another search of appellant’s cell phone, this time in the presence of the trial counsel in the Office of the Staff Judge Advocate. (JA 097, 104). Throughout the entire investigation, the government never obtained a civilian search warrant or a military search authorization to search appellant’s cell phone. As the military judge found, “CID relied upon [appellant’s wife’s] consent alone.” (JA 247).

Copies of conversations on the Kik application that SA Ralston found during the warrantless search of appellant’s cell phone were admitted as Prosecution Exhibit 1. (JA 201). Images that SA Ralston found during the warrantless search of appellant’s cell phone were admitted as Prosecution Exhibit 13. (JA 202-03).

In his written ruling denying the motion to suppress evidence obtained from appellant’s cell phone, the military judge made the legal conclusion that the

“accused’s request for the return of his cell phone on 5 June 2015 does not amount to a request that CID not search his cell phone.” (JA 250). He ruled that:

At most, the accused’s request for the return of his cell phone implicated the seizure of the phone, not the search. “Search” and “seizure” are separate concepts. *Wallace*, 66 M.J. at 8. Revoking consent to one does not revoke consent to the other. *Id.* The accused never told SA Nations not to search the phone. Instead, it appears the accused wanted the phone back, most likely so he could continue to use it. Because the phone had been in CID’s exclusive possession since it was voluntarily given to them by [appellant’s wife] on 2 June 2015, the seizure of the phone was complete and the accused’s request for its return ineffective. *See United States v. Hoffman*, 75 M.J. 120, 124 (CAAF [sic] 2016) (citations omitted) (“A seizure requires law enforcement agents to exercise a fair degree of dominion and control over the property.”).

(JA 250).

The military judge’s ruling neither addressed nor applied the inevitable discovery doctrine. The Army Court, however, opined “that even if appellant had withdrawn consent to search, the inevitable discovery doctrine would apply.”

United States v. Eugene, ARMY 20160438, 2018 CCA LEXIS 106, at *13 (A. Ct. Crim. App. February 28, 2018) (mem. op.).

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

When appellant asked for his cell phone back from law enforcement he effectively communicated that law enforcement no longer had consent to search and seize his cell phone. At the time of the revocation, the searches previously conducted by law enforcement had not revealed any incriminating information. As the reason for the ongoing seizure was no longer based upon consent, law enforcement was required to get a search warrant or search authorization. They did not. As such, the evidence should be suppressed. Furthermore, it would not have been inevitably discovered because law enforcement did not have any parallel investigation that would have revealed the same information and affirmatively documented in their file that they needed to obtain appellant’s consent to search his cellular phone. They took no steps to either obtain his consent or get a warrant. Accordingly, the exclusionary rule applies. Because the contents of the later digital forensic examination constituted the primary evidence against appellant, he was materially prejudiced and his conviction must be set aside.

I.

WHETHER APPELLANT'S REQUEST TO CRIMINAL INVESTIGATION COMMAND [CID] THAT HIS CELL PHONE BE RETURNED WAS A WITHDRAWAL OF THE THIRD PARTY CONSENT TO SEARCH GIVEN BY APPELLANT'S WIFE IN APPELLANT'S ABSENCE.

1. Appellant could revoke the third party consent to search and seize his cell phone originally provided to law enforcement by his wife.

Military Rule of Evidence 314(e)(3) states that consent to search “may be limited in any way by the person granting consent, including limitations in terms of time, place, or property and *may be withdrawn at any time.*” (emphasis added). This Court has clarified that consent to search may be withdrawn at any time, “provided of course that the search has not already been conducted.” *United States v. Dease*, 71 M.J. 116, 120 (C.A.A.F. 2012). “A consent to search is not irrevocable, and thus if a person effectively revokes his prior consent prior to the time the search is completed, then the police may not thereafter search in reliance upon the earlier consent.” Wayne R. LaFare, *SEARCH AND SEIZURE* § 8.2(f) 133 (5th ed. 2012).

Consent to search and seize may be given by a third party, provided both individuals have common authority over the item or place to be searched. “When the prosecution seeks to justify a warrantless search by proof of voluntary consent, it is not limited to proof that consent was given by the defendant, but may show

that permission to search was obtained from a third party who possessed common authority over . . . the premises or effects sought to be inspected.” *United States v. Matlock*, 415 U.S. 164, 171 (1974). However, “a defendant who is physically present may revoke third-party consent to search.” *Georgia v. Randolph*, 547 U.S. 103, 120 (2006). Although appellant was not initially present to revoke consent due to his military duties, he became physically present at the first opportunity upon returning from the field and revoked his consent prior to any inculpatory searches of his phone. Appellant, as the owner of the phone, and now physically present, could revoke the consent to search and seize his property previously given to law enforcement by a third party. The search of the phone that occurred before his revocation is not challenged in this case.

Accordingly, the military judge misapplied *United States v. Hoffman*, 75 M.J. 120 (C.A.A.F. 2016), and Mil. R. Evid. 316 by finding that “the seizure of the phone was complete and [appellant’s] request for its return ineffective” (App. Ex. X, p. 6). The Army Court furthered this erroneous holding on appeal by stating, “[A]ppellant’s 5 June request that his phone be returned was too late to constitute legal withdrawal of consent to seize.” *Eugene*, slip op. at *5. In *Hoffman*, the accused “consented to the search of . . . all items used for storage that are locked and unlocked. He further consented to the removal and retention of any property or papers found during the search which are desired for investigative purposes.”

75 M.J. at 123 (internal quotation marks omitted). However, after noticing “the investigators collecting various digital media,” Hoffman “withdrew his consent while the media were still sitting in his room” and the agents “did not meaningfully interfere with it until they removed it.” *Id.* at 124. This Court found that “[a]s the seizure of the media occurred after Appellant had withdrawn his consent, the seizure violated the Fourth Amendment.” *Id.*

Thus, if consent is withdrawn *before* an item is seized, then a subsequent warrantless seizure of that item *is* a Fourth Amendment violation. However, *Hoffman* does not stand for the inverse proposition: that if consent is withdrawn *after* an item is seized, then the subsequent *continued* seizure and *subsequent* search of the item *is not* a Fourth Amendment violation. To conclude that consent to seize cannot be withdrawn after an item has been seized – as the military judge and Army Court erroneously did in this case – is contradictory to the plain language of Mil. R. Evid. 314 and 316 and this Court’s decision in *Dease* that consent can be withdrawn at any time provided that the search has not occurred.

Under the plain language of the rule, Mil. R. Evid. 316 governs the variety of ways that the government can lawfully seize property. One of those ways is consent. The rule establishes that “[p]roperty or evidence may be seized with consent consistent with the requirements applicable to consensual searches under Mil. R. Evid. 314.” Mil R. Evid. 316(c)(3). Military Rule of Evidence 314

expressly permits limitations upon the consent offered, and expressly states that consent “may be withdrawn at any time.” Mil. R. Evid. 314(e)(3). Just as with consent to search, a plain reading of the rules establishes that consent to an ongoing seizure may also be withdrawn at any time.

This is not to say that return of the item is required. Instead, if law enforcement want to continue seizing the item following a revocation of consent, they must pursue a search warrant or search authorization, which would provide a different basis under Mil. R. Evid. 316 to perpetuate the seizure and make lawful any subsequent search. In this case, the law enforcement agents had “a reasonable belief that the property or evidence is . . . evidence of a crime.” Mil R. Evid. 316(c)(1). Furthermore, if law enforcement had already made copies of the contents of the cell phone during the period in which they actually had consent, they could have retained and searched those copies. *United States v. Lutcza*, 76 M.J. 698, 703 (A.F. Ct. Crim. App. 2017). However, as they had not made any copies and refused to return the phone, changing the basis for the seizure from consent to probable cause seizure has consequences as further discussed *infra*, in sub-section 4.

2. Even if appellant could not revoke the previously given consent to seize his cell phone he could still revoke consent to search the cell phone.

“Whether a search is reasonable depends, in part, on whether the person who is subject to the search has a subjective expectation of privacy in the object

searched and that expectation is objectively reasonable.” *United States v. Wicks*, 73 M.J. 93, 98 (C.A.A.F. 2014). In *United States v. Dease*, appellant originally consented to a urinalysis. *Dease*, 71 M.J. at 119. However, six days later, before his urine sample was shipped to a laboratory, he withdrew his consent. Even though Dease’s urine sample was already seized by the government, this Court held that Dease retained an ongoing privacy interest in his urine sample and therefore could assert his privacy interest by withdrawing his consent to search under Mil. R. Evid. 314. *Id.* at 120-121. In so doing, this Court analogized urine to a computer hard drive: “The evidentiary nature of the urine or blood sample is akin to that of a computer hard drive, whose evidentiary value is unknown until it is examined by forensic experts.” *Id.* This Court clarified that “by allowing the withdrawal of consent,” Mil. R. Evid. 314(e)(3) was protecting a service member’s privacy interest. *Id.* at 121.

The cell phone in this case is the equivalent of the hard drive referenced in *Dease* in that its evidentiary value was unknown until SA Ralston conducted a forensic examination. Like Dease’s privacy interest in his bodily fluid, appellant retained an ongoing privacy interest in his cell phone. Even though SA Nations attempted to search appellant’s cell phone by conducting a “logical extraction” on June 2, 2015, he was not able to find any incriminating evidence. It was not until

CID performed a digital forensic examination of appellant's cell phone in November 2015 that they were successful in locating items of evidentiary value.

As the Supreme Court stated in *Riley v. California*, “[c]ell phones . . . place vast quantity of personal information literally in the hands of individuals.” 134 S. Ct. 2473, 2485 (2014). “With all they contain and all they may reveal, they hold for many Americans the privacies of life.” *Id.* at 2494-95 (citation and internal quotation marks omitted). In fact, “a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house” *Id.* at 2491. Here, appellant continued to retain a privacy interest over the vast amount of information in his cell phone. Like the urine sample in *Dease*, the evidentiary nature of appellant's cell phone was unknown until it was examined by forensic experts in November 2015 – long after June 5. Because appellant retained an ongoing privacy interest in his cell phone, after it was seized by the government on June 2, 2015 but before it was searched in November, he could assert his privacy interest by withdrawing the consent to search under Mil. R. Evid. 314(e)(3).

3. Appellant revoked his consent to search and seizure following his interview with SA Nations by asking for the return of his cell phone.

The standard under the Fourth Amendment for determining the scope of a suspect's consent, including whether consent has been withdrawn, “is that of ‘objective’ reasonableness—what would the typical reasonable person have understood by the exchange between the officer and the suspect?” *United States v.*

Wallace, 66 M.J. 5, 8 (C.A.A.F. 2008) (citing *Florida v. Jimeno*, 500 U.S. 248, 251 (1991)) (internal quotation marks omitted).

Here, the military judge found that appellant “asked if he could have his cell phone back.” (App. Ex. X, p. 3) However, the judge then incorrectly concluded that “the accused’s request for the return of his cell phone on 5 June 2015 does not amount to a request that CID not search his cell phone” and “[a]t most, the accused’s request for the return of his cell phone implicated the seizure of the phone, not the search.” (App. Ex. X, p. 6).

In so doing, the military judge failed to apply the objective reasonableness test from *Wallace*. In *Wallace*, this Court recounted Wallace’s testimony concerning what he told the agents:

[The computer] has our life on it. It has our photo albums on it. It’s got our banking on it. All of our financial stuff is on there. You know, I use it to do all of our bill paying and everything else. Our online business is on there. I was like “You can’t take it.” Then my wife even started going nuts at that time.

Wallace, 66 M.J. at 6. After recounting Wallace’s subjective reason for his objection to law enforcement agents, this Court clearly stated that the scope of a consent “cannot be determined on the basis of the subjective intentions of the consenting party.” *Id.* at 8. Instead, “the standard is that of objective reasonableness – what would the typical reasonable person have understood by the

exchange between the officer and the suspect?” *Id.* (citing *Jimeno*, 500 U.S. at 251) (internal quotation marks omitted).

The military judge’s primary reason for his cursory conclusion that appellant’s request for the return of his cell phone did not amount to a request that CID not search his cell phone was that appellant “never told SA Nations not to search the phone.” (App. Ex. X, p. 6). However, that appellant did not specifically utter the words “do not search” is just one factor in the objective reasonableness analysis, particularly when appellant was not required to use any specific language, legal terminology, or “magic words” like “revocation” or “withdrawal of consent.” *See United States v. Gray*, 369 F. 3d 1024, 1027 (8th Cir. 2004) (“Withdrawal of consent need not be effectuated through particular ‘magic words,’ but an intent to withdraw consent must be made by unequivocal act or statement.”).

Instead of applying the objective reasonableness test from *Wallace*, the military judge relied on his determination that “it appears the accused wanted the phone back, most likely so he could continue to use it.” (App. Ex. X, p. 6). However, as this Court held in *Wallace*, the reason appellant wanted the phone back – his subjective intent – does not determine the scope of the consent. Whatever the reason, “the limitations [of one’s consent or lack of consent] cannot be determined on the basis of the subjective intentions of the consenting party.” *Wallace*, 66 M.J. at 8. This same logic applies to the revoking party. Moreover,

nowhere in Mil. R. Evid. 314 is the reason for appellant's desire to revoke consent relevant to his express ability to revoke. A person can revoke consent for any reason or no reason at all.

At most, appellant's reason for requesting return of his cell phone – if such information was even communicated to SA Nations – is only one factor in determining how the typical reasonable person would have understood by the exchange between SA Nations and appellant. The testimony at the suppression hearing does not indicate that appellant explained to SA Nations why he wanted the phone back. However, even if appellant told SA Nations that he wanted the phone back because he wanted to continue to use it, appellant's statements of subjective intent must be weighed in conjunction with the other factors in this case: SA Nations' knowledge that the phone was appellant's, not appellant's wife's; the fact that appellant was not present when his wife provided the phone to CID because he was in the field; the imbalance of power in that appellant was a Private and as a law enforcement officer SA Nations held a position of authority; and the admissions in the record that CID, including SA Nations, knew they did not have valid consent, as is demonstrated by the annotations in the investigation referencing the need for consent from appellant. (JA 244).

In *Wallace*, the appellant initially provided incriminating statements to law enforcement agents. Subsequently, he “signed a ‘Consent for Search and Seizure’

that clearly gave AFOSI the right to search Appellant's residence and computer and to take away anything they considered evidence of an offense.” *Wallace*, 66 M.J. at 8. He then took the agents to his home and even “led the agents to his computer.” *Id.* at 6. It was not until the agents began to remove the computer that Wallace said to them, “You can’t take it.” *Id.*

Based on the fact that Wallace himself affirmatively consented to both search and seizure, that he led the agents to the computer, and that he did not object until agents began to remove the computer, this Court held that “his pleas to investigators to leave the computer revoked his consent to this particular seizure, but not to the search.” *Id.* Thus a typical reasonable person would conclude that Wallace may not have objected to a search of the computer if the agents had complied with his request and searched the computer at his home without removal.

Unlike in *Wallace*, appellant never consented to either the search or seizure of his cell phone – his wife did in his absence. Appellant also did not lead the CID agents to his cell phone – his wife gave it to them without his permission or consultation. The typical reasonable person observing the exchange between appellant and SA Nations would understand that when appellant asked for his cell phone back at the end of his interview, CID no longer had knowing, intelligent, and voluntary permission to *have* appellant’s phone, that is, to continue the seizure or search. Nor did SA Nations return appellant’s phone and then ask to look at the

messages with appellant. Although revocation of consent to seize can be different from revocation of consent to search, in this case they are the same. One cannot search what one does not have and appellant, unlike Wallace, never consented to the search or seizure of the cell phone in the first place.

Lastly, Wallace was a twenty-six-year-old staff sergeant in the Air Force with nearly eight years of service. Cognizant of these facts, this Court noted that it was still doubtful that Wallace understood the legal concept of consent or withdrawal. *Id.* at 9. Here, appellant was a twenty-two-year-old, recently-enlisted, private first class (E-3), who spoke English as a second language. (JA 204, 214). While it is true that search and seizure are separate legal concepts, the typical reasonable person would not expect appellant to know the legal difference between the two words, especially when the CID agents themselves repeatedly conflated the two terms. (*See* JA 088-116).

In sum, when appellant requested the return of his cell phone, the plain and unequivocal message was that agents return his cell phone and thereby stop any police activities associated with it. The CID agents understood this request as such and recognized the need for either a warrant or subsequent consent from appellant.

4. Once appellant withdrew his consent, CID needed a search authorization or warrant to lawfully search his cell phone.

Once the legal authority for the search and seizure of appellant's cell phone changed from consent to probable cause, CID needed a search authorization or

warrant. Prior to appellant's revocation, the search was ostensibly voluntary,¹ and no warrant or search authorization was required. Mil. R. Evid. 314. However, searches and seizures based upon probable cause, require "a search warrant or search authorization, or under the exigent circumstances described in this rule." Mil. R. Evid. 315(a). As none of the exigent circumstances described in the rule were applicable, CID was required to obtain either a search warrant or a search authorization. They failed to obtain either.

In *Riley*, the Supreme Court's "answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple – get a warrant." *Id.* at 2495. Similarly, this Court's answer to the question of what CID must do before searching a cell phone currently seized based on probable cause should equally as simple – get a warrant or authorization. Even if appellant's request for the return of his cell phone implicated only the seizure of his phone, CID's continued searches of the cell phone based merely on probable cause to seize were unreasonable and violated both the Fourth Amendment and Mil. R. Evid. 315. Thus, the military judge erred in failing to suppress the evidence obtained therefrom.

¹ The voluntariness of the consent was contested at trial but is not part of the granted issue.

5. The military judge's error in denying the defense motion to suppress materially prejudiced the substantial rights of appellant.

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). In this case the error is a violation of the Fourth Amendment, and as such is of constitutional dimension.

“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).

The only substantial evidence supporting appellant's conviction for attempted viewing of child pornography and attempted sexual abuse of a child was the result of an unlawful search, the warrantless digital forensic examination of appellant's cell phone. The government could not have proved its case without Prosecution Exhibits 1 and 13, both of which were gathered as a result of the unlawful search. The evidence directly supporting the charge and its specifications came from the digital forensic examiner's 47-page direct examination about Prosecution Exhibits 1 and 13. (JA 192). None of the pictures or messages that appellant's wife observed on appellant's cell phone formed the basis for charges or specifications against appellant and were not presented by the government as evidence at trial. Therefore the government cannot establish that the admission of

the conversations on the Kik application and images obtained in violation of appellant's Fourth Amendment rights did not contribute to the verdict obtained.

II.

WHETHER THE ARMY COURT ERRED IN DETERMINING THE APPLICABILITY OF THE INEVITABLE DISCOVERY DOCTRINE WHERE (1) THE CID AGENTS FAILED TO TAKE ANY STEPS TO OBTAIN A WARRANT AND (2) THE CASE TOOK A "DEAD-END" UNTIL THE WARRANTLESS SEARCH.

Law and Argument

"The doctrine of inevitable discovery creates an exception to the exclusionary rule allowing admission of evidence that, although obtained improperly, would have been obtained by another lawful means." *Wallace*, 66 M.J. at 10 (citing *Nix v. Williams*, 467 U.S. 431, 444 (1984)). Under the inevitable discovery doctrine, this Court upholds an unlawful search if: (1) "overwhelming probable cause" exists, and (2) "routine police procedure made discovery of the evidence inevitable." *Id.* (citing *United States v. Owens*, 51 M.J. 204, 210-11 (C.A.A.F. 1999)).

Stated differently, for the inevitable discovery doctrine to apply, the government must demonstrate by a preponderance of the evidence that "when the illegality occurred, the government agents possessed, or were actively pursuing, evidence or leads that would have inevitably led to the discovery of the evidence"

in a lawful manner. *Dease*, 71 M.J. at 122 (quoting *United States v. Kozak*, 12 M.J. 389, 394 (C.M.A. 1982)). “[M]ere speculation and conjecture” as to the inevitable discovery of the evidence is not sufficient when applying this exception. *United States v. Maxwell*, 45 M.J. 406, 422 (C.A.A.F. 1996). This exception is only applicable “[w]hen the routine procedures of a law enforcement agency would inevitably find the same evidence.” *Owens*, 51 M.J. at 204.

Moreover, as this Court stressed in *United States v. Keefauver*, “the inevitable discovery doctrine cannot rescue evidence obtained via an unlawful search simply because probable cause existed to obtain a warrant when the government presents no evidence that the police would have obtained a warrant.” 74 M.J. 230, 237 (C.A.A.F. 2015) (citing *Wicks*, 73 M.J. at 103). *See also United States v. Romero*, 692 F. 2d 699, 704 (10th Cir. 1982) (“Under the inevitable discovery exception, unlawfully seized evidence is admissible if there is no doubt that the police would have lawfully discovered the evidence later.”); *United States v. Souza*, 223 F.3d 1197, 1204 (10th Cir. 2000) (“[A] court may apply the inevitable discovery exception only when it has a high level of confidence that the warrant in fact would have been issued and that the specific evidence in question would have been obtained by lawful means.”).

Appellant acknowledges that CID agents had probable cause based on the sworn statements of appellant and appellant’s wife. However, probable cause is

only one of the two required elements of the inevitable discovery doctrine. In addition to having probable cause, the government was required to demonstrate, by a preponderance of the evidence, that the routine procedures of CID would inevitably have led to the same digital evidence. *Owens*, 51 M.J. at 204. Despite testimony that a warrant was routine procedure, CID failed to seek one despite repeatedly recognizing the obligation to do so, and this Court should not have any confidence that the CID agents would inevitably have discovered the digital evidence in a lawful manner because: (1) the agents failed to take any step towards obtaining a search warrant or authorization despite their own internal procedure and guidance; and (2) the investigation reached a “dead-end” and the CID agents did not have any parallel investigation that would have inevitably led to the discovery of the digital evidence on the cell phone.

1. Criminal Investigation Command agents failed to take any steps to obtain a search warrant or authorization despite their own internal procedure and guidance.

The record of trial clearly indicates that the government did not seek to seize and search appellant’s phone through a warrant or search authorization despite having probable cause to do so. Indeed, the record of trial reveals several opportunities to obtain a warrant, search authorization, or renewed consent that were never executed.

First, SA Nations had multiple opportunities to seek a search warrant or search authorization, but he did not. He could have sought one on June 5, 2015, immediately after appellant asked for the return of his cell phone. He could have sought one on June 11, 2015, prior to submitting a request for a full digital forensic search of appellant's cell phone. He could have sought one on June 15, 2015, when he replied "Acknowledged" to an instruction in the Case Activity Summary that SA Nations needed to "obtain a federal search warrant to get the content associated with the offense." (JA 244). He could have sought one either before or after meeting with the trial counsel a few days before the suppression hearing where appellant's Fourth Amendment rights were to be litigated. Despite numerous opportunities to obtain a warrant or search authorization, SA Nations did not take a single step towards obtaining one.

Second, SA Tsuno also had several opportunities to seek a warrant or search authorization, but failed. He could have sought a warrant on June 16, 2015, when the case was reassigned to him and he annotated in the Case Activity Summary: "Obtain consent from PFC Eugene to search his cell phone." At a minimum, he should have attempted to determine whether appellant would consent to a search of his cell phone. Furthermore, by annotating this, he recognized that the previously given consent had been withdrawn and that the government needed a valid basis for further search of appellant's cell phone. He could have, but failed, to seek a

warrant or search authorization prior to conducting another search of appellant's cell phone in July 2015 by "put[ting] the phone on a network, and then . . . [going] on Kik Messenger app, and . . . look[ing] at each e-mail that PFC Eugene was conversing with." (JA 185). Not only did CID agents fail to ultimately obtain a warrant or search authorization, but they also never even started – let alone completed – the appropriate steps to obtain a warrant prior to the digital forensic examination.

Third, the agents failed to seek a warrant or search authorization even though they were briefing and consulting with the trial counsel throughout the investigation. In fact, SA Nations could not even remember "if [the issue of a search authorization] was ever brought up" when he discussed the case with the trial counsel. (JA 122-23). Additionally, when asked by the trial counsel, "Are there times that you also contact commanders for that authorization?" SA Nations responded, "I have never contacted a commander, no." (JA 090).

Fourth, SA Nations' testimony during the suppression hearing lacked credibility. The defense counsel asked SA Nations if appellant "asked for his phone back" on June 5, 2015. (JA 113). Special Agent Nations responded that he could not recall. The military judge found it "quite frustrating and incomprehensible that a trained CID agent would not be able to recall whether such a request was made." (JA 247). Furthermore, SA Nations' eventual testimony that

he would have contacted a military magistrate if he thought he did not have appellant's consent to search, testimony given at a suppression hearing which was triggered by his own failure to obtain a search warrant or authorization, is too self-serving to deserve credibility in light of the prior repeated failures to actually do so.

Simply put, this Court cannot have any confidence that the CID agents actually would have pursued and obtained a warrant based on the agents' numerous opportunities to obtain a warrant or search authorization and their persistent failure to do so.

2. The investigation took a “dead-end” and the CID agents did not have any parallel investigation that would have inevitably led them to the digital evidence on the cell phone.

CID agents would not have inevitably discovered the digital forensic evidence through other lawful investigative means because “the case took a dead-end” and the only way to keep the investigation going was to “wait for the DFE examination [sic] to be completed.” (JA 190). As the trial counsel conceded during the pretrial hearing, the digital forensic examination – which consisted of conducting a file system extraction of the digital files in appellant's cell phone – was what enabled the government “to find a number of message that were stored within the accused's phone that cannot be pulled up simply by pressing the app...” (JA 101).

In sum, where “the [digital forensic] evidence could not have been discovered without a subsequent search, *and* no exception to the warrant requirement applies, *and* no warrant has been obtained, *and* nothing demonstrates that police would have obtained a warrant absent the illegal search, the inevitable discovery doctrine has no place.” *United States v. Allen*, 159 F.3d 832, 841 (4th Cir. 1998) (emphasis in original). To accept that inevitable discovery would rescue the digital forensic evidence obtained via an unlawful search simply because probable cause existed to obtain a warrant when the government presented no evidence that the CID agents would have obtained one would allow the exception to swallow the rule. The Army Court’s application of the inevitable discovery doctrine to this case thus “emasculate[s] the search warrant requirement of the Fourth Amendment.” *Wallace*, 66 M.J. at 11 (Baker, J., concurring in the result) (quoting *Allen*, 159 F.3d at 842) (internal quotation omitted).

3. The military judge should have applied the exclusionary rule to suppress the evidence obtained through the DFE of appellant’s cell phone.

“The exclusionary rule applies only where it results in appreciable deterrence for future Fourth Amendment violations where the benefits of deterrence must outweigh the costs.” *Wicks*, 73 M.J. at 104. (citing *United States v. Herring*, 555 U.S. 135, 141 (2009)) (internal quotation marks omitted). The exclusionary rule “serves to deter deliberate, reckless, or grossly negligent conduct,

or in some circumstances recurring or systemic negligence.” *Herring*, 555 U.S. at 144.

In *Wicks*, this Court applied the exclusionary rule for three reasons: (1) “the Government’s search of Appellant’s cell phone exceeded [his girlfriend’s] private search, (2) “the Government conducted its searches” even while “it consulted the relevant legal office with probable cause in hand” and (3) “the Government ordered the most exhaustive analysis of Appellant’s cell phone during trial while the issue of Appellant’s Fourth Amendment rights was being litigated before the military judge.” *Id.* at 104-105.

This case is analogous to *Wicks*. Here, the government’s search of appellant’s cell phone exceeded his wife’s private search. Also like *Wicks*, the government conducted multiple searches even while it consulted with the trial counsel with probable cause in hand. Additionally, the government continued to repeatedly conduct warrantless searches of appellant’s phone, including immediately leading up to the suppression hearing. In fact, SA Nations conducted a search of appellant’s cell phone with the trial counsel as they were preparing to argue against appellant’s motion alleging a Fourth Amendment violation by conducting the same searches. (JA 97, 104).

There are also numerous additional factors that support exclusion: (1) after appellant requested his cell phone be returned, CID agents were internally directed

to seek a federal search warrant; (2) a CID agent annotated in the case notes that he needed to obtain appellant's consent to search the cell phone; and (3) CID agents faced no risk of evidence tampering or loss while they possessed the cell phone without a warrant or search authorization. Yet, the CID agents repeatedly failed to obtain a warrant or search authorization. The Army Court even noted "while the evidence does not rise to the level of inferring intentional evasion of the warrant requirement by SA GN and SA ST, it is nonetheless concerning." *Eugene*, slip op. at *8. Deterring "concerning" behavior by law enforcement officials is exactly the type of practice that the exclusionary rule is designed to encourage.

The Army Court erred by upholding the illegal search of appellant's cell phone despite these factors. Where no exigency existed, where CID agents repeatedly and systematically ignored their own standard operating procedure, and where CID agents acknowledged but ignored supervisory instruction to obtain a warrant or search authorization or consent, the exclusionary rule is not only appropriate but also necessary to deter their deliberate and reckless disregard of Soldiers' Fourth Amendment rights to be free from unreasonable search and seizure.

CONCLUSION

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



BENJAMIN A. ACCINELLI
Captain, Judge Advocate
Appellate Defense Counsel
Defense Appellate Division
U.S. Army Legal Services Agency
9275 Gunston Road
Fort Belvoir, Virginia 22060
(703) 693-0682
USCAAF Bar No. 36899



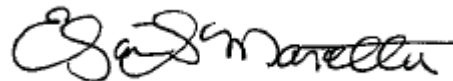
JULIE L. BORCHERS
Major, Judge Advocate
Branch Chief
Defense Appellate Division
USCAAF Bar No. 36843



For DANIEL C. KIM
Captain, Judge Advocate
Appellate Defense Counsel
Defense Appellate Division
USCAAF Bar No. 36754



CHRISTOPHER D. CARRIER
Lieutenant Colonel, Judge Advocate
Chief, Capital & Complex Litigation
Defense Appellate Division
USCAAF Bar No. 32172



ELIZABETH G. MAROTTA
Colonel, Judge Advocate
Division Chief
Defense Appellate Division
USCAAF Bar No. 34037

CERTIFICATE OF COMPLIANCE WITH RULE 24(d)

This brief contains 7,615 words.

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

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 July 18, 2018.



BENJAMIN A. ACCINELLI
Captain, Judge Advocate
Appellate Defense Counsel
Defense Appellate Division
U.S. Army Legal Services Agency
9275 Gunston Road
Fort Belvoir, Virginia 22060
(703) 693-0682
USCAAF Bar No. 36899

CERTIFICATE OF FILING AND SERVICE

I certify that a copy of the forgoing in the case of United States v. Eugene, Crim. App. Dkt. No. 20160438, USCA Dkt. No. 18-0209/AR, was electronically filed with the Court and Government Appellate Division on July 18, 2018.

A handwritten signature in cursive script that reads "Melinda J. Johnson".

MELINDA J. JOHNSON
Paralegal Specialist
Defense Appellate Division
(703) 693-0736