

**IN THE UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES**

UNITED STATES,	)	APPELLANT'S BRIEF IN
<i>Appellant,</i>	)	SUPPORT OF THE ISSUE
	)	CERTIFIED
v.	)	
	)	USCA Dkt. No. _____/AF
Senior Airman (E-4)	)	
AARON M. BUFORD, USAF	)	Crim. App. No. 2013-26
<i>Appellee.</i>	)	

---

**APPELLANT'S BRIEF IN SUPPORT OF THE ISSUE CERTIFIED**

---

THOMAS J. ALFORD, Captain, USAF  
Appellate Government Counsel  
Air Force Legal Operations Agency  
United States Air Force  
1500 W. Perimeter Road, Suite 1190  
Joint Base Andrews NAF, MD 20762  
(240) 612-4813  
Court Bar No. 34441

GERALD R. BRUCE  
Senior Appellate Government Counsel  
Air Force Legal Operations Agency  
United States Air Force  
1500 W. Perimeter Road, Suite 1190  
Joint Base Andrews NAF, MD 20762  
(240) 612-4800  
Court Bar No. 27428

DON CHRISTENSEN, Colonel, USAF  
Chief, Government Trial and  
Appellate Counsel Division  
Air Force Legal Operations Agency  
United States Air Force  
1500 W. Perimeter Road, Suite 1190  
Joint Base Andrews NAF, MD 20762  
(240) 612-4800  
Court Bar No. 35093

**INDEX**

TABLE OF AUTHORITIES ..... iii

ISSUE PRESENTED ..... 1

STATEMENT OF THE CASE ..... 1

STATEMENT OF FACTS ..... 4

SUMMARY OF THE ARGUMENT ..... 11

ARGUMENT ..... 12

**THE MILITARY JUDGE ABUSED HER  
DISCRETION BY GRANTING THE DEFENSE  
MOTION TO SUPPRESS EVIDENCE FROM THE  
DELL LAPTOP, HEWLETT-PACKARD LAPTOP,  
AND CENTON FLASH DRIVE BECAUSE, IN ALL  
INSTANCES, THE EVIDENCE WAS OBTAINED  
LAWFULLY** ..... 12

CONCLUSION ..... 43

CERTIFICATE OF FILING ..... 45

CERTIFICATE OF COMPLIANCE ..... 46

**TABLE OF AUTHORITIES**

**CASES**

**SUPREME COURT CASES**

<u>Coolidge v. New Hampshire,</u> 403 U.S. 443 (1971) .....	19
<u>Herring v. United States,</u> 555 U.S. 136 (2009) .....	40, 41, 42
<u>Hudson v. Michigan,</u> 547 U.S. 586 (2006) .....	40
<u>Illinois v. Gates,</u> 462 U.S. 213 (1983) .....	33, 40
<u>Illinois v. Krull,</u> 480 U.S. 340 (1987) .....	42
<u>Illinois v. Rodriguez,</u> 497 U.S. 177 (1990) .....	24
<u>Murray v. United States,</u> 487 U.S. 533 (1988) .....	27, 28, 34
<u>Nix v. Williams,</u> 467 U.S. 431 (1984) .....	26
<u>Riley v. California,</u> 573 U.S. ____ (2014) .....	39
<u>Skinner v. Railway Labor Executives' Ass'n,</u> 489 U.S. 602 (1989) .....	19
<u>United States v. Calandra,</u> 414 U.S. 338 (1974) .....	40
<u>United States v. Jacobsen,</u> 466 U.S. 109 (1984) .....	passim
<u>United States v. Leon,</u> 468 U.S. 897 (1984) .....	37, 38, 40, 41
<u>United States v. Matlock,</u> 415 U.S. 164 (1974) .....	23

<u>Walter v. United States,</u> 447 U.S. 649 (1980) .....	19, 22
<u>Weeks v. United States,</u> 232 U.S. 383 (1914) .....	40

**COURT OF APPEALS FOR THE ARMED FORCES**

<u>United States v. Ayala,</u> 43 M.J. 296 (C.A.A.F. 1995) .....	13
<u>United States v. Camanga,</u> 38 M.J. 249 (C.M.A. 1993) .....	36
<u>United States v. Chapple,</u> 36 M.J. 410 (C.M.A. 1993) .....	37
<u>United States v. Daniels,</u> 60 M.J. 69 (C.A.A.F. 2004) .....	14, 16, 17
<u>United States v. Dease,</u> 71 M.J. 116 (C.A.A.F. 2012) .....	26, 27
<u>United States v. Dohle,</u> 1 M.J. 223 (C.M.A. 1975) .....	32
<u>United States v. Fogg,</u> 52 M.J. 144 (C.A.A.F. 1999) .....	27, 28, 38
<u>United States v. Hester,</u> 47 M.J. 461 (C.A.A.F. 1998), <i>cert. denied</i> , 525 U.S. 850 (1998) .....	33
<u>United States v. Kozak,</u> 12 M.J. 389 (C.M.A. 1982) .....	26
<u>United States v. Lopez,</u> 35 M.J. 35 (C.M.A. 1992) .....	37
<u>United States v. Macomber,</u> 67 M.J. 214 (C.A.A.F. 2009) .....	34, 24
<u>United States v. McCrary,</u> 39 C.M.R. 104 (C.M.A. 1969) .....	32
<u>United States v. Mix,</u> 35 M.J. 283 (C.M.A. 1992) .....	33

<u>United States v. Owens,</u> 51 M.J. 204 (C.A.A.F. 1999) .....	27
<u>United States v. Portt,</u> 21 M.J. 333 (C.M.A. 1986) .....	passim
<u>United States v. Rader,</u> 65 M.J. 30 (C.A.A.F. 2007) .....	23
<u>United States v. Reister,</u> 44 M.J. 409 (C.A.A.F. 1996) .....	15, 17, 19
<u>United States v. Volante,</u> 16 C.M.R. 263 (C.M.A. 1954) .....	17, 18
<u>United States v. Wallace,</u> 66 M.J. 5 (C.A.A.F. 2008).....	13, 26, 30
<u>United States v. Weston,</u> 67 MJ. 390 (C.A.A.F. 2009) .....	23, 24
<u>United States v. White,</u> 40 M.J. 257 (C.M.A. 1994) .....	24, 25
<u>United States v. Wicks,</u> 73 M.J. 93 (C.A.A.F. 2014).....	passim

**COURTS OF CRIMINAL APPEALS**

<u>United States v. Gallo,</u> 53 M.J. 556 (A.F. Ct. Crim. App. 2000) .....	33, 34
<u>United States v. Turck,</u> 49 C.M.R. 49 (A.F.C.M.R. 1974) .....	32

**STATUTES**

Article 39, UCMJ.....	8
Article 67, UCMJ.....	1
Article 120, UCMJ.....	1
Article 134, UCMJ.....	1, 2
Article 62, UCMJ.....	1

**OTHER AUTHORITIES**

Mil. R. Evid. 311.....	13, 19, 21, 26, 37
Mil. R. Evid. 314.....	14
Mil. R. Evid. 315.....	14, 33
U.S. CONST. amend. IV.....	13

**IN THE UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES**

UNITED STATES, ) APPELLANT'S BRIEF IN  
                  *Appellant,* ) SUPPORT OF THE ISSUE  
                                  ) CERTIFIED  
                  v. )  
                                  ) USCA Dkt. No. \_\_\_\_\_/AF  
Senior Airman (E-4) )  
AARON M. BUFORD, USAF, ) Crim. App. No. 2013-26  
                  *Appellee.* )

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

**ISSUE PRESENTED**

**WHETHER THE MILITARY JUDGE ABUSED HER  
DISCRETION BY SUPPRESSING EVIDENCE FROM THE  
DELL LAPTOP, HEWLETT-PACKARD LAPTOP, AND  
CENTON FLASH DRIVE.**

**STATEMENT OF STATUTORY JURISDICTION**

The Air Force Court of Criminal Appeals (AFCCA) reviewed this case pursuant to Article 62, Uniform Code of Military Justice (UCMJ). This Honorable Court has jurisdiction to review this issue under Article 67(a)(2), UCMJ.

**STATEMENT OF THE CASE**

Appellee is charged with one charge and one specification of committing an indecent act with a minor, in violation of Article 120, UCMJ, and one charge and six specifications relating to receipt, possession (on three separate devices: a Dell laptop, a Hewlett-Packard (HP) laptop, and a Centon flash drive), access, and distribution of child pornography, in violation of Article 134, UCMJ. (J.A. at 25-26.) The charges

and specifications were preferred on 11 July 2013 and referred to a general court-martial on 8 August 2013. (Id.)

On 17 September 2013, Appellee, through his trial defense counsel, filed a motion to suppress evidence of child pornography contained on three electronic devices: The Dell laptop, HP laptop, and Centon flash drive. Appellee alleged that the evidence was obtained in violation of the Fourth Amendment and Appellee's statutory rights under the UCMJ. The government responded on 24 September 2013 by articulating several theories of admissibility for the electronic evidence, and by refuting any alleged constitutional or statutory violations.

On 3 October 2013, general court-martial proceedings began, and a motions hearing commenced on the same day. (J.A. at 28.) On 5 October 2013, the military judge granted the defense motion to suppress, issuing written findings of fact and conclusions of law. (J.A. at 99.) On 7 October 2013, the government filed a motion to reconsider the ruling, and also requested an opportunity to present additional evidence on the motion. (J.A. at 183-90.) On the same day, the military judge allowed the presentation of additional evidence and an evidentiary hearing again commenced. (J.A. at 99.)

On the evening of 7 October 2013, after the reconsideration motion hearing was closed, the military judge denied the



government's motion for reconsideration. (J.A. at 191-95.) The military judge issued written findings of fact and conclusions of law addressing the motion for reconsideration, as well as partly addressing the additional evidence presented by the government. (Id.) In her written findings, the military judge again ordered that "evidence resulting from the search and seizure of the Dell laptop, the HP laptop and the Centon thumb drive [be] suppressed." (Id.)

The government served a notice of appeal on the military judge and trial defense counsel on 8 October 2013. On 4 April 2014, the Air Force Court of Criminal Appeals (AFCCA) ordered that the "Government's appeal is denied as to the suppression of evidence from the Hewlett-Packard (HP) laptop." (J.A. at 9.) AFCCA granted the Government's appeal, however, with respect to the suppression of evidence from the Dell laptop and Centon thumb drive. (Id.) With respect to the HP laptop, AFCCA found that "the probable cause necessary to warrant a search cannot be based on illegally obtained information or evidence" and "the search warrant used for the search" was "based on information obtained by A1C RM's unconstitutional search of the appellee's Facebook and e-mail accounts." (J.A. at 7.) The government moved for reconsideration because the HP laptop contained the evidence necessary to effectively prosecute Appellee. (J.A. at 10.) AFCCA denied the government's motion on 9 May 2014.

## STATEMENT OF FACTS

The misconduct that formed the basis of the charges was first discovered by AB, Appellee's wife. (J.A. at 129-34.) In September 2009, AB found pornographic pictures on her husband's cellular telephone. (Id.) She continued to find pornographic photographs on his phone for several months after the two were married in December 2009. (Id.) AB also started noticing text messages to females on Appellee's cell phone, whereby Appellee would be asking the females to send him nude photographs "so he would be able to cum [ejaculate]." (Id.)

Though AB confronted Appellee several times in an effort to have him stop communicating with these females, Appellee ultimately chose not to halt his exploits (even after AB became pregnant with his child). (Id.) AB also began finding text messages sent by Appellee to underage girls. (Id.) During these conversations, Appellee would again request nude photographs in an effort to help him "cum." (Id.)

In the beginning of March of 2012, AB found a fake Facebook profile belonging to Appellee and using his e-mail address. (Id.) AB knew the profile was fake since it used a pseudonym-- "Brandon Williams"--and contained a photograph of a teenaged male who was clearly not Appellee. (J.A. at 129-34, 173-75.) In addition to the profile itself, AB witnessed several Facebook messages between Appellee, who was posing as "Brandon Williams,"

and several young females. (Id.) One of the young females stated in one of the messages that she was born in 1996. (J.A. at 129-34.) AB then logged into Appellee's e-mail account (the one associated with the fake Facebook profile) and saw several messages from a girl who stated she was 13-years-old and that her friend was 15-years-old. (Id.) AB also saw several pornographic pictures attached to the e-mails, and some of the girls in the photographs appeared to her to be underage. (Id.) AB did not report any of her observations immediately. (Id.)

On or about 17 May 2012, after an argument the day before with Appellee, AB traveled to the nearby residence of her friend, CH. (Id.) AB "came clean" to CH by discussing Appellee's fake Facebook profile, the e-mails she read, and an alleged incident of sexual assault where Appellee engaged in sexual intercourse with AB while she was under the influence of the prescription drug Ambien.<sup>1</sup> (J.A. at 61, 129-34.) While at CH's residence, AB showed CH the fake Facebook account using her own laptop (the Dell laptop) to connect to the internet. (J.A. at 62.) In the process of showing CH the fake Facebook profile, AB became upset. (J.A. at 61.)

---

<sup>1</sup> This allegation was not charged in this case since AB ceased cooperating with the government at some point after her written statement and the search of her residence. (J.A. at 41.) All other charges and specifications relied (at least in part) on the evidence contained on Appellee's HP laptop since the HP laptop included several images of contraband, chat logs, and evidence that could link Appellee to the Centon thumb drive and Dell laptop. AFCCA's decision to exclude that evidence, therefore, prevented the government from proceeding on each of the offenses charged.

(Then) A1C RM,<sup>2</sup> a member of the 48th Security Forces Squadron, who was off-duty at the time, was present at CH's residence and was working on a broken lawnmower with CH's husband. (J.A. at 58, 81, 129-34.) When he was on-duty, A1C RM worked either "gate duty" or vehicle patrols, but at no point had he received training in investigations, nor was he ever assigned to any investigatory duties with the squadron. (J.A. at 58-59, 108-09.)

After smoking cigarettes with CH's husband and helping him repair the family's broken lawnmower in the garage, A1C RM entered their home and quickly noticed AB "emotionally distraught" on the couch with a laptop in her lap. (J.A. at 61, 129-34.) AB showed A1C RM Appellee's fake Facebook profile on her laptop, and A1C RM quickly recognized an e-mail address that matched Appellee's name.<sup>3</sup> (J.A. at 62-63, 129-34.)

AB was initially taking "screenshots" of the Facebook profile and the sexually explicit messages within it, but she stopped because she was too upset, and asked A1C RM to finish taking screenshots of the profile and messages on her behalf. (J.A. at 62-63, 135-38.) A1C RM took the screenshot of Appellee's fake Facebook profile, including the portion of the Facebook account showing Appellee used his e-mail to create the

---

<sup>2</sup> A1C RM eventually separated from the Air Force and is now a college student. (J.A. at 58.)

<sup>3</sup> Both AB and Appellee were acquaintances of A1C RM at this point, and he usually interacted with the two at the CH's residence. (J.A. at 60.)

profile. (Id.) A1C RM also took screenshots of the sexually explicit conversations Appellee shared with at least three different young females. (Id.) According to A1C RM, the females appeared to "look[] underage" based on their own respective Facebook profiles. (J.A. at 64.)

A1C RM asked AB if she had access to the e-mail address that corresponded with Appellee's fake profile. (J.A. at 135-38.) AB answered affirmatively, again took possession of her laptop, and signed into Appellee's e-mail account using a password she knew. (J.A. at 65, 135-38.) After looking through Appellee's e-mail account the same way she had before, AB became upset again and then handed the laptop back to A1C RM. (J.A. at 135-38.) A1C RM began looking through some of the e-mails in the "sent" folder, and noticed "some e-mails that had subject lines with the number 13 and saying things such as '[t]his is 13.'" (J.A. at 65, 135-38.) One of the e-mails in particular, the same e-mail AB had viewed, labeled "13" and "15," had "two photo attachments showing nude females, which one of [sic] looked underdeveloped." (Id.) The photograph attachments were of "fully nude" girls who appeared underage, engaging in "sexually explicit actions." (J.A. at 66, 119.)

A1C RM once again took screenshots of the e-mails he reviewed, which AB requested that he do. (J.A. at 67.) A1C RM then put the screenshots of the e-mails onto a USB flash drive

and gave it to AB. (J.A. at 135-38.) After A1C RM told AB that "it was up to her [what she wanted to do] and it was her decision," AB said "that she wanted to go to [security forces] investigations." (J.A. at 68, 135-38.) A1C RM later testified that, while helping AB come forward, he was doing this as a mere friend, and at no point was he acting on behalf of the government.<sup>4</sup> (J.A. at 31, 43-44, 113.)

Still the same day, 17 May 2012, AB and A1C RM approached MSgt Trumbull, the on-duty security forces flight chief, with the information they had gathered. (J.A. at 69.) Security forces investigations was dispatched to MSgt Trumbull's office, and, once the investigators arrived, they briefly interviewed AB. (J.A. at 70.) Shortly after their interview, the case was referred to AFOSI. (Id.)

The following day, on 18 May 2012, A1C RM drove AB to the AFOSI detachment. (J.A. at 31, 71.) At the detachment, AB consented to the search of her Dell laptop, the flash drive A1C

---

<sup>4</sup> The following exchange took place between trial counsel and A1C RM during the Art. 39(a), UCMJ, hearing concerning the government's motion for reconsideration:

Q: Did you intend to act as law enforcement?

A: No.

Q: Did you believe you were acting as law enforcement?

A: No . . . I was trying to help a friend. It's something that I believe many people would do in the same situation . . . I was acting on my own.

(J.A. at 113.)

RM used to store the screenshots (a PNY brand 1 gigabyte flash drive<sup>5</sup>), and a 1 gigabyte memory card. (J.A. at 53, 142.) AB also provided a written statement to AFOSI. (J.A. at 129-34.) Child pornography was eventually found on the Dell laptop. (J.A. at 152.)

That same day, on 18 May 2012, AFOSI sought search authorization from Col Scott Benza, the 48th Fighter Wing Magistrate. (J.A. at 165.) After hearing the evidence and legal advice, Col Benza determined that there was probable cause that evidence of Appellee's crimes would be present at his residence. (Id.) He authorized a search via an Air Force (AF) Form 1176, which stated that the search and seizure be initiated within three days.<sup>6</sup> (Id.) Col Benza understood the three-day boilerplate time limit to mean that AFOSI had three days to search for and seize the items listed on the form. (J.A. at 100-01.) He did not think that the three days played any role in the time it took to forensically analyze any evidence gathered, such as the digital media in this case, and was well aware that it took several months for the evidence to be sent to the Defense Computer Forensic Laboratory (DCFL), analyzed, and returned. (J.A. at 101-02.)

---

<sup>5</sup> The screenshots stored on the PNY flash drive were ordered sealed in the record by the military judge. This is a different device than the Centon flash drive later obtained by A1C RM. (J.A. at 128.)

<sup>6</sup> This and the other original AF Form 1176s were later corrected for minor errors, which explains the duplicate AF Form 1176s contained within Appellate Exhibit XXV (J.A. at 165-72).

On 18 May 2012, in accordance with the search authorization and with AB's consent, agents with AFOSI began the search at Appellee's residence. (J.A. at 72.) Although AB became upset at some point during the search since she realized that certain electronic devices would be seized for a long period of time, she never revoked her consent. (J.A. at 72.) Various electronic storage devices were seized during this search, including the personal laptop of Appellee (the HP laptop). (J.A. at 49-50, 56.)

On or about 4 June 2012, AB discovered a black flash drive at her residence (the Centon flash drive). (J.A. at 129-34.) She gave it to A1C RM, who plugged it into his own laptop "to review anything on there and to [determine] if it was [applicable] to the case."<sup>7</sup> (Id.) After looking through multiple folders on the drive (which was not password protected and had nothing indicating it was Appellee's), A1C RM came upon sexually explicit photographs of what appeared to be underage individuals, as well as a photograph depicting bestiality. (J.A. at 77.) A1C RM relayed that he did not change, upload, modify, or delete any information from the flash drive at any time before he handed the device over to AFOSI on or about 5 June 2012. (J.A. at 78, 135-38.) AFOSI also seized the laptop

---

<sup>7</sup> A1C RM testified that it was his belief that AB consented to him taking the thumb drive, viewing the contents, and then giving it to AFOSI if there was anything pertinent to the investigation on it. (J.A. at 74-75.)



A1C RM used to view the contents of the flash drive, pursuant to A1C RM's consent. (J.A. at 79.)

On 11 June 2012, all electronic devices seized by AFOSI were packaged and shipped to DCFL for forensic imaging and analysis. (J.A. at 143-64.) The extraction of files started on 9 August 2012 for all electronic devices sent to DCFL. (Id.) Child pornography was found on the Dell laptop, HP laptop, and Centon flash drive. (Id.) The majority of the contraband found (photos and chat logs) was located on Appellee's HP laptop.

#### **SUMMARY OF THE ARGUMENT**

A1C RM, as a private, non-governmental actor, did not violate Appellee's constitutional or statutory rights when he viewed the contents of Appellee's Facebook profile and e-mail account. Additionally, Appellee's wife, AB, previously conducted a private search of Appellee's Facebook profile and e-mail account, which both contained communications with girls under the age of 16. This "search" by AB frustrated Appellee's expectation of privacy in that electronic evidence and, thus, the fruits of any subsequent search can be lawfully used against Appellee at trial.

Furthermore, AB consented to the "search" of her own laptop and to the "search" of Appellee's fake Facebook profile and e-mail account. She possessed both actual and apparent authority to consent. But even if this Court finds the viewing of

Appellee's fake Facebook profile and e-mail account was without consent and in violation of Appellee's rights, the evidence inevitably would have been discovered by the government, and AB served as an independent source as well.

Moreover, even if this Court concludes that A1C RM's initial search was improper, the probable cause supporting the search authorizations was based upon lawful evidence. But, even if this Court concludes that the search authorizations were tainted and based exclusively upon unlawful evidence, the AFOSI agents in this case acted in good faith reliance upon those authorizations, and were not complicit in the initial viewing of Appellee's e-mail and Facebook accounts by A1C RM.

Finally, even if the viewing of Appellee's Facebook and e-mail accounts violated the Fourth Amendment, and subsequent search authorizations were unlawful, the enormous cost of invoking the exclusionary rule under the specific circumstances of this case substantially outweighs the benefit of suppression.

#### ARGUMENT

**THE MILITARY JUDGE ABUSED HER DISCRETION BY GRANTING THE DEFENSE MOTION TO SUPPRESS EVIDENCE FROM THE DELL LAPTOP, HEWLETT-PACKARD LAPTOP, AND CENTON FLASH DRIVE BECAUSE, IN ALL INSTANCES, THE EVIDENCE WAS OBTAINED LAWFULLY.**

### ***Standard of Review***

An appellate court reviews a military judge's evidentiary ruling on a motion to suppress evidence for an abuse of discretion. United States v. Ayala, 43 M.J. 296, 298 (C.A.A.F. 1995); United States v. Wallace, 66 M.J. 5, 7 (C.A.A.F. 2008). As this Court recently stated:

In reviewing a military judge's ruling on a motion to suppress, we review factfinding under the clearly-erroneous standard and conclusions of law under the de novo standard. We apply this standard when reviewing evidentiary rulings under Article 62(b), UCMJ. Therefore, 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. Wicks, 73 M.J. 93, 98 (C.A.A.F. 2014).

### ***Law and Analysis***

The Fourth Amendment provides that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ." U.S. CONST. amend. IV. Military Rule of Evidence (Mil. R. Evid.) 311 states that evidence "obtained as a result of an unlawful search or seizure made by a person acting in a governmental capacity is inadmissible against the accused" if the accused makes 1) a timely objection, and 2) had a reasonable expectation of privacy in the person, place, or property searched, or the accused had a legitimate interest in

the property or evidence seized when challenging a seizure. Mil. R. Evid. 314(a) declares that “[e]vidence obtained from reasonable searches not requiring probable cause conducted pursuant to this rule is admissible at trial when relevant and not otherwise inadmissible under these rules.” Mil. R. Evid. 314(k) further states, “[a] search of a type not otherwise included in this rule and not requiring probable cause under Mil. R. Evid. 315 may be conducted when permissible under the Constitution of the United States as applied to the members of the armed forces.”

**1. A1C RM, as a private, non-governmental actor, did not violate Appellee’s constitutional or statutory rights when he viewed the contents of Appellee’s Facebook profile and e-mail account.**

A private invasion, whether “accidental or deliberate,” “reasonable or unreasonable,” does “not violate the Fourth Amendment because of . . . [its] private character.” United States v. Jacobsen, 466 U.S. 109, 115, (1984). The question of whether a private actor performed as a government agent does not hinge on subjective motivation, but rather on the degree of the government’s participation in the private party’s activities, a question that can only be resolved in light of all circumstances. United States v. Daniels, 60 M.J. 69, 71 (C.A.A.F. 2004) (citing Skinner v. Railway Labor Executives’ Ass’n, 489 U.S. 602, 614-15 (1989)). To implicate the Fourth Amendment in this respect, there must be clear indices of the

government's encouragement, endorsement, and participation in the challenged search. Id.

This Court has held that even when part of a house-sitter's motive was to help investigators by searching an accused's apartment, this fact did not make her an agent of the government because she was also motivated by "her own curiosity and [ ] confused feelings about" the accused. United States v. Reister, 44 M.J. 409, 415 (C.A.A.F. 1996). Additionally, this Court found in United States v. Portt, 21 M.J. 333, 334 (C.M.A. 1986), that the actions of a security forces member, who was performing janitorial duties when he searched an accused's locker, were not the actions of a government official and were thus not attributable to the government.

Here, A1C RM was not acting as an agent of the government. To be sure, when A1C RM visited the CH's residence that day, he did not do so at the direction of security forces or AFOSI. (J.A. at 58-59, 108-09.) He was not acting as a security forces gate guard, or a patrolman, and he certainly was not acting as an investigator, as this is a duty he was never trained to do. (J.A. at 109.) Further, A1C RM was not visiting CH's residence with an expectation that a crime had been committed, nor did he travel there thinking he would end up in the midst of a criminal investigation. (J.A. at 61, 95, 113.) In fact, it is clear exactly why A1C RM was present at CH's residence on 17 May 2012:

He was visiting his friends so that he could assist them in repairing their broken lawnmower. (J.A. at 61.) Much like the security forces Airman in Portt, A1C RM was performing an altogether different "duty" than his typical duty as a security forces member--in his own words, he was merely present there as a friend (and, ostensibly, as a lawnmower repairman). (J.A. at 113.)

Once AB voluntarily made A1C RM aware of the Facebook profile and of her access to Appellee's e-mail account, this act did not suddenly transform A1C RM into an agent of the government merely because he was a security forces member. As this Court made clear in Daniels, there must be clear indices of the government's encouragement, endorsement, and participation in a search. Daniels, 60 M.J. at 71. That did not occur here. Although A1C RM instinctively believed he should preserve the evidence of Appellee's crimes, and AB may have approached him knowing he was a member of security forces, A1C RM's subjective motivations and AB's intentions do not matter. Id. ("the question of whether a private actor performed as a government agent does not hinge on motivation."). Thus, unlike the roommate in Daniels, who was directed to retrieve cocaine from that accused by a superior, A1C RM was not acting at the behest of any government authority.

Moreover, A1C RM's actions did not go, as the military judge found, "far and beyond those expected of a private citizen" when he began perusing Appellee's Facebook profile and e-mail account. Again, in his words, he was "trying to help a friend." (J.A. at 113.) And when asked whether he thought he was acting on behalf of law enforcement, A1C RM testified, unequivocally, that he was acting on his own. (Id.) It is glaringly apparent in the record that A1C RM was not even sure what to do after he viewed the evidence of Appellee's crimes. (J.A. at 68.) And A1C RM even left the decision of what to do up to AB, who, on her own volition, decided that she wanted to go to security forces investigations--a fact that also shows AFOSI would have learned of Appellee's nefarious activities completely independent of A1C RM's "search" or actions.<sup>8</sup> (Id.)

The military judge completely ignored Jacobsen, Reister, Portt, and Daniels in her analysis, and instead appeared to rest her decision that A1C RM was a government actor entirely on a brief passage from the 1954 case of United States v. Volante, 16 C.M.R. 263 (C.M.A. 1954): "[A] search by a person duly assigned to law enforcement duty and made for the sole purpose of enforcing military law, is conducted by a person acting under the authority of the United States." Id. at 266 (emphasis

---

<sup>8</sup> If A1C RM was indeed acting as a government agent, he would have had an independent duty to report Appellee's crimes, not simply to leave it up to Appellee's wife.

added). But, in viewing the facts of Volante, even that Court ultimately found that the individuals in that case were acting in a private capacity because neither of them had “any official sanction for [their] action[s].” Id. at 267. Though there was some encouragement from their command to conduct the search in that case, the “sole” purpose of their search was not the enforcement of military law. Therefore, the search was lawful.

Here, the facts are similar: A1C RM was never ordered by anyone in a position of authority to search AB’s laptop (the Dell laptop), Appellee’s Facebook profile, or Appellee’s e-mail account. And even after the investigation began, A1C RM’s cursory “search” of Appellee’s flash drive (the Centon flash drive), was done in his capacity as a private citizen (after collecting his statement, there is no evidence whatsoever AFOSI directed A1C RM to be involved in the investigation against Appellee). Therefore, this Court should easily find that A1C RM was a private, non-governmental actor, and any “search” he conducted cannot be attributed to the government.

**2. AB’s private search of Appellee’s Facebook profile and e-mail account, which contained communications with girls under the age of 16, frustrated Appellee’s expectation of privacy in that evidence.**

The Fourth Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the government or those acting at their



direction. Skinner, 489 U.S. at 613-14. The Supreme Court has consistently construed the protections provided by the Fourth Amendment as proscribing only governmental action; it is wholly inapplicable "to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official." Jacobsen, 466 U.S. at 113 (citation omitted); Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971); see also Reister, 44 M.J. at 415-16. Again, Mil. R. Evid. 311(a) directs that the exclusionary rule for unlawful searches applies only to searches made by someone "acting in a governmental capacity." Hence, the Fourth Amendment and the exclusionary rule are not implicated by a private search. Reister, 44 M.J. at 415.

"Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information . . . ." Jacobsen, 466 U.S. at 117 (emphasis added). Additional invasions of privacy in the seized evidence by the government agent must be tested by the degree to which they exceeded the scope of the private search. Wicks, 73 M.J. at 100 (citing Jacobsen, 466 U.S. at 115); see also Walter v. United States, 447 U.S. 649 (1980); Reister, 44 M.J. at 415-16; Portt, 21 M.J. at 334 (after an Airman opened a locker in his private capacity and summoned AFOSI after finding

evidence of drug use, "subsequent opening of the locker was simply a continuation of that entry.")

The record demonstrates that on at least two occasions AB viewed the contents of Appellee's Facebook profile and corresponding e-mail account. (J.A. at 129-34.) Though AB did not testify at the motions hearings, her AF Form 1168, dated 18 May 2012 was before the military judge. (Id.) The military judge almost completely omitted the fact that AB conducted at least two of her own private "searches." (J.A. at 176.) ("[AB] stated that she became curious and logged onto his email account just to see what was going on."). The military judge neglected to recognize the very important fact that AB extensively viewed the contents of both Appellee's Facebook messages and his e-mail account. (J.A. at 129-34.) And it is undisputed that AB was not acting at the behest of any law enforcement or government agency when she took these steps in the context of her personal, marital relationship with Appellee.

AB's "search" of Appellee's fake Facebook account and e-mail account frustrated any expectation of privacy that he previously held in these messages. When viewing these messages, she undoubtedly observed "pornographic images . . . [s]ome looked to be of age [and] some looked to be underage." (Id.) In her sworn statement, she explicitly recalled viewing e-mail and Facebook messages: "I began to find pictures/instant

messages to and from of age and underage females. The messages typically asked their age and if they had a nude photo they could send." (Id.) She went on to state that Appellee had "several sent messages from a girl who said she was 13 and her friend was 15." (Id.) Applying the rationale from Jacobsen and Wicks, even assuming AlC RM was acting as a government agent, he was permitted to view these Facebook and e-mail messages to the same extent AB viewed them.

Under Mil. R. Evid. 311(a)(2), a search within the context of the Fourth Amendment only occurs when a person maintains an expectation of privacy in the item to be searched. After AB's searches, Appellee had no expectation of privacy in his fake Facebook account (and messages), nor did he have a remaining expectation of privacy in his e-mail. It is also interesting that AB had full access to both the fake Facebook profile and e-mail. Indeed, if Appellee gave AB his passwords or if they were readily available, this is even more of an indication that he had no reasonable expectation of privacy in these accounts. Unfortunately, the record is silent as to this fact since AB ceased cooperation with the prosecution. But, even if Appellee did not knowingly provide his passwords to his wife, this "search" still does not implicate the Fourth Amendment because the search was carried out by a wholly private citizen.

Additionally, unlike the law enforcement officer in Wicks, whose search exceeded the scope of the private actor in that case, A1C RM's "search" and "screenshotting" of the Facebook and e-mail messages, done at the behest of AB, did not exceed the scope of AB's "searches." A1C RM stated the following:

In the sent folder [of Appellee's e-mail account] there were some emails that had subject lines with the number 13 and saying things such as 'this is 13.' In other sent emails, which piggy-backed on the previously received emails, there were nude pictures and sexually explicit actions photographed. One email in particular mentioned that the first picture was 13 and the other was 15.

(J.A. at 137-38.) A1C RM's "search," done at the behest of AB, covers the exact same material and does not exceed the scope of AB's initial search of her husband's Facebook profile and e-mail account. (*Compare* J.A. at 132-33, with J.A. at 137-38.)

Therefore, the military judge abused her discretion when she found the government committed an unlawful search of Appellee's Facebook and e-mail accounts, and she compounded this error by completely failing to analyze AB's frustration of Appellee's reasonable expectation under Walter, Jacobsen, and Portt.

**3. AB consented to the "search" of her laptop and to the "search" of Appellee's fake Facebook profile and e-mail account. She possessed both actual and apparent authority to consent.**

There is no dispute in this case that AB had the authority to consent to her own Dell laptop being searched. (J.A. at 192.) ("[AB] gave [A1C RM] consent to search the Dell laptop

when she handed it to him on or about 17 May 2013. However, the Court finds that consent to search did not extend to the Facebook profile or email account of the accused.”). By not recognizing AB’s common authority to consent to the search of the Facebook profile and e-mail account, however, the military judge abused her discretion.

Consent to a warrantless search by one who possesses common authority or other sufficient relationship to the premises or effect sought to be inspected is valid as against an absent, non-consenting person with whom that authority is shared.

United States v. Matlock, 415 U.S. 164, 170-71 (1974).

Voluntary consent to search may be obtained from the person whose property is to be searched or from a person who shares common authority over the property. United States v. Weston, 67 M.J. 390, 392 (C.A.A.F. 2009) (citing Matlock, 415 U.S. at 171.)

Further, common authority over a home extends to all items within the home, unless the item reasonably appears to be within the exclusive domain of the third party. Id. (citing United States v. Gallagher, 66 M.J. 250, 253 (C.A.A.F. 2008) (holding that an unlocked briefcase located within an attached garage, which had been converted into a den, fell within the common authority of Appellant’s wife)).

In United States v. Rader, 65 M.J. 30 (C.A.A.F. 2007), this Court found that a roommate with shared access to another’s

computer has common authority over the computer and can grant consent. In addition, this Court also found, in accordance with Illinois v. Rodriguez, 497 U.S. 177, 188 (1990), that a search may be reasonable even though the person purporting to give consent lacks actual authority to consent, if the facts known to the government when the purported consent is given would warrant a man of reasonable caution to believe that the consenting party had authority over the premises. United States v. White, 40 M.J. 257, 258 (C.M.A. 1994).

The case at bar is similar to the facts of Weston, where the spouse in that case consented to the search of the house and seizure of her accused husband's computers. Weston, 67 M.J. at 393. In Weston, however, unlike here, the spouse revoked the consent to search. Agents in Weston were allowed to take with them the computer they had seized prior to the revocation of consent; they then searched the computer and discovered child pornography. This is similar to the viewing of Appellee's Facebook and e-mail accounts in this case, except, here, as stated above, AB never revoked consent. And it certainly reasonably appeared to A1C RM that AB had consent to give, since she had access to both the Facebook and e-mail accounts. See White, 40 M.J. at 258.

AB directed A1C RM to view Appellee's Facebook profile. (J.A. at 62-63.) She also asked him to take screenshots of the

contraband material she had previously viewed (and was viewing at the time of the consent). (Id.) When A1C RM asked for the password for the e-mail account, AB not only had the password, but she typed it into the computer readily. (J.A. at 65.) All indications are that AB had both actual and apparent authority to consent to the search of the accounts. So, even if A1C RM was acting as a government agent (and the government does not concede this point in the slightest), AB consented to the search of Appellee's accounts. And even assuming, *arguendo*, she did not have the authority to consent, a man of reasonable caution would believe that AB had authority over the fake Facebook and e-mail accounts. White, 40 M.J. at 259. This argument, by extension, applies with equal force to the search of the Centon flash drive: When AB gave the non-password-protected flash drive to A1C RM, she not only had authority to consent to the search of its unprotected contents (it was found in her home), but, from A1C RM's perspective, it appeared she had the ability to consent to the search of the flash drive as well.

Further, there is no dispute AB could consent to the search of her own Dell laptop and to the search of her home (and the items within her home). In fact, AB gave written consent to search her own laptop, which contained child pornography linked to Appellee according to the DCFL report. Appellee thus has absolutely no standing to contest the search of AB's Dell

laptop, and the military judge's arbitrary and capricious finding that Appellee does have standing to challenge its search underscores her abuse of discretion in this case.

AB consented to the search of her Dell laptop, the Centon flash drive, and the search of her home, which then caused AFOSI to properly search and seize Appellee's HP laptop pursuant to a search authorization. She also consented to A1C RM viewing the contents of Appellee's Facebook profile and e-mail account. Because AB clearly had access to her husband's Facebook and e-mail accounts, A1C RM was reasonable in his belief that AB had common authority over the accounts when he viewed them. Therefore, the military judge patently abused her discretion when she excluded evidence from all three electronic devices.

**4. Even if this Court finds the viewing of the fake Facebook profile and e-mail account violated the Fourth Amendment, the evidence inevitably would have been discovered by the government and AB served as an independent source for the evidence as well.**

Evidence obtained as a result of an unlawful search or seizure made by a person acting in a governmental capacity is admissible against the accused if the evidence would have been obtained even if such unlawful search or seizure had not been made. See Mil. R. Evid. 311(b)(2). This exception to the exclusionary rule is consistent with controlling case law. Nix v. Williams, 467 U.S. 431, 441 (1984); United States v. Kozak, 12 M.J. 389, 391-94 (C.M.A. 1982); United States v. Wallace, 66



M.J. 5, 7-10 (C.A.A.F. 2008); United States v. Dease, 71 M.J. 116, 121-22 (C.A.A.F. 2012); United States v. Owens, 51 M.J. 204, 211 (C.A.A.F. 1999).

This Court has upheld the legality of a warrantless search of an appellant's car and seizure of stolen stereo equipment because overwhelming probable cause and routine police procedure made discovery of the evidence inevitable. See Owens, 54 M.J. at 210-11. This standard was affirmed by this Court in Dease, where the majority in that case found that no probable cause existed to search the appellant's urine for the presence of drugs, nor had the government engaged in any parallel investigation that would lead to the discovery of the evidence. Dease, 71 M.J. at 121-22 (citing to Wallace and Owens for the proposition that a warrantless search should be upheld when overwhelming probable cause exists combined with the likelihood that routine police procedure would have made the discovery of the evidence inevitable).

Under the independent source doctrine, which is related to, but not the same as, the inevitable discovery doctrine, evidence initially discovered during an unlawful search, but later obtained independently through activities untainted by the illegality, may be admitted into evidence. Murray v. United States, 487 U.S. 533, 537 (1988); see also United States v. Fogg, 52 M.J. 144 (C.A.A.F. 1999). The independent source

doctrine balances two competing interests: “[T]he interests of society in deterring unlawful police conduct and the public interest in having juries receive all probative evidence of a crime.” Id. (quoting Nix v. Williams, 467 U.S. 431, 443 (1984)).

The overriding principle of the doctrine is to “put [] the police in the same, not a worse, position than they would have been in if no police error or misconduct had occurred.” Id. To establish that the independent source doctrine applies to evidence seized pursuant to a warrant obtained after an unlawful search, the government must show that the decision to seek the warrant was independent of the unlawful entry (*i.e.*, that police would have sought the warrant even if the initial entry had not occurred), and that the information obtained through the unlawful entry did not affect the magistrate’s decision to issue the warrant. Murray, 487 U.S. at 547.

In this case, the military judge abused her discretion by holding that the inevitable discovery and independent source doctrines were inapplicable. First, with regard to inevitable discovery, it is clear AB was hell-bent on making Appellee’s activities known after her fight with him on or about 16 May 2012. (J.A. at 129-34.) She purposely showed the Facebook profile and e-mail account to CH and A1C RM, who she knew to be a member of security forces. (Id.) While A1C RM may have

encouraged AB to go to security forces, it is clear based on the testimony that it was her choice, and that she was ultimately the one who decided to move the case forward. (J.A. at 68.) Further, AB finally "came clean" that she had been sexually assaulted and had decided that she wanted to report the incident the same day A1C RM conducted his private-actor "search." (J.A. at 129-34.) Based solely on AB's AF Form 1168, it is highly likely, far beyond a preponderance of the evidence standard, that AFOSI would have initiated a search of Appellee's residence, and would have still inevitably found Appellee's HP laptop. In fact, AFOSI did not even view the "screenshots" of Appellee's Facebook and e-mail accounts until after the DCFL analysis and well after they had received search authority:

TC: Do you remember whether or not you were actually personally able to view the screenshots made by [AB] and [A1C RM]?

SA Carag: Not initially, not until after we received a hard drive from DCFL.

TC: Okay; but you didn't actually go into what they had provided you; correct?

SA Carag: No, sir.

(J.A. at 45.)

Moreover, when AB found the Centon flash drive, A1C RM would still have turned the flash drive over to AFOSI absent his cursory "search" since that is precisely what AB directed him to do. (J.A. at 74-75.) ("I said I would probably take a look at

it to see if there was any evidence on it before turning it over to OSI.”) And, as regards AB’s own laptop, there is no doubt she still would have consented to any search at the same time she relayed Appellee’s crimes to AFOSI. (J.A. at 129-34.) Based on that consent, AFOSI would have developed separate probable cause to search Appellee’s residence because of the child pornography eventually found on her laptop--a laptop frequently used by Appellee.

In Wallace, this Court found that the images of child pornography on the appellant’s computer would have been inevitably discovered based on the overwhelming probable cause provided by appellant in his statement. Wallace, 66 M.J. at 10. Like Wallace, there was overwhelming probable cause to search the Buford residence, as well as the electronic devices seized and sent to DCFL, because of AB’s statements to law enforcement. The military judge seemed to think that merely because AB did not immediately report Appellee’s misconduct means that she would not have followed through absent A1C RM’s “search.” This defies the facts in the record and all common sense. AB, in her own words, had finally had enough and had conclusively decided to “come clean.” (J.A. at 129-34.) On 17 May 2012, she was telling anyone who would listen, including a security forces friend, and, eventually, AFOSI, that Appellee sexually assaulted her and possessed several images of child pornography.

Therefore, the military judge once again clearly abused her discretion when she twice found that the government did not establish that the evidence would have been inevitably discovered.

Further, under the independent source doctrine, this Court should conclude that AFOSI would have obtained a search authorization despite A1C RM's alleged "search." The decision in this case to seek a search authorization by AFOSI was completely independent of A1C RM taking "screenshots" of Appellee's Facebook profile and e-mail account. Absent that "screenshot" evidence, the government arguably had even better evidence: AB herself. She witnessed first-hand the messages in Appellee's e-mail and Facebook account, and she gave AFOSI a detailed description of what she observed (completely absent from any of A1C RM's actions). (J.A. at 129-34.) This is what the magistrate based his decision on as evidenced by the following exchange during the motions hearing:

TC: Can you recall generally what the basis for your search authorization, the beginning of this case on the 17th and 18th of May, what that would have been sir? Do you have any factual recollection of what the factual basis was for your granting of probable cause?

Col Benza: Well, what I remember on this case was that the alleged member's spouse reported some concerns about her husband's involvement in some type of child pornography type activity. And that's

really the extent of it without reading the affidavit over again.

(J.A. at 102-03.)

Thus, under the independent source doctrine, the HP and Dell laptops should without a doubt be admissible.

**5. Even if A1C RM's initial search was unlawful, the probable cause supporting the search authorization for the HP laptop was based upon lawful evidence.**

AFCCA concluded that Appellee's HP laptop should be suppressed because the "probable cause necessary to warrant a search cannot be based on illegally obtained information or evidence." (J.A. at 7.) (citing United States v. Turck, 49 C.M.R. 49, 51 (A.F.C.M.R. 1974)). But, the holding in Turck originated from the "old" Military Rules of Evidence,<sup>9</sup> contained within the 1969 edition of the Manual for Courts-Martial (MCM):

[I]f a search is unlawful because [it is] conducted without probable cause and a second search is conducted based on information supplying probable cause discovered during the first search, evidence obtained by the second search is inadmissible against an accused . . . even if the second search would otherwise be lawful.

MCM chapter XXVII, para. 152 (1969 ed.). This rule, contained within the 1969 edition of the MCM, pre-dated several important

---

<sup>9</sup> United States v. Turck, 49 C.M.R. 49 (A.F.C.M.R. 1974), cites to the 1969 edition of the MCM to support this rule, as well as United States v. McCrary, 39 C.M.R. 104 (C.M.A. 1969). McCrary was abrogated on different grounds by United States v. Dohle, 1 M.J. 223 (C.M.A. 1975).

CAAF and Supreme Court precedents in the area of search and seizure law.

The current state of the law is that probable cause exists when there is sufficient information to provide the authorizing official a reasonable belief that the person, property, or evidence sought is located in the place or on the person to be searched. Mil. R. Evid. 315(f); United States v. Mix, 35 M.J. 283 (C.M.A. 1992). Whether probable cause exists for a magistrate to issue an authorization to search is determined by the totality of the circumstances presented to the magistrate. Illinois v. Gates, 462 U.S. 213, 233 (1983); accord United States v. Hester, 47 M.J. 461, 463 (C.A.A.F. 1998), cert. denied, 525 U.S. 850 (1998).

In Gates, the Supreme Court emphasized the fact that the law does not demand that a magistrate make technical, legal determinations when deciding whether to issue a warrant. See Gates, 462 U.S. at 231. Instead, only a practical, common sense assessment is required, because the central question is whether there is probable cause, not whether there is proof beyond a reasonable doubt. Id. Searches authorized by magistrates are preferable to searches conducted under other bases. United States v. Gallo, 53 M.J. 556, 561 (A.F. Ct. Crim. App. 2000). Consequently, a magistrate's determination that probable cause existed is entitled to great deference. Id. (citing United

States v. Leon, 468 U.S. 897, 914 (1984)). This Court has interpreted the Supreme Court's guidance to require that resolution of doubtful or marginal cases should be largely determined by the preference for warrants and that "[c]lose calls will be resolved in favor of sustaining the magistrate's decision." United States v. Macomber, 67 M.J. 214, 218 (C.A.A.F. 2009)(citations omitted).

Whenever an affidavit in support of an application for a search authorization or warrant contains both admissible and inadmissible information, the affidavit is tested for sufficiency solely on the basis of the admissible information. Gallo, 53 M.J. at 562 (citing United States v. Camanga, 38 M.J. 249 (C.M.A. 1993)). If the remaining information is sufficient to establish probable cause, it is deemed to be from an independent source. Id. This approach follows the rationale of Murray v. United States, 487 U.S. 533 (1988), where the Supreme Court noted, "while the Government should not profit from its illegal activity, neither should it be placed in a worse position than it would otherwise have occupied."

In this case, the search authorization allowing AFOSI agents to seize electronic media from Appellee's residence was based on legally sufficient probable cause. On 18 May 2012, AFOSI sought search authorization from Col Scott Benza, the 48th Fighter Wing Magistrate, based on AB's written report. (J.A. at



129-34, 165-67.) After hearing the evidence and legal advice, Col Benza determined that there was probable cause that evidence of Appellee's crimes would be present at his residence. (Id.) He authorized a search via the Air Force (AF) Form 1176. (Id.) The relevant search authorization permitted the seizure of "[e]lectronic media to include Government Assigned or personal computers; government blackberry/mobile; personnel phones[;] Personal media storage devices and peripheral devices. Documents containing Screen/Usernames, passwords. Any child pornography images/pictures." (J.A. at 167.)

On 18 May 2012, in accordance with the search authorizations and with AB's consent, AFOSI agents began the search at Appellee's residence. (J.A. at 72.) Although AB became upset at some point during the search since she realized that certain electronic devices would be seized for a long period of time, she never expressly revoked her consent. (J.A. at 75.) Various electronic storage devices were seized during this search, including the personal laptop of Appellee (the HP laptop). (J.A. at 49-50, 56.)

The decision in this case to seek a search authorization by AFOSI was independent of A1C RM's search or his "screenshots" of Appellee's Facebook profile and e-mail account. As stated above, the government had even better proof than this "screenshot" evidence: AB's oral and written statements. In

March 2012, AB witnessed first-hand the messages in Appellee's e-mail and Facebook account, and she gave AFOSI a detailed description of what she observed. This was completely independent and separate from any of A1C RM's actions. The following excerpt is from her written to report to AFOSI on 18 May 2012:

In the beginning of March [2012] was when I found the fake facebook [sic] account. The name and photo are not him. The email address is his valid email account that he uses for everything. The messages in the fake facebook asked how old the girls were, if they wanted to skype, if they could send pictures to help make him cum. The one I remember most clearly was the young girl that he was speaking to. The girl was born in 1996. That's gross. I logged into his email account just to see what was going on. He had several sent messages from a girl who said she was 13 and her friend was 15 . . . the picture folder in his email was filled with pornographic images. Some looked to be of age. Some looked to be under age.

(J.A. at 129-34.)

AB reported Appellee's crimes voluntarily. (J.A. at 68.) She was not forced to do so by A1C RM. (Id.) And the search authority, Col Benza, testified that he based probable cause in large part on AB's statement. (J.A. at 102-03.) Applying Camanga to these facts, it is clear that there was sufficient probable cause to issue the search authorization based only on what AB had witnessed. See Camanga, 38 M.J. at 252 ("if the remaining information is sufficient to establish probable cause,

it is deemed to be from an independent source."). While it is not fully clear in the record whether the magistrate was influenced at all by A1C RM's search (it appears not), assuming, *arguendo*, the magistrate was exposed to information from that search, the search was still proper based on AB's independent observations. Therefore, evidence contained on the HP laptop is admissible at trial.

**6. Even if this Court finds that the search authorizations were based upon unlawful evidence, the AFOSI agents in this case acted in good faith reliance upon the search authorizations.**

The military judge altogether failed to analyze whether the AFOSI agents acted in good faith reliance upon the search authorization in this case. Mil. R. Evid. 311(b)(3), otherwise known as the "good faith exception" to the warrant requirement, originally derived from United States v. Leon, 468 U.S. 897 (1984), would permit the admission at trial of Appellee's HP laptop and the Centon thumb drive. See also United States v. Chapple, 36 M.J. 410 (C.M.A. 1993); United States v. Lopez, 35 M.J. 35 (C.M.A. 1992). Evidence obtained as a result of an unlawful search may be used if "officials seeking and executing [an] authorization [] reasonably and with good faith" relied on the authorization. Mil. R. Evid. 311(b)(3). The good faith exception will not apply if the information in the affidavit is false or provided recklessly, nor will it apply when the officers' search is not reasonably limited to "only those places

and for those objects that it was reasonable to believe were covered by the warrant." United States v. Fogg, 52 M.J. 144, 151 (C.A.A.F. 1999)(citing Leon, 468 U.S. at 914).

Here, the AFOSI agents never directed A1C RM to conduct the initial "search." In fact, due to A1C RM's continuing interference with the investigation, he was given an order not to contact AB. (J.A. at 94.) Thus, even if A1C RM was acting as an agent of the government (and the United States continues to insist that he was not an agent at the time of his "search"), A1C RM was acting without the approval or encouragement from law enforcement--specifically, AFOSI.

The good faith exception should also apply here because there is zero evidence that the agents provided Col Benza, the magistrate, with false or "reckless" information. See Leon, 468 U.S. at 914. Nor was there evidence provided to show that the agents exceeded the scope of the search authorization. Id. Simply put, when AFOSI agents do the right thing and obtain several search authorizations out of an abundance of caution, even though AB consented to the search of her home, the drastic judicially created remedy of exclusion should not apply.

By seeking a search authorization, the AFOSI agents interjected an orderly procedure by a neutral and detached magistrate who determined what actions could be taken. Fogg, 52 M.J. at 151 ("The officers were not trying to ignore or subvert

the Fourth Amendment . . . they were protecting the right to privacy by obtaining a search warrant, rather than making a warrantless entry." ). In short, these agents should not be penalized for seeking a search authorization. In fact, this Court and the Supreme Court have recently commanded that this is exactly the right course of action whenever there is any doubt. See, e.g., Wicks, 73 M.J. at 103 ("the Government made no effort to secure a warrant . . ."); Riley v. California, 573 U.S. \_\_\_\_ (2014)("get a warrant"). Therefore, even if the search authorization was not supported by sufficient probable cause, Appellee's HP laptop and the Centon thumb drive should be admitted.

**7. Even if the viewing of Appellee's Facebook and e-mail accounts violated the Fourth Amendment, the enormous cost of invoking the exclusionary rule under the specific circumstances of this case substantially outweighs the benefit of suppression.**

The military judge abused her discretion when she whistled past the necessary and separate step of analyzing whether the severe sanction of exclusion should appropriately be imposed in this case. Instead, the military judge determined that A1C RM's failure to obtain a search authorization required automatic exclusion of the challenged evidence and all derivative evidence therefrom. This arbitrary and *per se* exclusion reflected another erroneous view of the law: The exclusionary rule applies only where it results in appreciable deterrence for

future Fourth Amendment violations and where the benefits outweigh the costs. See Wicks, 73 M.J. at 104 (quoting Herring v. United States, 555 U.S. 136, 141 (2009) (internal citations omitted)).

The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,” but “contains no provision expressly precluding the use of evidence obtained in violation of its commands.” Herring, 555 U.S. at 139. Nonetheless, the Supreme Court’s decisions established an exclusionary rule that, when applicable, is designed to safeguard Fourth Amendment rights generally through its deterrent effect. See Weeks v. United States, 232 U.S. 383, 398 (1914); United States v. Calandra, 414 U.S. 338, 348 (1974).

The fact that a Fourth Amendment violation occurred does not necessarily mean that the exclusionary rule applies. Illinois v. Gates, 462 U.S. 213, 223 (1983). While early Supreme Court decisions viewed Fourth Amendment violations as synonymous with the application of the exclusionary rule, the Court’s more recent decisions clarify that exclusion “has always been our last resort, not our first impulse.” Hudson v. Michigan, 547 U.S. 586, 591 (2006). Today, whether exclusion is an appropriate remedy in a particular case is “an issue separate from the question whether the Fourth Amendment rights of the

party seeking to invoke the rule were violated by police conduct." United States v. Leon, 468 U.S. 897, 906 (1984). Current Supreme Court precedent requires a more contextual approach to application of the exclusionary rule.

"[T]he exclusionary rule is not an individual right and applies only where it 'results in appreciable deterrence.'" Herring, 555 U.S. at 141 (citation omitted). A reviewing court should focus on the efficacy of the rule in deterring Fourth Amendment violations in the future. Id. (citations omitted). The benchmark for assessing the propriety of exclusion is whether the benefits of deterrence outweigh the costs. Leon, 468 U.S. at 910. Even a marginal deterrent effect does not require the application of the exclusionary rule. Herring, 555 U.S. at 141. "'To the extent that application of the exclusionary rule could provide some incremental deterrent, that possible benefit must be weighed against [its] substantial costs.'" Id. (citation omitted). The principal cost of applying the rule is letting guilty and possibly dangerous criminals to go free--a notion that "offends basic concepts of the criminal justice system." Id. (citing Leon, 468 U.S. at 908). "'The rule's costly toll upon truth-seeking and law enforcement objectives presents a high obstacle for those urging [its] application.'" Id. (citation omitted).

The military judge in this case arbitrarily failed to narrowly analyze and explain why the unique circumstances of this case warrant application of the exclusionary rule. When taking that additional step, this Court should find that Appellee has not met the high burden of showing the drastic sanction of exclusion is warranted. In Illinois v. Krull, 480 U.S. 340, 348-349 (1987), for example, the Supreme Court determined that evidence should only be suppressed if it can be shown that the law enforcement agent had knowledge, or may be properly charged with knowledge, that the search was unconstitutional under the Fourth Amendment. As explained in Herring, to "trigger the exclusionary rule, police misconduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." Herring, 555 U.S. at 144. The exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence. Id. The pertinent analysis of deterrence and culpability is objective. Id.

A1C RM's conduct was not deliberate, reckless, or grossly negligent. The facts demonstrate that AB, a private actor, had access to Appellee's fake Facebook profile, e-mail account, and his Centon flash drive. Her actions were motivated by (understandable) spousal anger, and she was not acting in an



official law enforcement capacity. By extension, when A1C RM became involved as a friend, he had no knowledge that his viewing of the evidence was (as argued by Appellee) improper, especially given the fact that AB not only consented to the activity, but was actively persuading him to assist and was, in fact, engaged in a contemporaneous search of the same exact material while sitting next to or close by A1C RM.

When objectively analyzing A1C RM's actions using the information that was available to him at the time he was provided AB's laptop (and he had absolutely no reason to question her ownership of the device), it was reasonable for him not to seek search authorization before viewing Appellee's profile, e-mail, and flash drive. Additionally, the government writ large did not sanction or inspire A1C RM's activities. AFOSI and security forces were not involved at all during A1C RM's "search." Therefore, the government as a whole should not be saddled with the drastic remedy of suppression of all evidence for the alleged mistakes of a young, inexperienced security forces Airman. The military judge's condemnation of the young Airman was thus unsupported by the facts.

#### **CONCLUSION**

WHEREFORE, the United States respectfully requests this Honorable Court set aside the military judge's erroneous decision to suppress evidence resulting from the search of

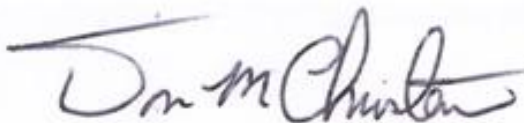
Appellee's Facebook and e-mail accounts and all derivative evidence therefrom, and expeditiously remand the case to the trial court for further proceedings.



THOMAS J. ALFORD, Capt, USAF  
Appellate Government Counsel  
Air Force Legal Operations Agency  
United States Air Force  
(240) 612-4813  
Court Bar No. 34441



GERALD R. BRUCE  
Senior Appellate Government Counsel  
Air Force Legal Operations Agency  
United States Air Force  
(240) 612-4800  
Court Bar No. 27428



DON M. CHRISTENSEN, Colonel, USAF  
Chief, Government Trial and  
Appellate Counsel Division  
Air Force Legal Operations Agency  
United States Air Force  
(240) 612-4800  
Court Bar No. 35093

**CERTIFICATE OF FILING AND SERVICE**

I certify that a copy of the foregoing was delivered to the Court and to the Air Force Appellate Defense Division on 8 July 2014 via electronic filing.

A handwritten signature in cursive script, appearing to read "Tom Alford".

THOMAS J. ALFORD, Capt, USAF  
Appellate Government Counsel  
Air Force Legal Operations Agency  
United States Air Force  
(240) 612-4813

COMPLIANCE WITH RULE 24(d)

1. This brief complies with the type-volume limitation of Rule 24(d) because:

This brief contains 9,930 words.

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

This brief has been prepared in a monospaced typeface using Microsoft Word Version 2010 with 12 point font using Courier New.

/s/

---

THOMAS ALFORD, Capt, USAF

Attorney for USAF, Government Trial and Appellate Counsel

Division

Date: 8 July 2014