UNITED STATES AIR FORCE COURT OF CRIMINAL APPEALS

U N I T E D S T A T E S,	)	**Misc. Dkt. No. 2013-26**
Appellant	)	
	)	
v.	)	
	)	**ORDER**
Senior Airman (E-4)	)	
AARON M. BUFORD,	)	
USAF,	)	
Appellee	)	**Panel No. 1**

ORR, Senior Judge:

The military judge in this case determined a Security Forces member was acting in an official capacity when, at the appellee's spouse's request, the Security Forces member viewed and collected evidence from the appellee's Facebook account, e-mail account, and thumb drive. In doing so, she ruled the Government violated the appellee's reasonable expectation of privacy under the Fourth Amendment[1] and suppressed all of the images and chat logs found on the appellee's wife's Dell laptop computer, the appellee's Hewlett Packard laptop computer, and the appellee's Centon thumb drive. The military judge further suppressed all derivative evidence. The Government claims the evidence was obtained lawfully, arguing the Security Forces member was not acting in an official capacity. The images and chat logs are the primary source of evidence showing the appellee wrongfully committed indecent conduct and wrongfully received and possessed child pornography in violation of Articles 120 and 134, UCMJ, 10 U.S.C. §§ 920, 934. After the military judge denied a request for reconsideration, the Government brought an appeal of her ruling under Article 62, UCMJ, 10 U.S.C. § 862. We heard oral argument on this issue on 16 January 2014.[2]

Jurisdiction and Standard of Review

The United States may appeal "[a]n order or ruling of the military judge which terminates the proceedings with respect to a charge or specification" in a trial by court-martial in which a punitive discharge may be adjudged. Article 62(a)(1)(A), UCMJ, 10 U.S.C. § 862(a)(1)(A). Each of the dismissed specifications in this case carries a maximum punishment that includes a punitive discharge. *Manual for*

[1] U.S CONST. amend. IV.
[2] Senior Judge Orr took part in oral argument and drafted this opinion prior to his retirement.

Courts-Martial (*MCM*), *United States*, Part IV, ¶ 68b.e. (2012 ed.); *MCM*, A27, ¶ 45.e.; *MCM*, A27, ¶ 87.e.; *MCM*, A28, ¶ 45.f.(6).

We review de novo matters of law in appeals under Article 62, UCMJ. In ruling on issues under Article 62, UCMJ, we "may act only with respect to matters of law." Article 62(b), UCMJ, 10 U.S.C. § 862(b). On matters of fact, we are bound by the military judge's factual determinations unless they are unsupported by the record or clearly erroneous. *United States v. Gore*, 60 M.J. 178, 185 (C.A.A.F. 2004). "Nonetheless, in entering a finding of fact, the military judge must rely on evidence of record which fairly supports that finding; in the absence of *any* such evidence, the finding is error as a matter of law." *United States v. Bradford*, 25 M.J. 181, 184 (C.M.A. 1987) (emphasis in original). We also review the judge's ruling on the suppression motion for an abuse of discretion. *United States v. Cote*, 72 M.J. 41, 44 (C.A.A.F. 2013). "The courts may make a de novo ad hoc judgment on the meaning of relevant facts when dealing with constitutional issues." Francis A. Gilligan & Fredric I. Lederer, *Court-Martial Procedure* § 25-83.00 (2d ed.1999) (citing *United States v. Abell*, 23 M.J. 99, 102-03 (C.M.A.1986)). "Similarly, the appellate courts normally should have the power to reverse when the trial judge misunderstood the legal significance of a fact found by the judge when that misunderstanding causes an error as to the court's ultimate finding." *Id.* (citing *United States v. Shakur*, 817 F.2d 189 (2d Cir.1987)).

We have reviewed the military judge's findings of fact and conclude that the findings are neither unsupported by the record nor clearly erroneous. We are thus bound by the military judge's findings of fact and summarize them below.

Military Judge's Findings

In March 2012, AB[3], wife of the appellee, found a "fake" Facebook account that was associated with the appellee's e-mail address. AB identified the page as a "fake" account because the name and photo associated with the account were not of the appellee, but the e-mail address belonged to him. She became curious and logged onto the appellee's e-mail account.

On or about 17 May 2012, Airman First Class (A1C) RM[4] was an active duty Security Forces member who was at the home of CH. AB was also present in the home, but the appellee was not. At some point that evening, A1C RM noticed AB was distraught while she was looking at the screen of her Dell laptop. AB, knowing that A1C RM was a Security Forces member, asked him to look at the laptop where he saw the appellee's "fake" Facebook page. While A1C RM thought it might involve

[3] While noting that the appellee and his wife both have the initials AB, for the purpose of this order, AB is only in reference to the appellee's wife and not the appellee.

[4] Airman First Class (A1C) RM is no longer on active duty in the Air Force and is now Mr. RM. Nevertheless, during the entire timeframe he was involved in this investigation, he was an active duty Security Forces member. Therefore, for the purpose of this order, he will be referred to as A1C RM.

something like the appellee cheating on his wife, A1C RM proceeded to search further for more information. He went into the "messages" section where he allegedly found multiple conversations with females, pictures of male genitalia, and other sexually explicit communication. A1C RM created "screen shots" of what he saw on the Facebook page as well as what was in the messages section. He saved these screen shots to a portable flash-drive. He then continued his search by going into the "Yahoo" e-mail account associated with the "fake" Facebook page using a password provided by AB.

AB gave A1C RM consent to search her Dell laptop. However, the "fake" Facebook account and the associated e-mail account belonged to the appellee. The e-mail account was password protected. There was no evidence on how AB obtained the password to either of these accounts. Although the Facebook account and the e-mail account were accessed through AB's laptop, they do not physically reside on the laptop.

Based upon his law enforcement background, A1C RM encouraged AB to go to the Security Forces investigations flight chief. A1C RM drove her to the Security Forces Squadron (SFS) and explained to the SFS flight chief what was happening. The SFS flight chief looked at the information on the flash-drive and turned the case over to the Air Force Office of Special Investigations (AFOSI). In an interview with the AFOSI, AB provided a written statement and signed a form consenting to the search and seizure of a Dell laptop, a PN 8GB Flashdrive, and a one gigabyte memory card. Later that day, the AFOSI agents conducted a search of the joint residence of the appellee and AB. A1C RM informed AB, that based on his knowledge and experience investigations could take quite a bit of time, and that during that time she would not have access to any items she gave to the AFOSI. During the search, A1C RM acted as a "conduit" between AB and the AFOSI agents because "he was a cop and he could relate to them." AB became upset when the AFOSI agents were seizing a video camera that contained photos and/or pictures of her son, so A1C RM, on her behalf, asked about a warrant. A1C RM "didn't want [AFOSI] to overstep their bounds." Because of A1C RM's question about a warrant, the AFOSI agents stopped the search and obtained a warrant. After retuning with a warrant, they seized a Hewlett Packard (HP) laptop which belonged to the appellee.

In early June 2012, AB gave A1C RM a Centon thumb drive[5] that AB found behind the television in her home. A1C RM conducted his own "search" to see whether there was actually evidence on it. A1C RM opened multiple folders in the thumb drive, some of which contained work materials such as Air Force Instructions and others which contained pornography. Based on the information on the thumb drive, A1C RM determined it belonged to the appellee. A1C RM contacted an AFOSI agent to turn in the thumb drive. The AFOSI agents took possession of the thumb drive the next day.

[5] We use "Centon thumb drive" or "thumb drive" throughout this order to distinguish it from the flash drive used by A1C RM on 17 May 2012 to save screenshots from his search of the appellee's Facebook and e-mail account, which he conducted on AB's Dell laptop.

Although A1C RM stated he was not acting in his official capacity, his testimony was inconsistent with this position. A1C RM stated, "[AB] asked [me] to look at the laptop because [I] was a cop; that [I] began searching for and collecting evidence; that [I] didn't want evidence to get lost; that [I]was going off [my] instincts as a SFS member; that [I] searched the messages section because [I] knew that's where people hide stuff; that once [I] saw the names associated with the pictures [I] became more curious." He also stated, "[I] encouraged [AB] to go to investigations and that [I] felt responsible until the laptop was turned over to SFOI then OSI."

An AFOSI agent testified that if AB had brought only the information regarding the adultery and "fake" Facebook account to their attention, they were unlikely to open an investigation. The agent's impression of A1C RM was that he "took screen shots to preserve evidence; that he wanted to be involved in the investigation, and that the AFOSI agents actually questioned his motivation and whether or not he 'planted' evidence."

Discussion

We accept the judge's factual findings, which leaves us only to review her application of the law.

> 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. The abuse of discretion standard calls for more than a mere difference of opinion. The challenged action must be arbitrary. . . , clearly unreasonable, or clearly erroneous.

United States v. Wicks, 73 M.J. 93, 98 (C.A.A.F. 2014) (internal quotation marks and citations omitted).

The military judge granted the defense motion to suppress after concluding that, although A1C RM stated he was not acting in an official capacity, his testimony led the military judge to believe otherwise. In support this ruling, the military judge stated A1C RM's actions went far beyond those expected of a private citizen. The military judge noted the deficiencies in the Government's argument and concluded that but for the actions of A1C RM, a "conduit" between AB and the AFOSI, the search of the Dell laptop would not have occurred. As a result, the Government had not proven by a preponderance of the evidence that the items seized and ultimately searched (the Dell Laptop, the Hewlett Packard Laptop and Centon thumb drive) were seized in accordance with the Fourth Amendment and the Military Rules of Evidence.

Government Agent

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures."[6] The Supreme Court has determined that "[a] 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed[,]" and "a 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). It is well established that the protection against unreasonable searches and seizures only applies to Governmental action and is not applicable when effected by a private individual who is not acting as a Government agent or with participation or knowledge of any Governmental official. *Id*. When determining whether someone was acting as a Government agent, it does not matter what the person's individual/subjective motivation may have been, you must look at the "degree of the Government's participation in the private party's activities, a question that can only be resolved 'in light of all the circumstances.'" *United States v. Daniels*, 60 M.J. 69, 71 (C.A.A.F. 2004) (quoting *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602, 614-15 (1989)). To trigger the Fourth Amendment in this way, it must be clear that the Government encouraged, endorsed, and participated in the challenged search. *Id*.

Not every search by a military member constitutes a Government search. *United States v. Volante*, 16 C.M.R. 263, 266 (C.M.A. 1954). Our Superior Court has stated, "[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*. However, not all searches by law enforcement individuals have been deemed Government searches. *United States v. Portt*, 21 M.J. 333 (C.M.A. 1986) (holding that a security policeman acted in his private capacity when he searched the accused's locker out of curiosity while performing janitorial duties). Therefore, A1C RM's status as a Security Forces member does not categorically make him a Government actor for the purpose of the searches at issue. Instead, the analysis is fact specific as to whether A1C RM was acting under the authority of the United States.

Unlike the security policeman in *Portt*, in the case at hand, there is substantial evidence in the record of trial to support the finding that A1C RM was acting as a Government agent. Consistent with the military judge's conclusions and in light of all the circumstances, we are convinced A1C RM acted as a Government agent for several reasons to include: (1) As a Security Forces member his job was to enforce the law; (2) A1C RM and AB were mere acquaintances prior to this investigation; (3) AB asked for A1C RM's help knowing he was a law enforcement officer; (4) He actively inserted himself on multiple occasions into the role of an investigator both prior to and during the formal investigation; and (5) He participated in the challenged search and collected evidence for future law enforcement use.

[6] U.S CONST. amend. IV.

Because we concur with the military judge that A1C RM was acting as a Government agent, we then turn to whether his warrantless search fell within one of the few specifically established and well-delineated exceptions. *Wicks*, 73 M.J. at 99.

Warrantless Search

When the Government obtains evidence in a warrantless search that was conducted pursuant to one of the few specific exceptions allowing such a search, the Government bears the burden of establishing that the exception applies. *Id.* Voluntary consent to search by a person possessing authority is one of the "carefully drawn" exceptions. *United States v. Weston*, 67 M.J. 390, 392 (C.A.A.F. 2009).

We concur with the military judge's determination on the issue of consent. AB gave consent to the search of the Dell laptop and had both actual and apparent authority over that laptop. Nevertheless, we also agree that consent to search the Dell laptop did not extend to the Facebook and email accounts of the appellee. Consent to search an electronic device does not automatically extend to consent to search all electronic "papers" not contained on the device but accessed through the device. Here, A1C RM had clear indications the "fake" Facebook account and the e-mail account belonged to the appellee. The e-mail account was password protected. The evidence is that A1C RM should have known the e-mail account was not under the authority of AB. *Cf. United States v. Gallagher*, 66 M.J. 250 (2008) ("[A]bsent evidence tending to show that an officer should have known that the closed container was not under the authority of person who consented to the search, the search of a closed container belonging to a third party will be deemed reasonable.") Although AB had knowledge of the password, this does not automatically result in a conclusion that she had actual or apparent authority over an otherwise private separate account maintained by her husband. In an Article 62, UCMJ, appeal for a motion to suppress, we review the evidence in the light most favorable to the prevailing party at trial. *United States v. Barker*, 70 M.J. 283, 288 (C.A.A.F. 2011). A third-party's control over property or effects is a question of fact. *United States v. Rader*, 65 M.J. 30, 33 (C.A.A.F. 2007). We concur with the military judge's ruling that the Government failed to meet its burden of establishing that the consent exception applied to the search of the Facebook and e-mail accounts.

We next consider whether AB's search of the appellee's Facebook account amounted to a private search that frustrated the appellee's expectation of privacy. There are two limitations to the private search exception: (1) The Government cannot conduct or participate in the private search; and (2) The Government may not go beyond the scope of the private party's search, to include expanding the search into a general search. *Wicks*, 73 M.J. at 100. When applied to modern computerized devices such as laptops and cell phones, "[T]he scope of the private search can be measured by what the private actor *actually* viewed as opposed to what the private actor had access to view." *Wicks*, 73 M.J. at 100. AB accessed the appellee's Facebook and email accounts in March 2012

and was accessing his Facebook account again on 17 May 2012 when she asked A1C RM to look at the account. Because the record is not clear about exactly what AB viewed during her private searches of the appellee's Facebook messages and e-mail account, we are not convinced A1C RM's subsequent search mirrored AB's private search. Therefore, because we must review the evidence in the light most favorable to the prevailing party, *Barker*, 70 M.J. at 288, it is impossible for us to conclude the Government met the requirements of this exception. Therefore, the private search exception does not apply to these subsequent searches.

Subsequent Search Warrant

Next, we must determine whether the Government had proper search authority with regards to the HP laptop. The probable cause necessary to warrant a search cannot be based on illegally obtained information or evidence. *United States v. Turck*, 49 C.M.R. 49 (A.F.C.M.R. 1974). The search warrant used for the search of the home of AB and the appellant where the HP laptop was seized was based on information obtained by A1C RM's unconstitutional search of the appellee's Facebook and e-mail accounts. Therefore, the Government cannot rely on the subsequent search warrant as legal authorization to search the HP laptop.

Consent Search

We turn next to the Centon thumb drive. A few weeks after the AFOSI's thorough search of her home, AB found a thumb drive near her television. AB provided the thumb drive to A1C RM. A1C RM then searched the thumb drive to determine if it contained any evidence. The thumb drive was not password protected. Because A1C RM was a Government agent, we examine to see if an exception applies. In this instance, we disagree with the military judge and conclude that AB was authorized to provide consent to the search of the thumb drive. "Where one party has joint access and control to a property and voluntarily consents to a search, the warrantless search is reasonable." *United States v. Weston*, 67 M.J. 390, 393 (C.A.A.F. 2009). "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.* at 392. Here the thumb drive was in the home AB shared with the appellee. There is no evidence the thumb drive was in the exclusive domain of the appellee. In the context of personal computers and associated digital devices, "[C]ourts examine whether the relevant files were password-protected or whether the [appellee] otherwise manifested an intention to restrict third-party access." *United States v. Rader*, 65 M.J. 30, 34 (C.A.A.F. 2007). Examining the evidence in the light most favorable to the appellee, (1) He had a thumb drive he solely used; (2) He left it in the common area of the house he shared with his wife; and (3) He did not password protect it to prevent her access to the device. The thumb drive is not like a cellphone or a laptop connected to the internet, it is a "static storage container" more akin to an electronic briefcase. *Cf. Wicks*, 73 M.J. at 102. Much like the briefcase in *Gallagher*, the thumb drive "was kept in a common area and opened without manipulation of the

tumblers." *United States v. Gallagher*, 66 M.J. 250, 254 (C.A.A.F. 2008). We conclude AB had common authority over this unsecured device in her home, and like any other unsecured storage device, she had the ability to consent to the search of the thumb drive. Because proper search authority was given by AB's consent, the military judge abused her discretion in the application of the law by suppressing the evidence from the search of the Centon thumb drive.

Similarly, the military judge found that AB gave consent to A1C RM to search the Dell laptop. AB also gave written consent for the AFOSI to search the Dell laptop when she provided it to the AFOSI on 18 May 2012. While there is some evidence that AB became upset as the AFOSI agents searched and planned to seize additional items from her home, there is no evidence that she ever revoked her consent to search her Dell laptop. For the reasons explained above, AB had actual and apparent authority over the Dell laptop and was able to provide consent to search the device. We distinguish the search of the hard drive which is a physical component of the laptop from using the laptop as a conduit to access electronic data through internet based services. We conclude that AB was able to consent to the search of the Dell laptop. The military judge abused her discretion in the application of the law as to AB's consent to the search of the Dell laptop.[7]

Conclusion

We hold the military judge did not err in granting the motion to suppress the evidence derived from the appellee's Facebook account, e-mail account, and HP laptop. The military judge made detailed findings of facts supported by the record, accurately described the applicable law, and reasonably concluded the Government had not met its burden on the admissibility of those items of evidence. As such, with regards to the evidence derived from the appellee's Facebook account, e-mail account, and HP laptop, the military judge did not abuse her discretion.

We hold that the military judge erred when granting the motion to suppress the evidence contained on the Dell laptop and the Centon thumb drive.

We remand the case to the trial court for further proceedings.

On consideration of the Appeal by the United States under Article 62, UCMJ, it is by the Court on this 4th day of April, 2014,

[7] As our fact finding power is limited during an Article 62 appeal, we leave as unresolved the issue as to whether the evidence obtained from the Dell laptop is evidence that was contained on the laptop prior to the illegal search or was derivative evidence that was created by the illegal search.

ORDERED:

That the Government's appeal is hereby **DENIED in part and GRANTED in part.**

The Government's appeal is denied as to the suppression of evidence from the Hewlett-Packard (HP) laptop.

The Government's appeal is granted as to the suppression of evidence from the Dell laptop and Centon thumb drive. .

HARNEY, Senior Judge, and MITCHELL, Judge, concur.

FOR THE COURT

STEVEN LUCAS
Clerk of the Court