UNITED STATES AIR FORCE COURT OF CRIMINAL APPEALS

UNITED STATES

v.

Captain WALTER M. PLUSH
United States Air Force

ACM 35134

21 September 2004

Sentence adjudged 25 January 2002 by GCM convened at Ellsworth Air Force Base, South Dakota. Military Judge: Mark R. Ruppert.

Approved sentence: Dismissal, confinement for 5 months, and forfeiture of $2,432.00 pay per month for 5 months.

Appellate Counsel for Appellant: Colonel Beverly B. Knott, Major Terry L. McElyea, Major Patricia A. McHugh, and Captain Diane M. Paskey.

Appellate Counsel for the United States: Colonel LeEllen Coacher, Lieutenant Colonel Lance B. Sigmon, and Lieutenant Colonel Jennifer R. Rider.

Before

PRATT, ORR, and MOODY
Appellate Military Judges

OPINION OF THE COURT

This opinion is subject to editorial correction before final posting.

MOODY, Judge:

The appellant was convicted, in accordance with his pleas, of violating a lawful general regulation, in violation of Article 92, UCMJ, 10 U.S.C. § 892. He was convicted, contrary to his pleas, of four specifications of conduct unbecoming an officer, in violation of Article 133, UCMJ, 10 U.S.C. § 933. The general court-martial, consisting of officer members, sentenced the appellant to a dismissal, confinement for 5 months, and forfeiture of $2,432.00 pay per month for 5 months. The convening authority approved the sentence as adjudged. The appellant has submitted three assignments of error: (1)

The military judge erred in not suppressing the results of a search and seizure of the appellant's computers; (2) The evidence is legally and factually insufficient as to the contested charge of conduct unbecoming an officer; and (3) The action is ambiguous in that the convening authority approved the sentence to forfeitures while at the same time waiving mandatory forfeitures, contrary to *United States v. Emminizer*, 56 M.J. 441 (C.A.A.F. 2002). Finding error, we order corrective action in the form of new post-trial processing.

Facts

During the times alleged in the charges and specifications, the appellant was assigned to the 28th Communications Squadron at Ellsworth Air Force Base (AFB), South Dakota. In January of 2001, the appellant brought a government laptop computer in for repair of a cracked screen. The computer had been issued to him for use during a recent deployment, and he had maintained custody and control of it ever since. After removing the hard drive, the noncommissioned officer in charge of computer maintenance, Master Sergeant (MSgt) Giancarlo, sent the computer to the manufacturer for repair.

Upon the computer's return, MSgt Giancarlo, while performing routine maintenance on it, found unusually large files in the recycle bin and the temporary Internet files. MSgt Giancarlo later testified that the recycle bin was 40 times larger than normal. He also found approximately 1,200 graphics files. Examining three of them, he discovered that they contained sexually explicit photographs. MSgt Giancarlo notified the Security Forces Office of Investigations (SFOI), which advised him to bring the laptop to them. At SFOI, Staff Sergeant (SSgt) Wimmer, who was an investigator, MSgt Giancarlo, and the computer network administrator then accessed approximately 100 sexually explicit photographs from among the 1,200 graphics files on the laptop, among which were interspersed photographs of the appellant.

Based upon the discovery of these photographs, SSgt Wimmer sought a search authorization for the appellant's official desktop computer. Specifically, SSgt Wimmer requested authorization to search the appellant's office and to seize a "Government computer PC" issued to the appellant and "any computer discs within the confines of his office." The supporting affidavit read, in part:

> I reviewed the lap top and discovered numerous personal pictures, downloaded from the internet and a digital camera of [the appellant]. I also discovered numerous pornographic photographs downloaded from the internet. There is [sic] numerous material on the lap top that indicates [the appellant] is the primary user if not the only user of the system. Investigation also revealed a picture of [the appellant] in uniform downloaded from the internet at 2306 on 12 Dec 00 and numerous pornographic photographs within minutes before and after the photo of [the

> appellant] was downloaded. There is [sic] also several photographs of a males [sic] anatomy I suspect to be [the appellant's]. I believe there is sufficient evidence connecting [the appellant] with the pornographic material and have a strong indication there will be pornographic material on his office computer.

SSgt Wimmer discussed the evidence with the legal office at Ellsworth AFB, which agreed that it was sufficient to establish probable cause. Based upon the affidavit and the opinion of the legal office, the magistrate, Colonel Mathis, authorized the search and seizure. Subsequently, SSgt Wimmer entered the appellant's office, seizing numerous floppy and zip disks and two Micron desktop computers.

SSgt Wimmer sent the computers and disks to the United States Army Criminal Investigation Lab (USACIL) for forensic analysis. Before conducting the examination, the USACIL analyst, Ms. Neuendorf, requested two further search authorizations, one for the laptop and another to permit her examination of all the computers to extend beyond the three days allotted in the authorizations.

During her analysis, Ms. Neuendorf clicked on a hypertext markup language (HTML) script, which resulted in her discovery of 15 sexually explicit pictures. Originally believing these were located on one of the hard drives, she subsequently discovered that she had actually, though inadvertently, accessed them from the appellant's Yahoo account on the Internet. She stated at trial that this was unusual, in that one would normally expect to see a password prompt or other warning prior to accessing an Internet site. All in all, Ms. Neuendorf discovered that the three computers contained nearly 4,500 sexually explicit images. In addition, she discovered that, on at least one occasion, the appellant had used one of the desktops to email a photograph of his exposed penis to another person.

Suppression of the Evidence

This assignment of error pertains only to Charge II and its specifications, to which the appellant pled not guilty. *See* Rule for Courts-Martial 910(j).

This court reviews a judge's ruling on a motion to suppress for an abuse of discretion. *United States v. Monroe*, 52 M.J. 326, 330 (C.A.A.F. 2000). *See Illinois v. Gates*, 462 U.S. 213, 236 (1983) (a magistrate's probable cause determination should be paid "great deference" by reviewing courts). *See also United States v. Mason*, 59 M.J. 416, 421 (C.A.A.F. 2004) (in reviewing a determination of probable cause, courts should consider the information made known to the magistrate at the time of his decision, "considered in the light most favorable to the prevailing party").

"A person may challenge the validity of a search only by asserting a subjective expectation of privacy which is objectively reasonable." *Monroe*, 52 M.J. at 330. "Individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer. . . . Public employees' expectations of privacy in their offices, desks, and file cabinets . . . may be reduced by virtue of actual office practices and procedures, or by legitimate regulation." *O'Connor v. Ortega*, 480 U.S. 709, 717 (1987).

In cases in which the search invades the accused's reasonable expectation of privacy, and in which no exception to the warrant requirement can be found, the search must be based upon a magistrate's determination of probable cause. "Probable cause to search exists when there is a reasonable belief that the . . . evidence sought is located in the place or on the person to be searched." Mil. R. Evid. 315(f)(2); *United States v. Hall*, 50 M.J. 247, 249 (C.A.A.F. 1999); *United States v. Figueroa*, 35 M.J. 54, 55-56 (C.M.A. 1992). Good faith reliance by law enforcement personnel upon a subsequently invalidated warrant does not require suppression of the fruits of the search. *United States v. Leon*, 468 U.S. 897, 909 (1984). *See also United States v. Chapple*, 36 M.J. 410 (C.M.A. 1993).

We begin our consideration of the case sub judice with the threshold question of whether the appellant enjoyed an expectation of privacy in the laptop computer. Its contents were initially examined without a search authorization. This examination constituted the basis for the search and seizure of the two desktop computers as well as for the subsequent forensic analysis conducted by USACIL.

Our superior court has stated that the nature of military life provides members with a "minimal expectation" of privacy in government property, due to government ownership, the "nonpersonal nature of military offices," and the inherent right of command to inspect property under its control. *United States v. Muniz*, 23 M.J. 201, 206 (C.M.A. 1987).

Air Force policy requires the monitoring of telecommunication systems, including computers, to ensure that they are being used for the conduct of official business and provides that use of such equipment constitutes consent to monitoring. *See* Air Force Instruction (AFI) 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*, ¶ 13 (15 May 2000). This instruction further requires a notice and consent log-on banner to be installed on all computers. This banner advises that the computer may be monitored "for all lawful purposes" and that such monitoring extends to "[a]ll information, including personal information, placed on or sent over [the] system." AFI 33-219, ¶ A2.3.5.

In light of this, we find that the appellant, who was assigned to the Communication Squadron, could not reasonably have expected a right of privacy as to his

laptop computer. "One does not acquire a reasonable expectation of privacy in Government property designated or assigned under these circumstances even if capable of being secured and regardless of that person's status." *United States v. Tanksley*, 50 M.J. 609, 620 (N.M. Ct. Crim. App. 1999), *aff'd*, 54 M.J. 169 (C.A.A.F. 2000). The appellant's act in having voluntarily turned the laptop over to the maintenance workcenter for repair further vitiated any claim of privacy as to its contents. Once he relinquished custody of the computer, he was in no position credibly to expect that government officials such as MSgt Giancarlo or SSgt Wimmer would turn a blind eye to contraband so easily discovered.

Of course, the appellant's privacy interests in the two desktops were also limited by the legal and policy considerations discussed above. However, as stated above, the seizure of these two computers, as well as the forensic examination of all three computers conducted by USACIL, were based on search authorizations. Our analysis will focus on the legal sufficiency of these authorizations.

The laptop contained a substantial number of sexually explicit images, interspersed with photographs of the appellant in uniform. One of the pictures of the appellant was downloaded at the same time as many of the lubricious photographs, giving rise to the reasonable belief that the appellant was trolling the Internet for pornography while on duty. We conclude that the facts available to the magistrate establish a "fair probability" that the other computer equipment issued to the appellant for use in his office for the performance of official duties would contain pornography. *See Figueroa*, 55 M.J. at 56. Of course, there were two computers in the appellant's office corresponding with the "Government computer PC" described in the search authorization. We find that in seizing both, SSgt Wimmer did not exceed the scope of the authorization.

Even if the evidence fell short of probable cause, the record contains no basis to conclude that SSgt Wimmer acted with "reckless disregard of the truth" in preparing the affidavit which he submitted to Colonel Mathis in support of his request for a search authorization. *Leon,* 468 U.S. at 923. In addition, he obtained the opinion of the legal office that the facts were sufficient to establish probable cause. Colonel Mathis, whose prior knowledge of the appellant was not so extensive as to impair his impartiality *(See* Mil. R. Evid. 315(d) and *United States v. Lopez*, 35 M.J. 35, 40 (C.M.A. 1992)), provided SSgt Wimmer with a facially valid search authorization. The record is most consistent with SSgt Wimmer having acted in "objectively reasonable reliance" upon that authorization. Therefore, even if probable cause is found to be lacking, we conclude that the good faith exception to the exclusionary rule permitted the introduction of the evidence found on the appellant's computers. Mil. R. Evid. 311(b)(3). *See United States v. Pond,* 36 M.J. 1050, 1059 (A.F.C.M.R. 1993).

Finally, we conclude that no error occurred in Ms. Neuendorf's access of the photographs located on Yahoo. She was legitimately searching the contents of the appellant's computer, she discovered the Yahoo photographs inadvertently, and they were clearly incriminating. *See United States v. Van Hoose*, 11 M.J. 878, 882 (A.F.C.M.R. 1981). Therefore, we hold that the military judge did not abuse his discretion in denying the motion to suppress.

Legal and Factual Sufficiency of the Evidence

The test for legal sufficiency is whether any rational trier of fact, when viewing the evidence in the light most favorable to the government, could have found the appellant guilty of all elements of the offenses, beyond a reasonable doubt. *Jackson v. Virginia*, 443 U.S. 307, 319 (1979); *United States v. Reed*, 54 M.J. 37, 41 (C.A.A.F. 2000).

Our superior court has determined that the test for factual sufficiency is whether, after weighing the evidence and making allowances for not having observed the witnesses, this Court is convinced of the appellant's guilt beyond a reasonable doubt. *Reed*, 54 M.J. at 41 (citing *United States v. Turner*, 25 M.J. 324, 325 (C.M.A. 1987)).

We find that the appellant maintained pornographic images on a government computer and in a Yahoo web site, sending one of them to another person by email. The appellant may have hoped or even subjectively expected that these photographs would remain undiscovered and, to that extent, private. Nevertheless, "[t]he conduct of an officer may be unbecoming even when it is in private." *United States v. Moore*, 38 M.J. 490, 493 (C.M.A. 1994). We conclude that the appellant's conduct in this case "seriously compromises [his] standing as an officer." *Manual for Courts-Martial, United States (MCM)*, Part IV, ¶ 59(c)(2) (2000 ed.). Examining the appellant's case in light of the criteria described above, we hold that his conviction for conduct unbecoming an officer is both legally and factually sufficient.

Post-Trial Processing

We review post-trial processing de novo. After the trial, the convening authority waived mandatory forfeitures for a period of six months and directed that the money be paid to the appellant's spouse. The convening authority did not, however, disapprove or suspend the adjudged forfeitures, as required by *Emminizer*. In light of our superior court's holding in *United States v. Lajaunie*, No. 04-0168/AF (21 Jul 2004), we conclude that this is error, requiring a new action.

The action of the convening authority is set aside. The record of trial is returned to The Judge Advocate General for remand to the convening authority for post-trial processing consistent with this opinion. Thereafter, Article 66(b), UCMJ, 10 U.S.C. § 866(b), will apply.

OFFICIAL

ANGELA M. BRICE
Clerk of Court