IN THE U.S. NAVY-MARINE CORPS COURT OF CRIMINAL APPEALS
WASHINGTON NAVY YARD
WASHINGTON, D.C.

BEFORE

Charles Wm. DORMAN **D.A. WAGNER** **R.W. REDCLIFF**

UNITED STATES

v.

Jennifer N. LONG
Lance Corporal (E-3), U.S. Marine Corps

PUBLISH
NMCCA 200201660 Decided 11 May 2005

Sentence adjudged 3 October 2001. Military Judge: E.W. Loughran. Review pursuant to Article 66(c), UCMJ, of Special Court-Martial convened by Commanding Officer, Headquarters Battalion, HQMC, Henderson Hall, Arlington, VA.

CHARLES W. GITTINS, Civilian Appellate Counsel
LtCol ERIC B. STONE, USMC, Appellate Defense Counsel
LT JASON GROVER, JAGC, USN, Appellate Defense Counsel
Maj KEVIN HARRIS, USMC, Appellate Government Counsel
LT FRANK GATTO, JAGC, USNR, Appellate Government Counsel

WAGNER, Judge:

A special court-martial composed of officer and enlisted members convicted the appellant, contrary to her pleas, of use of ecstasy, ketamine, and marijuana, in violation of Article 112a, Uniform Code of Military Justice, 10 U.S.C. § 912a. The appellant was sentenced to confinement for 2 months, reduction to pay grade E-1, and a bad-conduct discharge. There was no pretrial agreement. The convening authority approved the sentence as adjudged.

The appellant claims that the military judge erred by denying the defense motion to suppress e-mails sent and received by the appellant on her Government computer. The appellant contends these e-mails were seized from the Government network domain server at the behest of law enforcement officials, without the appellant's consent, and without a lawful search authorization based on probable cause.

After carefully considering the record of trial, the appellant's sole assignment of error, the Government's response, the appellant's reply brief, and oral argument, we conclude that the military judge erred in admitting the e-mails. We also conclude that the error did not materially prejudice the appellant's substantial rights. Therefore, we decline to grant relief. Arts. 59(a) and 66(c), UCMJ.

Facts

The appellant was charged with using ecstasy, ketamine, and marijuana with fellow-Marines in the barracks. The evidence at trial consisted primarily of eye-witness testimony. The Government also sought to admit 17 pages of e-mail transcripts (Prosecution Exhibit 1) wherein the appellant discussed her fear of urinalysis testing and her own efforts to mask her drug use. The e-mails in the exhibit consisted of three strings of e-mail exchanges between the appellant and three different individuals.

During the motion stage of the trial, the defense unsuccessfully moved to suppress the e-mails. The defense asserted the e-mails were seized without the appellant's consent or a lawful search authorization and, therefore, in violation of the 4th Amendment of the Constitution.

The only witness to testify on the motion was the senior network administrator for Headquarters, Marine Corps. The following facts relating to the seizure of the e-mails are derived from that testimony and are uncontroverted. The appellant was assigned a Government computer, including an e-mail account. Although issued for official use, personal use of Government computers and e-mail accounts was permissible as long as such use did not interfere with official business or constitute a prohibited use under departmental regulations. Access to e-mail required a user-generated password, which prevented unauthorized users from accessing an individual's Government e-mail account. E-mails originating from or being received by a Government computer within the network went to a central Government computer system domain server for delivery to their intended recipients via the domain server network or the internet. Copies of sent e-mails remained on the domain server unless the user specifically set up their e-mail account to not save outgoing messages. Even e-mails thereafter deleted by the user could be retrieved using a "restore" function. A system administrator could access all e-mail accounts serviced by the domain server.

E-mail could be sent from the Government computer workstation or from a remote computer. When accessing the network via the Government computer workstation a banner was displayed warning the user of possible monitoring of the computer network system. The banner was titled "Notice and Consent to Monitoring." The text is reproduced in whole, as follows:

> This is a Department of Defense computer system. This computer system, including all related equipment, networks and network devices (specifically including Internet access), are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

Appellate Exhibit XIII. A different banner appeared when accessing the network remotely that simply notified the user that they were accessing the Government network.

The system administrator conceded in testimony that the e-mails in question were not retrieved during monitoring of the system or discovered as a result of the appellant's unauthorized use of a Government computer. Rather, they were retrieved as the result of a specific request by law enforcement officials to provide any e-mails related to the appellant's drug use. No search warrant or authorization accompanied the request. There was no ongoing monitoring of the system by the network administrator at the time the request was received.

The military judge found that the network administrator's actions constituted a search for evidence and that there was no actual consent by the appellant to this search. He also found that there was no search authorization issued based on probable cause. The military judge found, however, that the appellant had no reasonable expectation of privacy in the e-mail account and denied the motion to suppress on that sole basis.

Three enlisted Marines testified for the prosecution regarding the appellant's use of ecstasy, ketamine, and marijuana. All three testified that the appellant had used ecstasy in their presence and two of them testified that they had observed the appellant using ketamine and marijuana in their presence. Specifically, the Government witnesses testified that during June and July of 2000, they used ecstasy, ketamine, and marijuana in the barracks with the appellant and other Marines.

They described the drugs and the effects they felt from using the drugs. They also testified to observing the physical effects of the drugs in the appellant's behavior following her ingestion of each substance. The witnesses testified about methods used to mask the smell of marijuana smoke in the barracks, such as gathering in the bathroom and turning on the shower and exhaust fan during use. They testified that the drug use typically occurred on a Friday or Saturday night, prior to going out to local clubs or after returning from the clubs. Each testified to the use of sensory enhancements such as music, blacklights, menthol inhalers, and massage intended to heighten the drug-induced experience. The three witnesses all testified under grants of immunity and following nonjudicial or court-martial action for their respective roles in the drug activities.

A civilian law enforcement officer then testified regarding the physiological effects of illegal drugs, common slang used for illegal drug use, and common methods of using and enhancing the use of illegal drugs. The military judge thereafter admitted Prosecution Exhibit 1 over defense objection.

In further support of its case on the merits, the Government then introduced testimony from a fellow-Marine, Corporal (Cpl) "U", who had been friends with the appellant since 1998. He testified that they kept in contact with each other primarily by e-mail. Cpl U testified that he had a face-to-face conversation with the appellant in August of 2000 in which she told him that there was a urinalysis upcoming, and at the time, the appellant appeared to be worried about it. Cpl U also stated that the appellant admitted to him during their conversation that she had used marijuana and ecstasy. He stated that the conversation continued thereafter by exchange of e-mails, copies of which were contained in pages 10 through 17 of Prosecution Exhibit 1. He testified that the appellant asked him for advice on what would happen to her if she had a positive urinalysis.

In the defense case on the merits, the defense presented the testimony of one of the active duty Marines named as a participant in the drug activity by the Government witnesses. He testified that he was facing similar charges in a court-martial scheduled to begin a few weeks later. The witness stated that he did not use marijuana, ketamine, or ecstasy in the barracks and that he had never seen the appellant use those drugs. He also denied socializing with any of the Marines other than his roommate, who was also named as a participant. His roommate, now involuntarily separated from the Marine Corps, also testified for the defense, and denied that he had ever used marijuana, ketamine, or ecstasy in the barracks or seen drug use in the barracks. He further testified that he had never seen the appellant use drugs.

Another Marine testified that he tested positive for marijuana in July of 2000 on a urinalysis and subsequently acted as a confidential informant. He stated that he used marijuana

with fellow Marines in the barracks, but never saw the appellant use drugs. He testified that his job as a confidential informant was to ferret out drug activity in the barracks. Another former Marine testified that she socialized with the appellant while on active duty and that she never used drugs and had never seen the appellant use drugs.

Motion to Suppress

The appellant asserts that the military judge erred in denying her motion to suppress her personal e-mails sent and received via the Government computer network that were retrieved from the system's domain server. The appellant asks this court to reverse the military judge's denial of her motion to suppress the e-mails, set aside the findings of guilty and the sentence, and return the record of trial to the Judge Advocate General for a rehearing. We conclude that the military judge erred in admitting the e-mails, but also conclude that error did not materially prejudice the appellant's substantial rights, and, therefore, we decline to grant relief.

We review a military judge's 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). In doing so, we must determine whether the military judge's findings of fact are clearly erroneous or the conclusions of law are incorrect. *Id*. We review *de novo* the question of whether the military judge "correctly applied the law." *Id*. We are required to consider the evidence "in the light most favorable" to the "prevailing party." *United States v. Reister,* 44 M.J. 409, 413 (C.A.A.F. 1996). We have reviewed the military judge's findings of fact and, finding no clear error, we adopt them as our own. We turn then to the question of whether the military judge correctly applied the law.

The 4th Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." This protection has been applied to non-law enforcement Government officials through appellate case law. *O'Connor v. Ortega,* 480 U.S. 709 (1987)(public hospital administrators); *New Jersey v. T.L.O.,* 469 U.S. 325, 334 (1985)(public school officials); *Marshall v. Barlow's, Inc.*, 436 U.S. 307, 312-13 (1978)(regulatory inspectors). This protection extends beyond the traditional boundaries of private homes and persons and reaches into the workplace, including Government offices. *O'Connor*, 480 U.S. at 715-16.

In the instant case, the actions of the Government employees charged with administering the computer network are subject to the strictures of the 4th Amendment. There is also no doubt under the facts of this case that the actions of the network administrator in looking for, retrieving, and turning over the subject e-mails to law enforcement officials amounted to a

search. The administrator testified that there was no active and ongoing monitoring of the network at the time and that he specifically acted at the behest of law enforcement officials in retrieving the e-mails. He also testified that he knew he was looking for evidence of criminality, not evidence of misuse or abuse of the computer network.

Answering the question of whether those actions pass constitutional muster must begin with the question of whether this appellant has standing under the 4th Amendment to challenge the validity of the search. The appellant may challenge the validity of the search for evidence only if she can assert: (1) "a subjective expectation of privacy," and, (2) that the expectation of privacy is also "objectively reasonable," *United States v. Monroe,* 52 M.J. 326, 330 (C.A.A.F. 2000)(citing *Minnesota v. Olson,* 495 U.S. 91, 95 (1990)).

(1) Subjective Expectation of Privacy

The Supreme Court has ruled that an employee may have an expectation of privacy in the workplace vis-à-vis intrusion by law enforcement officials. *O'Connor,* 480 U.S. at 716. Such an expectation of privacy, however, may be limited by the practices and procedures of the employer, and any expectation of privacy in the workplace must be determined based on the facts presented in each case. *Id.* at 718. Among the factors to be considered in determining whether an expectation of privacy exists are: the amount of control the employee has over the area in question or the evidence seized; whether the employee took precautions to safeguard the privacy; and whether the employee could exclude others from the area or items of evidence. *United States v. Mendoza,* 281 F.3d 712, 715 (8th Cir. 2002).

On the other hand, many courts have held that if: (1) the employer owns and operates the computer network; (2) the employee uses the network to send and receive e-mails; and (3) the employee has been warned that the electronic information in the system is not confidential and may be viewed by network administrators and others, then the employee cannot claim an expectation of privacy as to his or her computer files. *Muick v. Glenayre Electronics,* 280 F.3d 741, 743 (7th Cir. 2002); *United States v. Simons,* 206 F.3d 392, 398 (4th Cir. 2000);) *United States v. Bailey,* 272 F.Supp.2d 822, 835 (D. Neb. 2003)(citing *United States v. Angevine,* 281 F.3d 1130 (10th Cir. 2002)); *Garrity v. John Hancock Mut. Life Ins. Co.,* 2002 U.S. Dist. LEXIS 8343 (D. Mass 2002); *Wasson v. Sonoma County Junior Coll.,* 4 F.Supp.2d 893 (N.D. Cal. 1997); *Monroe,* 52 M.J. 326. These cases focus on the area of work-related searches by employers. Other cases imply searches that are not work-related and those that are solely searches for evidence of a crime would require a showing of probable cause and a resulting search warrant or other lawful authorization. *O'Connor,* 480 U.S. at 721.

An expectation of privacy does not have to be an "all-or-nothing" idea. *Id*. at 717. An expectation of privacy also need not be an expectation that the subject item or information is completely private from all third-party knowledge. For example, the Court of Appeals for the Armed Forces (C.A.A.F.) has held that there is a limited expectation of privacy in messages sent or received via a private, non-governmental, internet provider. *United States v. Maxwell,* 45 M.J. 406, 418 (C.A.A.F. 1996). Such an expectation of privacy by an employee may, however, be limited by the practices and procedures of the employer. *O'Connor,* 480 U.S. at 717. The extent of the expectation of privacy will turn on the type of e-mail and internet provider involved, as well as the intended recipients. *Maxwell*, 45 M.J. at 418-19. Crucial to the issue of privacy in *Maxwell* was the fact that the internet provider had contractually agreed not to disclose its subscriber's e-mails to anyone other than authorized users of the network. *Id.* at 417. Finally, an employee's use of passwords to restrict access to computer files is evidence of a subjective expectation of privacy in those electronic records. *United States v. Slanina,* 283 F.3d 670, 676 (5th Cir. 2002), *vacated on other grounds*, 537 U.S. 802 (2002), *remanding*, 313 F.3d 891 (5th Cir. 2002).

The military judge made no explicit finding regarding whether the appellant had carried her burden to establish that she had a subjective expectation of privacy in her sent and received e-mails. The evidence presented at trial, however, established that the appellant's e-mail account was password protected and that she actively accessed and used the network. Thus, the appellant had nearly complete control over access to her e-mail account through user-generated passwords. The appellant's control was only limited by the administrator's role in monitoring and maintaining the Government computer network. The appellant's use of the password system provided precautions necessary to safeguard her privacy in her e-mails, as well as her ability to exclude others from her e-mail account.

The warning banner that the Government relies on in this case to establish that the appellant could have had no subjective or objective expectation of privacy focuses entirely on the issue of monitoring of the network. The banner is titled "Notice and Consent to Monitoring." After informing the user that this is a Government computer system, the banner states that such a system can be monitored for all lawful purposes, including looking for unauthorized use and protection of the system. The banner goes on to describe monitoring and states that information discovered during monitoring may be reproduced and used for "all authorized purposes." The banner also states that all information on the system is subject to monitoring, that any use of the system constitutes consent to monitoring, and the user may be prosecuted for unauthorized use of the system. Nowhere does the banner mention search and seizure of evidence of crimes unrelated to unauthorized use of a Government computer.

We find, based on the evidence adduced at trial, that the appellant held a subjective expectation of privacy in her e-mail account as to all others but the network administrator.

(2) Reasonable Expectation of Privacy

Having established that the appellant did have a subjective expectation of privacy in her e-mail account, we turn to whether or not that expectation of privacy was reasonable under the circumstances in this case. In other words, is this an expectation of privacy that the general public is willing to accept. *California v. Greenwood,* 486 U.S. 35, 39-40 (1988). The reasonableness of an employee's claim to an expectation of privacy may be undermined, however, by an employer's notification that electronic files and e-mail may be monitored. On the other hand, the courts have readily recognized that expectations of privacy vis-à-vis law enforcement are routinely reasonable.

Our superior court has determined that an authorized user of a Government computer network has no reasonable expectation of privacy in e-mails sent and received on that system from monitoring by personnel responsible for operating and maintaining the system. *Monroe,* 52 M.J. at 330. Left unanswered, however, is the question of whether the authorized user of a Government computer system may have a reasonable expectation of privacy in such e-mails from warrantless search and seizure by or on behalf of law enforcement.

In *Monroe,* the system administrators discovered evidence of criminal misconduct while monitoring the system for the cause of system slowdowns. The administrators properly notified law enforcement and turned over files they suspected contained pornography only after their inadvertent discovery during the routine actions of the administrators in monitoring and maintaining the network. *Monroe,* 52 M.J. at 328. The court cited to the statutory authority found in statutory protection of stored electronic communications, 18 U.S.C. §2702 (1999) and found that system administrators are permitted to turn over electronic evidence of a crime to law enforcement authorities if the evidence was discovered inadvertently by the service provider while maintaining or operating the computer network or system. *Id.* at 331.

In the instant case, there was no ongoing monitoring of the system in question when the e-mails were found and seized. The network administrator, acting solely at the request of law enforcement officials, went into the network server specifically looking for evidence of criminality in the e-mails sent or received by the appellant. The military judge concluded, however, that there was no "reasonable expectation of privacy" in the e-mail account and that "anyone who saw that banner on an ongoing basis would not believe that they had a reasonable expectation of privacy in any e-mails that were sent." Record at 101. We disagree.

The common foundation of the case law permitting warrantless, but reasonable, searches by non-law enforcement officials lies in their responsibility to effectively protect and operate the entity under their control. For example, a hospital administrator has the responsibility to ensure that the hospital staff is adhering to hospital regulations and to investigate allegations of work-related malfeasance and may authorize any reasonable search of hospital offices and property for evidence bearing on these issues without establishing probable cause and obtaining a search warrant. *O'Connor,* 480 U.S. at 725. Likewise, public school officials may conduct reasonable searches of students and their belongings without probable cause in furtherance of their charge to protect the student body and to ensure that forbidden activity such as drug use and cigarette smoking remain outside of the school boundaries. *T.L.O.,* 469 *U.S*. at 340. Finally, computer network administrators may reasonably search the networks under their care for the cause of malfunctions and for evidence of improper use of network systems without obtaining a search authorization based on probable cause. *Monroe,* 52 M.J. at 330.

Law enforcement involvement either prior to, or in the course of, the search, "changes the result for every case that has been reviewed." *Picha v. Wielgos,* 410 F.Supp. 1214, 1219 (N.D. Ill. 1976). As the *Picha* court stated so very well, "Where the police have significant participation, Fourth Amendment rights cannot leak out the hole of presumed consent to a search by an ordinarily non-governmental party." *Id.* (citing *Piazzola v. Watkins,* 316 F.Supp. 624 (M.D. Ala. 1970), *aff'd*, 442 F.2d 284 (5th Cir. 1971)).

For example, in a case involving the discovery of pornographic material by a commercial carrier as the result of an employee conducting a search of a package based on the suspicious actions of the sender, the reasonableness of an expectation of privacy turns on the degree of involvement by law enforcement:

> Where the search is made at the behest of or with the assistance of law enforcement officers, there must be probable cause, and in appropriate instances an authorizing warrant, if the search is to pass constitutional muster. But where the search is made on the carrier's own initiative for its own purposes, Fourth Amendment protections do not obtain for the reason that only the activities of individuals or nongovernmental entities are involved. So frequently and so emphatically have the courts enunciated and applied these principles that, at least for the time being they must be regarded as settled law.

United States v. Pryba, 502 F.2d 391, 398 (U.S. App. D.C. 1974). Also, in a case involving searches of students conducted by public school officials, the involvement of law enforcement

officials in instigating the search was critical in determining the students' limited expectation of privacy:

> However, no case can be found contradicting the notion that when a government official works with the police to conduct a search which is, at least in part, in the nature of a criminal investigation, and which occasions such an invasion of privacy as in the present case, that search is subject to the reasonableness of the Fourth Amendment.

Picha, 410 F.Supp. at 1220.

In the case at bar, the computer network system administrator maintains his unique status enabling him to conduct reasonable, but warrantless, searches of the Government network only so long as he remains independent of law enforcement. So long as he conducts his activities through ongoing system monitoring or confines his searches to those necessitated to ensure that the system is operating properly and that no user is abusing the system or using the system in an unauthorized manner, the system administrator can also properly turn over any evidence of criminal conduct to the authorities. Once he becomes the agent of law enforcement, however, either through conducting a search for criminal activity at their request or by permitting them to participate actively in his monitoring and administering function, he loses that special status afforded him under the law and becomes equally subject to the requirements of the 4th Amendment regarding probable cause and proper search authorization.

We conclude that it is reasonable, under the circumstances presented in this case, for an authorized user of the Government computer network to have a limited expectation of privacy in their e-mail communications sent and received via the Government network server. Specifically, while the e-mails may have been monitored for purposes of maintaining and protecting the system from malfunction or abuse, they were subject to seizure by law enforcement personnel only by disclosure as a result of monitoring or when a search was conducted in accordance with the principles enunciated in the 4th Amendment.

We conclude that the appellant had a subjective expectation of privacy in the e-mails sent and received on her Government computer vis-à-vis law enforcement and that this expectation of privacy was reasonable. The military judge therefore erred in denying the defense motion to suppress the e-mails at trial.

(3) Prejudice

The military judge's error in admitting the e-mails is subject to a "harmless error" review, where the appellant is entitled to relief unless the error is found to be "harmless beyond a reasonable doubt." *United States v. Simmons*, 59 M.J.

485, 489 (C.A.A.F. 2004)(quoting *Chapman v. California,* 386 U.S. 18, 24 (1967))(citing *United States v. Hall,* 58 M.J. 90, 94 (C.A.A.F. 2003)). The court in *Simmons* also defined the harmless error inquiry under the *Chapman* analysis as whether it is "beyond a reasonable doubt that the error complained of did not contribute to the verdicts obtained." *Id.* (quoting *Neder v. United States,* 527 U.S. 1, 15 (1999)).

The strictures of this standard and the case-by-case application of the *Chapman* analysis has been the subject of much appellate debate. In its 1967 holding, the Supreme Court in *Chapman* flatly rejected the proposition that all federal constitutional errors must be deemed harmful and relief afforded accordingly. *Chapman,* 386 U.S. at 21-22. In establishing a harmless error rule for such cases, the Court stated its preference for its own approach established in the case of *Fahy v. Connecticut,* 375 U.S. 85 (1963). In *Fahy*, the Court framed the question as "whether there is a reasonable possibility that the evidence complained of might have contributed to the conviction." *Id*. at 86-87. The Court in *Chapman* goes on to explain that an error "admitting plainly relevant evidence which possibly influenced the jury adversely to a litigant cannot, under *Fahy*, be conceived of as harmless." *Chapman,* 386 U.S. at 23-24.

The Court in *Chapman* concluded that there are "some constitutional errors which in the setting of a particular case are so unimportant and insignificant that they may, consistent with the Federal Constitution, be deemed harmless, not requiring the automatic reversal of the conviction." *Id*. at 22. To find harm, then, in the erroneous admission of any piece of relevant evidence would be to establish the very automatic error rule that *Faye* and *Chapman* endeavored to prevent.

In applying the harmless error analysis to the facts in *Chapman*, a case in which the error was comment on the petitioner's right not to testify at trial, the Court found that the prosecution "continuously and repeatedly" argued inferences to be taken from the failure of the petitioner to testify. *Id*. at 25. Also, the prosecution's case itself was based on circumstantial evidence. *Id*. In such a case, the Court found that, absent the erroneous comments of the prosecutor, "honest, fair-minded jurors might very well have brought in not-guilty verdicts." *Id*. at 26.

In 1991, the Supreme Court revisited the *Chapman* analysis in a case involving the erroneous admission at trial of coerced confessions. In *Arizona v. Fulminante,* 499 U.S. 279, 296 (1991), the Court made it clear that the Government has the burden of establishing that an error did not contribute to the conviction. In that case, the Court found that, without the confessions, it was "unlikely that Fulminante would have been prosecuted at all, because the physical evidence from the scene and other circumstantial evidence would have been insufficient to convict."

Id. at 297. The Court also found that the confessions influenced the sentencing phase of the trial. *Id*. at 301.

The Court in *Fulminante* distinguished between "trial error," an error in the presentation of the case to the jury that can be "quantitatively assessed in the context of other evidence presented in order to determine whether its admission was harmless," and an error in the structural defects in the trial itself, such as the right to an impartial judge. *Id*. at 307-09. In the case of a "classic `trial error[,]'" such as we have before us in the appellant's case, the Court in *Fulminante* concluded that the *Chapman* analysis involved more than simply finding that the evidence other than the involuntary confession would have been sufficient to sustain the verdict. *Id*. at 309.[1] In concluding that the admission of the coerced confessions was not harmless, the *Fulminante* Court stated that the appellate courts, when reviewing issues involving erroneous admission of evidence at trial, "simply review[] the remainder of the evidence against the defendant to determine whether the admission of the confession was harmless beyond a reasonable doubt." *Id*. at 310.

In *Neder,* 527 U.S. at 15-17, the Court found that the trial judge's failure to include an element of the offense in his jury instructions was error, but harmless under the *Chapman* analysis. The Court stated that, based on the overwhelming evidence of guilt, the verdict would have been the same without the judge's error and, because of that, the error "did not contribute to the verdict obtained." *Id*. at 17 (quoting *Chapman,* 386 U.S. at 24). The Court went on to express its belief that classic trial errors subject to the harmless error analysis necessarily "infringe on the jury's factfinding role and affect the jury's deliberative process in ways that are, strictly speaking, not readily calculable." *Id*. at 18. In other words, the Court recognized the fact that every piece of relevant evidence presented to a jury has an impact on the jury's deliberations. To make it clear that the *Chapman* analysis does not require reversal for every evidentiary error involving relevant evidence, the Court went on to say that such a high barrier would produce absurd results in cases where the remaining evidence of guilt is clear. *Id*.

The Court in *Neder* thus defined the *Chapman* analysis as follows: "Is it clear beyond a reasonable doubt that a rational jury would have found the defendant guilty absent the error?" *Id*.

Our superior court has described its focus in applying the *Chapman* harmless error analysis as "whether the error had or reasonably may have had an effect upon the members' findings." *United States v. Bins,* 43 M.J. 79, 86 (C.A.A.F. 1995). We cannot

[1] The Court in *Chapman* overturned their earlier holding in *Payne v. Arkansas,* 356 U.S. 560, 567 (1958) that an error in admitting evidence was harmless if the remaining evidence was sufficient, when standing alone, to support the verdict.

affirm findings in a case involving constitutional error "unless we determine beyond a reasonable doubt that the error did not contribute to the findings of guilty." *United States v. Hall,* 58 M.J. 90, 94 (C.A.A.F. 2003).

In *Simmons,* our superior court addressed an issue involving the erroneous admission of an illegally seized letter and the derivative videotape. The court found that the error could not be deemed harmless where the admission of the evidence may have had an impact on the defense strategy of having the appellant testify at trial regarding the information contained in the tainted evidence. *Simmons,* 59 M.J. at 491. In so holding, the court stated that the trial counsel referred to the illegally seized evidence "in the beginning, middle and end of his closing argument." *Id*. The court also found that the evidence in question was the "centerpiece" of the Government's case, as well as the only evidence aside from the appellant's testimony on the issue at trial. *Id*.

The e-mails in question in the instant case were damning evidence that corroborated the testimony of the Government's witnesses and undermined the testimony of the defense witnesses. As relevant evidence, there can be little doubt that the e-mails were considered by the members during deliberation. But further analysis is necessary to determine whether the e-mails contributed to the verdict of the members.

The witnesses for the Government were credible, uniform, and detailed in their testimony concerning the appellant's unlawful drug use. They also testified to admissions made by the appellant regarding her drug use. On the other hand, all the witnesses for the defense, with the exception of the informant, denied their own drug use while members of the Marine Corps. One was pending his own trial within a few weeks of the appellant's trial. All had significant motive to fabricate. The informant did not testify that the appellant had not used drugs, but rather that he had not seen the appellant using drugs.

Cpl U testified to verbal conversations with the appellant where she was discussing an upcoming urinalysis and appeared worried. She also admitted drug use during these conversations with Cpl U. We note that 10 of the 17 pages of the challenged e-mails, erroneously admitted by the military judge, are but a continuation of the discussion that occurred earlier in person with the appellant. Cpl U authenticated those pages as a string of e-mails and response e-mails between himself and the appellant. There is no claim or evidence in the motion to suppress the e-mails that Cpl U's testimony is derived from the discovery of the e-mails. Additionally, there was no objection to his testimony at trial or to the authentication of the e-mails.

Pages 1-9 of the challenged e-mails also contain discussions of the appellant's fear of detection as well as the techniques

for diluting her urine to avoid detection. The relevant evidence for the members derived from those pages is no different than the evidence provided in testimony and in the 10 pages of e-mails authenticated by Cpl U: namely, that the appellant displayed consciousness of guilt regarding her own drug use.

Based on the overwhelming evidence of guilt provided by the Government witnesses, we conclude, beyond a reasonable doubt, that the erroneous admission of Prosecution Exhibit 1 did not contribute to the verdict of the members in this case. *See Hall,* 58 M.J. at 95.

Conclusion

Accordingly, the findings of guilty and the sentence, as approved by the convening authority, are affirmed.

Chief Judge DORMAN and Judge REDCLIFF concur.

For the Court

R.H. TROIDL
Clerk of Court