UNITED STATES, Appellant and Cross-Appellee

v.

Jennifer N. LONG, Lance Corporal
U.S. Marine Corps, Appellee and Cross-Appellant

No. 05-5002

Crim. App. No. 200201660

United States Court of Appeals for the Armed Forces

Argued February 21, 2006

Decided September 27, 2006

GIERKE, C.J., delivered the opinion of the Court, in which EFFRON, BAKER, and ERDMANN, JJ., joined. CRAWFORD, J., filed a dissenting opinion.

Counsel

For Appellee and Cross-Appellant: Charles Gittins, Esq. (argued); Lieutenant Commander Jason S. Grover, JAGC, USN (on brief); Lieutenant Brian L. Mizer, JAGC, USN.

For Appellant and Cross-Appellee: Major Kevin C. Harris, USMC (argued); Commander Charles N. Purnell II, JAGC, USN (on brief); Colonel Ralph F. Miller, USMC.

Amicus Curiae for Appellee and Cross-Appellant: Stephanie Knott (law student) (argued); H. Brian Holland, Esq. (supervising attorney) and Patrick E. Tolan, Esq. (supervising attorney) (on brief) - for Barry University, Dwayne O. Andreas School of Law.

Military Judge: E. W. Loughran

Chief Judge GIERKE delivered the opinion of the Court.[1]

This case presents us with questions certified by the Judge Advocate General of the Navy regarding the reasonable expectation of privacy a military person has in e-mail messages sent and stored on a government computer system.[2] Lance Corporal Long, in a cross-petition, questions the holding by the lower court that the search and seizure violation it found was harmless beyond a reasonable doubt.[3] We conclude that based on

---

[1] Oral argument in this case was heard on February 21, 2006, at Barry University, Dwayne O. Andreas School of Law, in Orlando, Florida, as a part of this Court's "Project Outreach." See United States v. Mahoney, 58 M.J. 346, 347 n.1 (C.A.A.F. 2003). This practice was developed as part of a public awareness program to demonstrate the operation of a federal court of appeals and the military justice system.

[2] The Judge Advocate General of the Navy certified the following issues:

> I. WHETHER THE NAVY-MARINE CORPS COURT OF CRIMINAL APPEALS ERRED WHEN [IT] DETERMINED THAT, BASED ON THE EVIDENCE ADDUCED AT TRIAL, APPELLEE HELD A SUBJECTIVE EXPECTATION OF PRIVACY IN HER E-MAIL ACCOUNT AS TO ALL OTHERS BUT THE NETWORK ADMINISTRATOR.
>
> II. WHETHER THE NAVY-MARINE CORPS COURT OF CRIMINAL APPEALS ERRED WHEN [IT] DETERMINED 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 COMPUTER NETWORK SERVER.

[3] We granted the following issue submitted by Appellee and Cross-Appellant:

> WHETHER THE LOWER COURT ERRED IN FINDING THAT THE MILITARY JUDGE'S ERROR IN ADMITTING E-MAILS SENT AND RECEIVED BY LANCE CORPORAL LONG ON HER GOVERNMENT COMPUTER WAS HARMLESS BEYOND A REASONABLE DOUBT.

the particular facts of this case, Appellee[4] did have a subjective expectation of privacy in these e-mails, that her expectation of privacy was objectively reasonable, and that the error in admitting these e-mails was not harmless beyond a reasonable doubt.

FACTS

Appellee was charged with several specifications of unlawful drug use in violation of Article 112a, Uniform Code of Military Justice (UCMJ).[5] The Government's case was based, in part, on several e-mails that were sent and received by Appellee and that were retrieved from a government server. These e-mails contained statements written by Appellee indicating, among other things, a fear that her drug use would be detected by urinalysis testing and the steps she had taken in an attempt to avoid such detection.

At trial, the defense made a motion to suppress the e-mails because they were the result of a search which was not properly authorized. The military judge denied the motion holding that Appellee had no expectation of privacy in the e-mails stored on

[4] Lance Corporal Long is the Appellee on the certified issues and the Appellant on her cross-petition. For clarity we will refer to her as Appellee throughout this opinion. We will refer to her opponent as the Government.
[5] 10 U.S.C. § 912a (2000).

the government server. Contrary to her pleas, Appellee was convicted by members of the charged offenses.[6]

On appeal, Appellee challenged the ruling of the military judge on the motion to suppress her e-mails. The United States Navy-Marine Corps Court of Criminal Appeals disagreed with the military judge, holding that the search was unlawful, but further concluding that the error in admitting the e-mails was harmless beyond a reasonable doubt.[7]

EVIDENCE ON THE MOTION TO SUPPRESS

Mr. Flor Asesor, the Senior Network Administrator for the government computer network, was the sole witness to testify on the motion. He testified that Captain Fitzharris, an investigator for the Marine Corps Inspector General, was looking for evidence of misconduct.[8] Captain Fitzharris told Mr. Asesor to retrieve the e-mails from Appellee's e-mail account. Mr. Asesor retrieved her e-mails which had been stored on the government server and provided them to Captain Fitzharris.

---

[6] Appellee was sentenced to confinement for two months, reduction to the lowest enlisted pay grade and a bad-conduct discharge. The convening authority approved the sentence as adjudged.

[7] United States v. Long, 61 M.J. 539, 546, 549 (N-M. Ct. Crim. App. 2005).

[8] Although there is no evidence in the trial transcript explaining the nature of Captain Fitzharris's investigation, there are averments in the prosecution trial brief on the motion to suppress indicating that the investigation involved allegations of an improper relationship between Appellee and an officer. Although the details are not clear, the military judge's finding of fact that Captain Fitzharris was searching for evidence of misconduct is fully supported by the testimony of Mr. Asesor.

The Court of Criminal Appeals found that the e-mails were retrieved as the result of a specific request by law enforcement officials[9] and concluded that "[t]here 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."[10] These findings and conclusions are consistent with the finding by the military judge that this was a "search for evidence" and the Government's concessions in their brief and oral argument before this Court. Mr. Asesor authenticated Appellate Exhibit XIII, a log-on banner which appeared anytime a user logged onto his or her office computer. This banner contained the following information:

> 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,

[9] Id. at 541.
[10] Id. at 543.

> criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

Mr. Asesor also explained that each individual user of the computer system had his or her own unique password known only to them. Users were required to change their password every ninety days. As the network administrator, Mr. Asesor did not have access to user passwords, and the only way he could access individual accounts was to lock the individual user out of the account. As the network administrator, Mr. Asesor was able to access the entire network or any part of it, including personal e-mails sent by individual users such as Appellee.

He testified that in conducting the monitoring described in the banner, it was general policy to avoid examining e-mails and their content because it was a "privacy issue." Mr. Asesor indicated that the examination and seizure of the e-mails in this case were not related to the monitoring program and were not the result of concerns about a security violation or unauthorized use. Instead, he conceded that they were retrieved as a part of a search for evidence of misconduct.

Based on these facts, the military judge denied the motion to suppress. He concluded that this was a search for evidence; there was not actual consent by the accused to this search; and there was no search authorization issued by a commander. The linchpin of the military judge's ruling was that Appellee had no reasonable expectation of privacy in the e-mail account. In

explaining his conclusion, the military judge stated, "I find 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."

THE COURT OF CRIMINAL APPEALS DECISION

The Navy-Marine Corps Court of Criminal Appeals examined the case and concluded that the military judge should have suppressed the e-mails.[11] The court held that Appellee had a reasonable expectation of privacy in the e-mails sent and received on her government computer.[12] The court further indicated that the banner relied upon by the military judge to find no privacy expectation may have limited Appellee's expectation of privacy with regard to non-law enforcement monitoring of the computer system, but that the seizure of the e-mails in this case was for law enforcement purposes.[13] The court then tested the error for prejudice and ultimately concluded that the error was harmless beyond a reasonable doubt.[14]

DISCUSSION

The Fourth Amendment of the Constitution protects individuals, including servicemembers, against unreasonable

[11] Long, 61 M.J. at 546.
[12] Id.
[13] Id.
[14] Id. at 546-49.

searches and seizures.[15] We have described a search as an official governmental intrusion into an individual's reasonable expectation of privacy.[16] Whether such an expectation of privacy exists is therefore a question in any search and seizure analysis. The question is resolved by examining whether the individual challenging the alleged intrusion had a subjective expectation of privacy which was objectively reasonable.[17] If such an expectation is established, the inquiry then moves to the remaining issues raised by the Fourth Amendment.

Official intrusions into protected areas in the military require search authorization supported by probable cause, unless they are otherwise lawful under the Military Rules of Evidence (M.R.E.) or the Constitution of the United States as applied to members of the armed forces.[18]

The determination of the reasonableness of an expectation of privacy, "is understood to differ according to context."[19] The present case involves a military member's claimed expectation of privacy in e-mails sent and received on a government computer. The Supreme Court has recognized that in the context of the government workplace, employees may have a

[15] United States v. Daniels, 60 M.J. 69, 70 (C.A.A.F. 2004).
[16] Id. at 71.
[17] Minnesota v. Olson, 495 U.S. 91, 95-96 (1990); United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000).
[18] See M.R.E. 314(k).
[19] O'Connor v. Ortega, 480 U.S. 709, 715 (1987) (plurality opinion).

reasonable expectation of privacy against certain intrusions.[20] However, "[p]ublic 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."[21] The rationale for this suggestion is the "efficient and proper operation of the agency."[22] Thus, an "employee's expectation of privacy must be assessed in the context of the employment relation."[23]

If the practices of the workplace establish an environment where the employee enjoys no reasonable expectation of privacy, the underlying search and seizure issue is easy to resolve. In such a situation the protections of the Fourth Amendment would simply not apply. If an expectation of privacy is supported by the workplace environment, however, the analysis must continue. The Supreme Court instructs us that, in the government workplace, a reasonable expectation of privacy may not provide the employee with complete Fourth Amendment protection. The Supreme Court, in O'Connor, concluded that the need for a search warrant based on probable cause was not required for legitimate workplace searches conducted by supervisors.[24] Instead, "[P]ublic employer intrusions on the constitutionally protected

[20] Id. at 716.
[21] Id. at 717.
[22] Id. at 723.
[23] Id. at 717.
[24] Id. at 725.

privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances."[25] This conclusion was based on the Supreme Court's recognition that "[W]hile police, and even administrative enforcement personnel, conduct searches for the primary purpose of obtaining evidence for use in criminal or other enforcement proceedings, employers most frequently need to enter the offices and desks of their employees for legitimate work-related reasons wholly unrelated to illegal conduct."[26]

O'Connor, therefore, presents two situations where employer searches into zones of privacy are legitimate even if not supported by normal Fourth Amendment warrant and probable cause requirements. The first exception is where the search is for noninvestigatory, work-related purposes. The second is if the search by the employer is investigatory but involves matters of workplace misconduct. In either of these situations the search is evaluated using the standard of reasonableness based on all the surrounding facts and circumstances.[27] When the reasonableness standard is applicable, the government must establish: (a) that the search "was justified at its

[25] Id. at 725-26.
[26] Id. at 721.
[27] Id. at 725-26.

inception"; and (b) that the conduct of the investigation was "reasonably related in scope to the circumstances which justified the interference in the first place."[28]

We must note that the military workplace is not the usual workplace envisioned by the Supreme Court in O'Connor. The military workplace can range from an office building to a bunker or tent in a combat zone. Similarly, military leaders and their subordinates are different than civilian public officials and their employees. Military commanders have authority and powers not possessed by civilian employers. Military commanders, for example, can authorize searches of their personnel,[29] order them confined,[30] and bring criminal charges against them.[31] Military personnel operate in a system that provides criminal sanctions for workplace misconduct.[32] Accordingly, we need to keep these unique aspects of the military environment in mind whenever we apply the O'Connor decision to workplace searches.

As this is a case certified to this Court by the Judge Advocate General of the Navy, we will focus our analysis on the questions certified. We therefore turn to the ultimate question presented: did Appellee have a reasonable expectation of

[28] Id. at 726 (citations and quotation marks omitted).
[29] M.R.E. 315(d)(1).
[30] Article 9, UCMJ, 10 U.S.C. § 809 (2000).
[31] Articles 22, 23, and 24, UCMJ, 10 U.S.C. §§ 822, 823, 824 (2000).
[32] See, e.g., Article 86, UCMJ, 10 U.S.C. § 886 (2000), which provides criminal sanctions for what would be addressed through administrative measures in the civilian workplace.

privacy in the e-mail communications sent and received via the Headquarters, Marine Corps (HQMC) computer network server?

As noted, in examining Fourth Amendment privacy interests, the courts look first to whether the individual had a subjective expectation of privacy.[33] If the courts ascertain that a subjective expectation of privacy exists, they then determine if that expectation is one that society is prepared to accept as reasonable.[34]

The first question is one of fact, which is reviewed using a clearly erroneous standard.[35] The second is one of law, which we review de novo.[36] In this case the military judge did not differentiate between the subjective and objective expectations of privacy. Instead, he simply concluded that there was no expectation of privacy. For purposes of our discussion, we will assume that the military judge found that any subjective expectation of privacy held by Appellee was not objectively reasonable and will review that determination de novo.

THE SUBJECTIVE EXPECTATION OF PRIVACY

This Court previously considered military members' subjective expectations of privacy in Maxwell[37] and Monroe.[38] In Maxwell, the accused used America Online's (AOL) e-mail service

[33] Olson, 495 U.S. at 95-96; Monroe, 52 M.J. at 330.
[34] Ortega, 480 U.S. at 715.
[35] United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996).
[36] United States v. Reister, 44 M.J. 409, 413 (C.A.A.F. 1996).
[37] 45 M.J. at 417-19.
[38] 52 M.J. at 330.

to communicate with another junior Air Force officer about the accused's sexual interests and to send and receive obscene material and child pornography.[39] This Court concluded that Maxwell possessed a subjective expectation of privacy where it was AOL's policy to offer "contractual privacy protection," including nondisclosure of e-mail without a court order.[40]

In Monroe, this Court concluded that, in contrast to Maxwell, the e-mail system in question was owned by the government.[41] We noted that Monroe's subjective expectation of privacy was not governed by contractual agreement, as in Maxwell, and we concluded that, based on the totality of the circumstances, Monroe had no expectation of privacy, at least from persons maintaining the electronic mail host system.[42]

In making the case that she had an expectation of privacy, Appellee argues that access to her computer and therefore her e-mail account was protected by a password known only to her. Indeed, the network administrator testified that he did not know her password.

In response to the argument that Appellee's password created an expectation of privacy, the Government points out that the passwords are required as a part of the government computer security concerns in order to limit unauthorized access

[39] 45 M.J. at 414.
[40] Id. at 417.
[41] 42 M.J. at 330.
[42] Id.

to the government system. Accordingly, the Government concludes that passwords protect governmental interests, not individual privacy concerns.

The Government relies most heavily on the log-on banner to support its notion that Appellee could not have believed her e-mail communications were private. The Government argues that courts have looked at similar warnings and policies, and found them sufficient to establish that the employee had no expectation of privacy.[43] Conversely, Appellee argues that the language of the banner is not sufficient to remove her expectation of privacy from unreasonable, warrantless searches conducted for law enforcement purposes.

In light of the particular facts of this case, we conclude that the lower court was not clearly erroneous in its determination that Appellee had a subjective expectation of privacy in the e-mails she sent from her office computer and in the e-mails that were stored on the government server.

We conclude that the testimony of the network administrator is the most compelling evidence supporting the notion that Appellee had a subjective expectation of privacy. Mr. Asesor repeatedly emphasized the agency practice of recognizing the privacy interests of users in their e-mail. The fact that

[43] See United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000); United States v. Angevine, 281 F.3d 1130, 1135 (10th Cir. 2002).

Appellee had a password known only to her, supports Mr. Asesor's testimony regarding the attitude toward privacy and the lower court's conclusion that Appellee had a subjective expectation that access to her e-mails was protected and severely limited. Her subjective expectation was not diminished by the fact that the password may also have served certain governmental interests. The language of the log-on banner also confirms the privacy interests testified to by Mr. Asesor. The banner described access to "monitor" the computer system, not to engage in law enforcement intrusions by examining the contents of particular e-mails in a manner unrelated to maintenance of the e-mail system. In summary, we find that the password and the language of the banner, in light of Mr. Asesor's testimony, support the lower court's conclusion that Appellee met her burden of demonstrating a subjective expectation of privacy.

THE REASONABLENESS OF THE PRIVACY EXPECTATION

In O'Connor, the Supreme Court recognized that there may be an expectation of privacy in a government workplace but that there is no talisman for determining the reasonableness of such an expectation in cases involving public employees.[44] Instead, the reasonableness of a privacy expectation will differ according to the context, and the "operational realities of the

[44] 480 U.S. at 715.

workplace."[45] M.R.E. 314 discusses searches not requiring probable cause, and subsection (d) of M.R.E. 314 deals specifically with searches of government property. M.R.E. 314(d), which is consistent with the holding in O'Connor, indicates that searches of government property may be made without probable cause unless an individual has a reasonable expectation of privacy in that property and that the determination of the reasonableness of an expectation of privacy "depends on the facts and circumstances at the time of the search."

The e-mails seized in this case were originally prepared in an office in HQMC on a computer owned by the Marine Corps and issued to Appellee. They were transmitted over the HQMC network system, stored on the HQMC server, and retrieved by the HQMC network administrator. Each of those factors might arguably fit a situation where society would be unwilling to recognize an individual expectation of privacy.[46] Other evidence in this case, however, convinces us that Appellee's subjective expectation of privacy in these e-mails is one that society is prepared to accept as reasonable.

We consider the testimony of Mr. Asesor, the network administrator, describing the agency practices and policies to be most persuasive. We look to office practices because the

[45] Id. at 717.
[46] See Bond v. United States, 529 U.S. 334, 338 (2000).

Supreme Court in O'Connor indicated that privacy expectations in the workplace may be reduced by virtue of office practices, procedures, or regulation.[47] In this case, the policies and practices of HQMC reaffirm rather than reduce the expectations regarding privacy on office computers. These policies, among other things, require individual users to have passwords known only to themselves and to change their passwords periodically to ensure privacy. Additionally, these policies limit outside network access to the network administrator and describe very limited conditions under which he would monitor the network for unauthorized use.

The testimony of the Government's witness about policies and practices is strong evidence that Appellee's subjective expectation of privacy was objectively reasonable. Mr. Asesor explained that HQMC's policy regarding using the network to send personal e-mails had always been lenient and that such use of the network was considered authorized. Mr. Asesor further testified that when doing the testing and monitoring of the network, he did not monitor individual accounts because "it's a privacy issue."

This Court in Monroe held that a military member did not have a reasonable expectation of privacy with respect to the

[47] 480 U.S. at 717.

content of e-mail messages.[48] In Monroe, we held that the appellant, despite any subjective expectation of privacy, had no objectively reasonable expectation of privacy because the incriminating e-mails were discovered as part of the routine monitoring described in the log-on banner message in use.[49]

The totality of the circumstances in this case leads us to conclude that, unlike in Monroe, Appellee's expectation of privacy was objectively reasonable. The HQMC log-on banner explained that the network administrator had access to Appellee's computer as a "monitoring" function. The e-mails retrieved in this case were from Appellee's account on an unclassified government computer system on which she was authorized limited personal use and were not obtained for maintenance or monitoring purposes. Mr. Asesor testified that prior to accessing Appellee's e-mail account, he had no information based on his previous monitoring that she was using her account in an unauthorized manner. As noted, Mr. Asesor further testified that he retrieved Appellee's e-mails to look for evidence of misconduct. If Mr. Asesor had been doing the monitoring described in the log-on banner when he came across Appellee's incriminating e-mails, this case would fall within the parameters of O'Connor and Monroe, thus presenting a different analytic framework and potentially a different result.

[48] 52 M.J. 330.
[49] Id.

Instead, Mr. Asesor confirmed that the sole purpose of seizing the e-mails was to search for evidence of misconduct. Accordingly, this case is not like Monroe where the incriminating e-mail evidence was found inadvertently by personnel performing routine systems maintenance described in the log-on banner. To the contrary, the evidence seized in this case was done so as a part of a search for law enforcement purposes.[50]

The result we reach in this case is not inconsistent with other federal court decisions that have considered similar situations and found no privacy expectation. In Simons,[51] the court was dealing with a very different, very specific policy regarding use of the computer system. In Simons the Internet policy both restricted use, including e-mail use, to official government business and indicated to employees that ongoing use of the system was subject to audit and inspection.[52] In the present case, however, Appellee was authorized to use the government computer for personal use and the banner described a less intrusive monitoring program directed to unauthorized use. In Angevine, the log-on banner expressly informed the employee that e-mail messages "contain no right of privacy or

[50] See Long, 61 M.J. at 541.
[51] 206 F.3d at 396.
[52] Id.

confidentiality."[53] The banner in the instant case did not provide Appellee with notice that she had no right of privacy. Instead, the banner focused on the idea that her use of the system may be monitored for limited purposes.

Based on our review of precedent and the totality of the circumstances in this case, we conclude that while the log-on banner may have qualified Appellee's expectation of privacy in her e-mail, it did not extinguish it. Simply put, in light of all the facts and circumstance in this case, the "monitoring" function detailed in the log-on banner did not indicate to Appellee that she had no reasonable expectation of privacy in her e-mail.

Based on this evidence, we conclude that Appellee's expectation of privacy was, in fact, recognized as reasonable by virtue of the rules, regulations, practices, and procedures of HQMC. Accordingly, her subjective expectation of privacy was one which society is prepared to recognize as reasonable.

THE EXPECTATION OF PRIVACY –- CONCLUSION

The fact that the seizure of Appellee's e-mails in this case was solely for law enforcement purposes is not in dispute. While government employers may need to enter an employee's office space or intrude into an employee's computer or e-mail account for work-related reasons, searches conducted for the

[53] 281 F.3d at 1133 (emphasis added).

primary purpose of obtaining evidence of illegal conduct require probable cause.[54] As this search went beyond work-related monitoring or an investigatory search of work-related misconduct, it was not one exempt from the probable cause requirement. Thus, to be admissible, the evidence obtained in the search must have been pursuant to authorization.[55] Because there was no command authorization, the evidence should have been suppressed.[56]

HARMLESS ERROR

After concluding that the search was unreasonable and that Appellee's e-mails should have been suppressed, the Court of Criminal Appeals determined that the error was harmless beyond a reasonable doubt.[57] Appellee, in her cross-appeal, takes issue with this conclusion.

---

[54] O'Connor, 480 U.S. at 724.
[55] See M.R.E. 314; M.R.E. 315.
[56] Even if this had been an intrusion for noninvestigatory, work-related purposes or an investigation of work-related misconduct which, under O'Connor, would have been measured by a reasonableness standard, the Government would still fail. O'Connor requires the government to demonstrate reasonableness by showing that: (a) the search "was justified at its inception"; and (b) the conduct of the investigation was "reasonably related in scope to the circumstances which justified the interference in the first place." 480 U.S. at 726 (citations and quotation marks omitted). In the case at bar, the Government presented no evidence on either question and relied solely on the argument that Appellee had no reasonable expectation of privacy.
[57] Long, 61 M.J. at 546-49 (citing United States v. Simmons, 59 M.J. 485, 489 (C.A.A.F. 2004); Neder v. United States, 527 U.S. 1, 15 (1999)).

After reviewing all the evidence, we agree with Appellee. The lower court concluded that the witnesses for the Government were "credible, uniform, and detailed in their testimony regarding the appellant's unlawful drug use,"[58] which was in sharp contrast to the defense witnesses whom the lower court found to be less than credible because they all had "significant motive to fabricate."[59]

Although the lower court's skepticism regarding the credibility of the defense witnesses may be well founded, there are substantial reasons why one might be equally skeptical of the credibility of the Government witnesses. The prosecution witnesses were all admitted drug users who had incentives to testify for the Government in this case. Additionally, they were all potential accomplices and the court members were instructed by the military judge that their testimony should therefore be viewed with great caution.

Perhaps most important to our determination of the harmless error issue is trial counsel's reliance on the e-mails in his presentations to the court members. Trial counsel ended his opening statement referring to the importance of those e-mails because they were Appellee's own account of her worries and fears about upcoming urinalysis testing.

[58] Id. at 548.
[59] Id.

Similarly, the subject of Appellee's e-mails was emphasized in trial counsel's closing argument. In discussing the members' task of evaluating the evidence, trial counsel explained that the evaluation is made much easier by the e-mails, which contain Appellee's own words. He then proceeded to read from several of the e-mails and concluded by saying: "Gentlemen, I submit to you, if there was anything even resembling reasonable doubt, those e-mails should pretty much clear that up."

Whether error is harmless beyond a reasonable doubt is a question of law reviewed de novo.[60] The burden is on the Government to show whether "it appears beyond a reasonable doubt that the error complained of did not contribute to the verdict obtained."[61]

In Simmons, we concluded that the error in admitting certain evidence was not harmless beyond a reasonable doubt when trial counsel in that case "referred to the illegally seized letter in the beginning, middle, and end of his closing argument."[62] We are faced with almost identical facts in this case, where constitutionally inadmissible evidence was a

[60] Chapman v. California, 386 U.S. 18, 24 (1967); Arizona v. Fulminate, 499 U.S. 279 (1991).
[61] Mitchell v. Esparza, 540 U.S. 12, 16 (2003) (per curiam) (quoting Neder, 527 U.S. at 15 (quotation marks omitted); see also United States v. Hall, 58 M.J. 90, 94 (C.A.A.F. 2003); Simmons, 59 M.J. at 489.
[62] Simmons, 59 M.J. at 491.

cornerstone of trial counsel's opening statement and his closing argument.

Trial counsel obviously felt that the e-mails were very important to his case. We agree. Accordingly, we cannot conclude that the erroneous admission of the e-mails was harmless beyond a reasonable doubt.

CONCLUSION

The certified questions are answered in the negative: the United States Navy-Marine Corps Court of Criminal Appeals did not err when it found that Appellee had a subjective expectation of privacy in her e-mail communications. Further, we hold that the lower court did not err when it concluded that Appellee's privacy expectation was reasonable. Because we are not convinced that the error in admitting the e-mail communications was harmless beyond a reasonable doubt, we decide the granted issue in favor of Appellee. Accordingly, the findings and sentence are set aside. The record of trial is returned to the Judge Advocate General of the Navy. A rehearing is authorized.

CRAWFORD, Judge (dissenting):

I respectfully dissent from the majority's holding that despite the Department of Defense (DoD) log-on banner and Appellee's consent to monitoring, she had both the subjective and objective expectation of privacy in e-mails seeking advice from her friends regarding concealing her drug use. This case impacts on the DoD policy as set forth in the banner. "DoD computer systems may be monitored for all lawful purposes . . . . Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system." This banner, which appears on nearly all DoD systems, constitutes consent to monitoring. See Scott A. Sundstrom, You've Got Mail! (And the Government Knows It): Applying the Fourth Amendment to Workplace E-mail Monitoring, 73 N.Y.U. L. Rev. 2064, 2090 (1998) (citing Scot L. Gulick, Memorandum from Office of General Counsel to All Computer Users, The Standards of Ethical Conduct (United States Department of Defense), Sept. 1997, at 1). Our analysis should determine whether there is coverage and protection under the Fourth Amendment.* See, e.g.,

* Since 1960, this Court has held that the Bill of Rights applies to servicemembers "except those [rights] which are expressly or by necessary implication inapplicable." United States v. Jacoby, 11 C.M.A. 428, 430-31, 29 C.M.R. 244, 246-47 (1960); cf. Davis v. United States, 512 U.S. 452, 457 n.* (1994) (Supreme Court has "never had occasion to consider whether Fifth Amendment privilege . . . applies of its own force to the military . . . ."); United States v. Taylor, 41 M.J. 168, 171

Taylor, 41 M.J. at 170. The question hinges on whether Appellee had a subjective and objectively reasonable expectation of privacy. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). If there is, what protection does Appellee deserve?

In United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000), we held that a defendant does not have an expectation of privacy in his e-mail, "at least from the personnel charged with maintaining the EMH [electronic mail host] system." We left open the issue presented in this particular case. Here the Government banner removes any subjective or objective expectation of privacy by requiring all employees to consent to monitoring before they may use their computers. See Wyman v. James, 400 U.S. 309, 318-24 (1971)(notice to welfare benefits recipient was factor in determining no violation of the Fourth Amendment).

The majority mistakenly believes that an objective reasonable expectation of privacy can be preserved for some forms of seizure despite being nonexistent for others. The majority cites no legal authority to support this position. Once Appellee was given notice of and consented to monitoring of

---

(C.M.A. 1994) (application of Bill of Rights "is not only of academic importance, but also it is important to the President in deciding what rules should be applied to the military").

any kind, she could not maintain a reasonable expectation of privacy against other forms of intrusion. As the Supreme Court writes, "'Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the . . . information . . . .'" Georgia v. Randolph, 126 S. Ct. 1515, 1534 (2006) (quoting United States v. Jacobsen, 466 U.S. 109, 117 (1984)). Knowledge of actual monitoring negates any reasonable expectation of privacy. See United States v. Hatcher, 323 F.3d 666, 674 (8th Cir. 2003) (holding prisoners and their attorneys had no reasonable expectation of privacy since they knew their conversations were being recorded); United States v. Madoch, 149 F.3d 596, 602 (7th Cir. 1998) (no spousal privilege when communicating to an inmate, knowing that inmate communications are monitored). Appellant in the present case was aware of and consented to the monitoring and archiving of electronic communications originating from her government computer. She therefore could not have a reasonable expectation of privacy in those communications. That the communications were obtained specifically for law enforcement purposes has no bearing on her expectation of privacy.

The majority cuts too fine a line in trying to distinguish applicable federal precedent based on the wording of the banner. The majority states that United States v. Angevine, 281 F.3d

1130, 1133 (10th Cir. 2002), is not applicable because in that case, the banner included the explicit term, "contain no right of privacy or confidentiality." While a rewording of subsequent DoD Internet usage banners may be advisable, the language of the banner at issue here leaves no doubt as to its invasiveness: "All information, including personal information, placed on or sent over this system may be monitored." The majority seems to think that the average servicemember would not understand the plain meaning of that sentence without the magical phrase "no expectation of privacy." This conclusion is disconcerting. The majority ignores a number of other cases with less specific banner language where the courts found no reasonable expectation of privacy. See Kaufman v. SunGard Inv. System, No. 05-CV-126(JLL), 2006 U.S. Dist. LEXIS 28149, at *12, 2006 WL 1307882, at *4 (D.N.J. May 9, 2006)(letter-opinion and order); Muick v. Glenayre Elec., 280 F.3d 741, 743 (7th Cir. 2002); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000). The purpose of the banner was to give notice that computer activity would be monitored, and as imprecise as it may be, the language of the banner unambiguously conveyed that message.

The majority also attempts to distinguish Simons based on the "very specific policy regarding use of the computer system" in that case. This is a distinction that should not be made. As stated above, a reasonable expectation of privacy is not

divisible. The majority refuses to directly acknowledge applicable federal precedent on this issue. In doing so, they ignore a clear trend in the federal courts that there is no expectation of privacy in situations, like this one, where there is a DoD banner clearly announcing a departmental monitoring policy. When an employee knows that an employer is monitoring his or her e-mail, there cannot be a reasonable expectation of privacy, especially when the employee is notified each time that logging on constitutes consent to monitoring.

The court noted in Simons, 206 F.3d at 398, that "office practices, procedures, or regulations may reduce legitimate privacy expectations." Likewise, in Angevine, 281 F.3d at 1134, the court held that a university professor had no expectation of privacy to files erased on his computer because the university's "policy explicitly cautions computer users that information flowing through the University network is not confidential either in transit or storage on a University computer." Thus, university users were aware that administrators and others had free access to the downloaded Internet material. The court held that deleting the files "was not sufficient to establish a reasonable expectation of privacy." Id. at 1135. "[G]iven the absence of the city policy placing [defendant] Slanina on notice that his computer use would be monitored and the lack of any indication that other employees had routine access to his

computer, we hold that Slanina's expectation of privacy was reasonable." United States v. Slanina, 283 F.3d 670, 677 (5th Cir. 2002), vacated on other grounds by 537 U.S. 802 (2002).

In United States v. Bailey, 272 F. Supp. 2d 822, 835-36 (D. Neb. 2003), the court held that a defendant had no reasonable expectation in his computer at his civilian work site which had a log-on banner. The log-on banner stated:

> These computer resources are solely owned by the Company. Unauthorized access or use is a violation of federal law and could result in criminal prosecution. Users agree not to disclose any company information except as authorized by the company. Your use of this computer system is consent to be monitored and authorization to search your personal computer to assure compliance with company policies.

Id. at 831. The company's policy available to the workers said:

> It is critical that all agents, employees, suppliers and vendors understand these information security policies and comply with them when accessing and using American Family's electronic resources. All of us -- as individuals and as a Company -- will be held accountable for knowing and adhering to these policies. Each of us as individuals and as a Company can be held liable for failing to comply with these policies.

Id. at 832.

Additionally, the company policy posted on the Intranet site explained that while personal use of computers was not prohibited, it could not be used for unlawful purposes, and the workers had "no expectation of privacy associated with the

information they store in or send through these systems." Id. at 832, 836. As to the expectation of privacy, the court stated:

> Absent a legitimate and constitutionally protected expectation of privacy in e-mail files, defendant cannot successfully assert a Fourth Amendment violation. United States v. Bach, 310 F.3d 1063, 1066 (8th Cir. 2002). Factors relevant to determining if a legitimate expectation of privacy exists include ownership, possession and/or control of the area searched or item seized; the defendant's historical use of the property or item; whether the defendant can exclude others from that place; whether he took precautions to maintain the privacy; and whether the defendant had a key to the premises.

Id. at 834-35.

The fact that an individual has a password does not change the expectation of privacy. Garrity v. John Hancock Mut. Life Ins. Co., No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343, at *5-*6, 2002 WL 974676, at *2 (D. Mass. May 7, 2002); see also Bailey, 272 F. Supp. 2d at 835-37 (the facts, including "employer's notice [that] . . . internet use[] and e-mail may be monitored," undermine[] an employee's claim that the information was private and "any expectation of privacy that the employee has is not one that society is willing to accept and protect"). In Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996), the court indicated that an employee has no reasonable expectation of privacy in e-mail because "the company's interest in preventing inappropriate and unprofessional comments or even

illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments."

The majority improperly uses Appellee's authorization for personal use of her e-mail account to support their finding of a reasonable expectation of privacy. However, her personal account was her work account and Appellee's communications fall within the scope of work-related communications. Appellee discussed her diminished ability to perform her job as well as her appearance at work in e-mails sent to Ms. KS between 9:46 a.m. and 1:07 p.m. on August 15, 2000, the day of her urinalysis test. The times the e-mails were sent indicate that they were sent while she was at work. The systems administrator testified that the e-mail accounts were "authorized specifically for doing your job within DOD" and that personal use is something they have been "lenient on allowing." The distinction between a work-related e-mail and e-mail unrelated to work would be difficult, if not impossible, to make in many instances.

The perception of one administrator in a department as large as the DoD, with over 2.5 million servicemembers, excluding civilians, is not binding on the department itself. The belief of an administrator is even more attenuated considering how computers are used on the job. Cf. United States v. Muniz, 23 M.J. 201, 206 (C.M.A. 1987) ("[W]e note that the credenza, like any other item of Government property within

the command, was subject at a moment's notice to a thorough inspection. That omnipresent fact of military life, coupled with indisputable government ownership and the ordinarily nonpersonal nature of military offices, could have left appellant with only the most minimal expectation -- or hope -- of privacy." (citation omitted)).

As the United States Court of Appeals for the Ninth Circuit stated in United States v. Ziegler, 456 F.3d 1138, 1146 (9th Cir. 2006), "Employer monitoring is largely an assumed practice, and thus we think a disseminated computer-use policy is entirely sufficient to defeat any expectation that an employee might nonetheless harbor." Every time Appellee turned on her computer, she was aware of the computer-use policy of her service and could not have a reasonable expectation of privacy.

While the Supreme Court has not heard an e-mail case, the Supreme Court's expectation of privacy approach applies. Certainly, the possibility of exposure to the public eye diminishes or alleviates one's expectation of privacy, and undoubtedly when one is so warned of monitoring, there is no expectation of privacy. Just as the Supreme Court indicated, there is no reasonable expectation of privacy in numbers dialed on a telephone because "[w]hen he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the

ordinary course of business." Smith v. Maryland, 442 U.S. 735, 744 (1979), superseded by statute, Electronic Communications Privacy Act of 1986, 18 U.S.C. § 3121(a) (2000). Similarly, as to business records, the Supreme Court indicated that financial statements and deposit slips are "voluntarily conveyed to the banks and exposed to their employees." United States v. Miller, 425 U.S. 435, 442 (1976), superseded by statute, Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401 (2000), as recognized in SEC v. Jerry T. O'Brien Inc., 467 U.S. 735, 745 (1984). Based on the hierarchy as to sources of rights, a statute can grant more rights than the Fourth Amendment. See United States v. Lopez, 35 M.J. 35, 39 (C.M.A. 1992). Thus, there is no expectation of privacy. Miller, 425 U.S. at 443-44.

One "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government," id. at 443, thus providing a basis for the conclusion that the subscriber lacks an expectation of privacy in communications held by a service provider, especially when there is a log-on notice and no statutory protection.

Even when there is a reasonable expectation of privacy, one of the exceptions is consent to search. Consent is such that one would not rely upon an assumption of risk that the service provider would not reveal this information to law enforcement officials. Hoffa v. United States, 385 U.S. 293, 302-03 (1966).

Likewise, in Lopez v. United States, 373 U.S. 427, 465 (1963), the Supreme Court acknowledged that a conversation surreptitiously recorded by a government agent was admissible even though there was no prior judicial authorization for the recording. See also Osborn v. United States, 385 U.S. 323, 327-31 (1966) (holding that a tape-recorded conversation based on surreptitious surveillance was properly admitted). Certainly, a communicator's expectation of privacy is not reasonable once he or she has given consent to search. Expectation of privacy is also lessened when the user recognizes that his or her communications are recorded. Where consent is given to an administrator or someone with mutual use of the property, see United States v. Matlock, 415 U.S. 164, 171 (1974), the originators of e-mail assume the risk that the administrator may give consent to law enforcement officials. This is not an instance where the police went to the Internet provider as in United States v. Maxwell, 45 M.J. 406, 412 (C.A.A.F. 1996). The possession of the password means that this information is protected against other individuals logging onto Appellee's computer or to another computer and trying to obtain her e-mails. The password is not a protection against the systems administrator or law enforcement. For the aforementioned reasons, I respectfully dissent.