

64 M.J. 57

U.S. Court of Appeals for the Armed Forces.

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

Decided Sept. 27, 2006.

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

Chief Judge GIERKE delivered the opinion of the Court.

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. 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. We conclude that based on the particular facts of this case, Appellee 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), 10 U.S.C. § 912a. 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 the government server. Contrary to her pleas, Appellee was convicted by members of the charged offenses.

[...]

#### **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[—possibly an affair with an officer]. 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.

The Court of Criminal Appeals found that the e-mails were retrieved as the result of a specific request by law enforcement officials 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.” 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, 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. . . . 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.”

[...]

## DISCUSSION

The Fourth Amendment of the Constitution protects individuals, including servicemembers, against unreasonable searches and seizures. We have described a

search as an official governmental intrusion into an individual's reasonable expectation of privacy. 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. 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.

The determination of the reasonableness of an expectation of privacy, "is understood to differ according to context." 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 reasonable expectation of privacy against certain intrusions. [*O'Connor v. Ortega*, 480 U.S. 709 (1987)]. 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." The rationale for this suggestion is the "efficient and proper operation of the agency." Thus, an "employee's expectation of privacy must be assessed in the context of the employment relation." *Id.*

[...]

*O'Connor* . . . 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. When the reasonableness standard is applicable, the government must establish: (a) that the search "was justified at its 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."

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, order them confined, and bring criminal charges against them. Military personnel operate in a system that provides criminal sanctions for workplace misconduct. Accordingly, we need to keep these unique aspects of the military environment in mind whenever we apply the *O'Connor* decision to workplace searches.

[...]

#### THE SUBJECTIVE EXPECTATION OF PRIVACY

This Court previously considered military members' subjective expectations of privacy in *Maxwell* and *Monroe*. In *Maxwell*, the

accused used America Online's (AOL) e-mail service to communicate with another junior Air Force officer about the accused's sexual interests and to send and receive obscene material and child pornography. 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.

In *Monroe*, this Court concluded that, in contrast to *Maxwell*, the e-mail system in question was owned by the government. 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.

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 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. 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 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. Instead, the reasonableness of a privacy expectation will differ according to the context, and the “operational realities of the workplace.” . . . .

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. 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 Supreme Court in *O'Connor* indicated that privacy expectations in the workplace may be reduced by virtue of office practices, procedures, or regulation. 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 content of e-mail messages. 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.

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. 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.

[...]

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.

[...]

#### **HARMLESS ERROR**

[The Court found the error to not be harmless. The Court authorized a rehearing.]