Public Interest Law Reporter

Volume 7
Issue 1 *Spring 2002*

Article 2

2002

The Price of Technology: Curbing Employee Internet Abuse

Michael J. Malone
Chief Counsel, Defense Reutilization and Marketing Service

Feature: Internet Abuse

THE PRICE OF TECHNOLOGY: CURBING EMPLOYEE INTERNET ABUSE

By Michael J. Malone*

I am the chief counsel for a Department of Defense agency that provides logistics services to the military. For over five years, we have actively embraced electronic commerce and aggressively converted our systems to web-based applications. The increases in our efficiency have enabled us to drastically reduce our workforce and to provide improved services faster and cheaper. Our workforce has been transformed from "box kickers" to "knowledge workers," operating under the slogan--"*Moving information not materiel.*"

In* O'Connor v. Ortega, *the Supreme Court held that "public employer intrusions on the constitutionally protected privacy interests of government employees for non-investigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all circumstances."

For a time, it appeared that there would be no down side to the advantages gained from the agency's use of electronic mail systems and the Internet. A call from our information security office early in our transition served notice that there would be some novel legal issues associated with placing this new technology in the hands of our workforce. The caller alerted me that an employee had been accused of harassing fellow employees with bizarre and threatening emails. It was also suspected that he was devoting substantial duty time to "surfing the web." Information security wanted to know if the hard drive in the employee's computer could be reviewed and whether disciplinary action could be taken against the employee if the review disclosed misconduct. Naturally, our legal advice to management required consideration of a wide range of legal issues. This article will touch on a few of them.

It is not surprising that our agency and many other employers have encountered legal questions related to employee misuse of electronic communications. *CNNMoney* cited a research firm's report that "30 to 40 percent of Internet use in the workplace is not related to business. News, sports and financial sites are at the top of the list."[1] Some level of non-productive use of email and the Internet is expected and tolerated by many employers. Occasionally, the misuse becomes a disciplinary problem and the employer must decide to take remedial action.

A threshold question for any employer, public or private, is whether employees have a reasonable expectation of privacy in emails and other materials transmitted or stored on computer systems owned by their employers. A common law cause of action in tort for invasion of privacy would arise if it could be shown that by accessing the employee's email, the employer "intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another in his private affairs or concerns" and if the intrusion is "highly offensive to a reasonable person."[2]

Recognizing the importance of facts in particular cases, courts have generally been reluctant to conclude that employees have a reasonable expectation of privacy in email initiated or received over the employer's email systems and have found such acts not to be torts.[3]

As a government entity, our agency faced an additional legal concern--reviewing the employee's email or seizing the computer hard drive might violate the Fourth Amendment of the United States Constitution. In a leading case, *O'Connor v. Ortega*, after concluding that Ortega had a reasonable, though diminished expectation of privacy in his office, the Supreme Court held that "public employer intrusions on the constitutionally protected privacy interests of government employees for non-investigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of rea-

sonableness under all circumstances."[4] Under the standard, the search would have to be justified from its inception (i.e. when there were reasonable grounds to suspect that the search would turn up evidence of work-related misconduct). Also, it would have to reasonably relate in scope to the objectives of the search and not be excessively intrusive in light of the purpose of the search. Searches not satisfying the reasonableness standard violate the Fourth Amendment.

The *Ortega* case, however, did not involve a computer search. A recent case, *Leventhal v. Knapek*, applies the reasonableness test to a computer search.[5] In that case, Leventhal, an accountant employed by the state of New York, challenged his demotion for conducting a private tax consultation business during work hours. He contended that searches of the personal computer in his office violated the Fourth Amendment. The Court found that the search was reasonable in its inception and appropriate in scope. An anonymous tip indicated that Leventhal was preparing tax returns for private clients on the state-owned personal computer. Investigators printed out a list of non-standard software on the computer and examined the computer to identify various tax preparation programs.

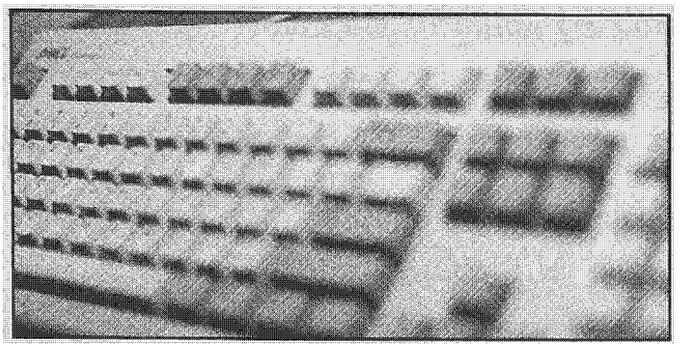
Both public and private employers who access an employee's email or computer files may face allegations that they have violated the Electronic Communications Privacy Act (ECPA), or the Stored Communications Act.

In contrast to that view, however, is the case of *U.S. v. Simons*.[6] In that case, given the agency policy defining prohibited Internet use and warning of network audits, the Court found that the employee did not have a reasonable expectation of privacy in files downloaded from the Internet and concluded a warrantless search of his office computer that located pornographic pictures did not violate the Fourth Amendment.

The difficulty in predicting how the ECPA and the Stored Communications Act will be applied to employee communications and emails can be avoided by notifying each employee that management will periodically review such communications without notice and by obtaining the employee's written consent to these reviews.

Both public and private employers who access an employee's email or computer files may face allegations that they have violated the Electronic Communications Privacy Act (ECPA)[7], or the Stored Communications Act.[8] The former was designed to extend federal restrictions on wiretapping to the interception of electronic communications, including email. The latter was designed to protect such communications from unauthorized "access" while they are in electronic storage. "Electronic storage" is defined in the Stored Communications Act as either "temporary, intermediate storage...incidental to the electronic transmission or storage for purposes of backup protection of the communication."[9]

The difficulty in predicting how the ECPA and the Stored Communications Act will be applied to employee communications and emails can be avoided by notifying each employee that management will periodically review such communications without notice and by obtaining the employee's written consent to these reviews. The respective statutory provisions, 18 U.S.C. § 2511(d) and 18 U.S.C. § 2702(b)(3), expressly provide that their prohibitions do not apply where one party to a communication has consented to its interception or disclosure. Many states have enacted laws similar to the ECPA in an effort to protect the privacy rights of employees and to regulate the monitoring and disclosure of electronic communications.



The policies developed to regulate employees' use of the Internet and of email should be realistic.

To minimize productivity losses due to casual use of email and Internet in the workplace and to guard against other legal problems, all employers should develop a comprehensive, written policy governing the use of its computers, electronic communications, the Internet and electronic records. The policy should clearly and unequivocally state that the employer will monitor all systems and may review any electronic communications or electronic records prepared or received by employees. All employees should receive a written copy of the policy. They should also be required to sign a written acknowledgement that they have received and understand the policy and consent to monitoring of all records and communications by the employer. It is also advisable to have a log-on screen greeting, which gives notice to employees that they are using the employer's system. The screen greeting can also indicate that by clicking on "OK," employees consent to the conditions imposed by the employer.

The policies developed to regulate employee's use of the Internet and of email should be realistic. If an employer is willing to tolerate employees using the Internet during lunch hour to read the news or to send an email to a friend, the policy should not prohibit all personal use. A reasonable policy that is evenly administered is unlikely to be subject to an attack that the employer has waived the policy by routinely ignoring violations. A host of other issues, including privileged information, intellectual property rights and confidentiality, to name a few, should also be covered. Taking these kinds of affirmative steps will decrease the magnitude of time lost because of Internet misuse and will reduce potential liability when the employer finds it necessary to enforce its workplace policies.

ENDNOTES

[1] <http://www.cnn.com>, *CNNMoney*, (visited June 27, 2000).

[2] Restatement 2d of Torts, § 652 (b).

[3] *See e.g., McLaren v. Microsoft Corporation*, 1999 Tex. App. LEXIS 4103 (unpublished), where Microsoft's review and dissemination of email stored in "personal folders" on the employee's office computer was held not to constitute and invasion of privacy. Similarly, in *Bourke v. Nissan*, No. B06875, Cal. 22 App. Dist. 1993 (unpublished), the court found no invasion of privacy where the employee had acknowledged in writing that the email system was to be used only for business purposes and was aware it could be monitored at will by the employer.

[4] 480 U.S. 709, 718 (1987).

[5] 266 F. 3d 64 (2d Cir. 2001).

[6] 206 F. 3d 392 (4th Cir. 2000).

[7] 18 U.S.C. 2510-22 (West 2000).

[8] 18 U.S.C. 2701-11 (West 2000).

[9] *Ibid.* Significantly, violations of each of these statutes can result in criminal or civil liability. *See, e.g., Fraser v. Nationwide Mutual Insurance Co.*, 135 F. Supp. 2d 623 (E.D. Pa. 2001); *Konop v. Hawaiian Airlines*, 236 F. 3d 1035 (9th Cir. 2001) (withdrawn with a subsequent opinion to be filed later), 262 F. 3d 972 (9th Cir. 2001). Both cases contain excellent discussions of these statutes. The decisions highlight their lack of clarity and discuss the confusion regarding their scope.

** Michael J. Malone has been the Chief Counsel for the Defense Reutilization and Marketing Service (DRMS) since 1997. He has also served as the Chief Trial Attorney for DRMS from 1980 to 1984. He has a degree from Michigan State University and is an alumnus of Loyola University Chicago School of Law (Class of 1974). He is a specialist in environmental law and government contracts.*