Journal of Technology Law & Policy

Volume 5 | Issue 1 Article 1

January 2000

You Got Mail but Your Employer Does Too: Electronic Communication and Privacy in the 21st Century Workplace

Amy Rogers

Journal of Technology Law & Policy
Volume 5 Spring 2000 Issue 1
Published by Students at the University of Florida College of Law

return to table of content | comment on this article

You Got Mail But Your Employer Does Too: Electronic Communication and Privacy in the 21st Century Workplace

Amy Rogers

"The only secure computer is one that is turned off, locked in a safe, and buried twenty feet down in a secret location— and I'm not completely confident of that one, either."

--Bruce Schneier, Computer Security Expert[1]

Cite as: Amy Rogers, *You Got Mail But Your Employer Does Too: Electronic Communication and Privacy in the 21st Century*, 5.1 J. TECH. L. & POL'Y 1, <http://grove.ufl.edu/~techlaw/vol5/emailfinal.htm> (2000).

TABLE OF CONTENTS

I. The Use and Importance of Electronic Communication in Today's Workplace

{1} The key to creating and maintaining a successful business in today's market is the management of people and information. The Internet provides access to the world without the expense and inconvenience of travel. The click of a mouse replaces the hassle of coordinating face-to-face meetings and productivity supplants indecision. As with most technological improvements, however, the myriad ways that e-mail and the Internet create problems in the workplace are just emerging[2].

{2}Americans tend to embrace products and services that offer convenience and immediate results. This trend accounts for the popularity of plastic surgery, drive-through windows, and now, e-mail and the Internet. By the time problems emerge, we often find ourselves inextricably attached to such devices that satiate our need for instant gratification. This is the case with electronic communication in the workplace.

{3} E-mail is a convenient communication method that instantaneously delivers messages between computers. Paper correspondence is no longer required to transmit documents and other important information. Companies exhibit increased productivity and profitability by reducing the time and money spent on correspondence. Unfortunately, they also frequently exhibit a lack of attention to exactly who has access to certain information, and to whom such information is being transmitted. The possibility for abuse of e-mail and the Internet in the workplace is great. Estimates show that workers with on-line access spend five to ten hours per week searching the World Wide Web for non-work-related sites or sending e-mails of a personal nature.[3] Ironically, while e-mail has the potential to increase productivity, the most prevalent problem related to its use is the reduction of productivity.

II. General Liability Concerns

{4} Recent polls estimate that approximately 2/3 of the workforce uses e-mail.[4] By the year 2000 this will be more than 40 million workers[5]. Many companies view the Internet as an interactive library rather than a communication medium requiring regulation and monitoring.[6] The ease of use and illusion of anonymity of the Internet lulls corporations into a false sense of security concerning employees' use of this resource. Both e-mail and the Internet generate a significant amount of litigation, and as more companies become connected to one another and to cyberspace the number of lawsuits continues to grow[7]. Many companies are not even aware of the dangers presented by e-mail and Internet use.[8] Decreased productivity due to personal use of these mediums during work hours is the most obvious, but also the easiest to control[9]. Violation-of-privacy suits resulting from monitoring of employees' e-mail and Internet use, and improper material entering the workplace from Internet sites are more insidious[10]. Companies also face increased liability due to inadvertent disclosure of proprietary information, electronic message retention and spoliation, Internet chat rooms and message boards, and, recently, employee's personal web sites.

{5} Liability dangers are often hidden. Each time an Internet user visits a particular site a record of that visit is left behind. Commonly called "mouse droppings" or "cookies," these can be traced back to the company if the site is accessed from a workplace domain. "We tell people, don't go to a site that you wouldn't walk into physically and lay your business card on the table."[11] A company could potentially face an investigation into their standards or ethics based on sites visited from internal systems. For example, visits to a website dedicated to discrimination of a particular racial group could provide ammunition for a discrimination lawsuit. While not as common, lawsuits arise from employee's home use of communication systems as well. Employees have had more success defending their right to

privacy in personal e-mails and Internet use from home[12], but the potential for harming the employer's reputation is great and employees should be aware of this possibility.

{6} Another dangerous problem related to personal use of Internet and e-mail resources is the inadvertent dissemination of information and inappropriate messages sent to the wrong recipient[13]. Although it is difficult to imagine, e-mail is misdirected frequently enough to cause concern. Proprietary information could fall into the hands of someone who will use it to exploit the company. Information security on the Internet is a significant problem faced by many companies.[14] Although several of these businesses have now have firewalls in place to prevent unauthorized access to computing systems, these barriers can often be bypassed.[15] For these reasons it is important that employees safeguard all information they have access to and avoid sending or storing sensitive data on company systems as much as possible. Companies should also be aware that inappropriate messages, such as those containing racist or sexist slurs or pictures downloaded from the Internet, can lead to lawsuits if they are sent to the wrong person. In fact, merely glimpsing a questionable Internet site on a colleague's computer monitor could be classified as sexual harassment.[16]

{7} As use of e-mail and the Internet in the workplace grows, more areas of concern to employers surface. For example, Internet bulletin board services, or message boards as they are commonly called, are sites where almost anyone can anonymously post messages on a given topic[17]. While these areas often contain legitimate information about a company, they more frequently serve as "virtual water coolers" where employees and others exchange gossip and complaints about the company. Because postings at these sites are often exaggerated and damaging to the company, it is important to have a policy in place to address such issues.[18]

{8} Companies must also be aware of the danger of copyright infringement. Software transferred by e-mail or downloaded from the Internet often violates copyright laws[19]. There is also danger of downloading viruses when software or other information is received in this way. If such software is used on a company computing system, the company may be liable for any violations.

III. Developments in Litigation

A. Workplace Cases

{9} The issue most often litigated between employers and employees regarding e-mail and Internet privacy is employee's expectations of privacy versus the monitoring practices of the company.[20] While unpopular with employees, monitoring of computing and communication systems is an effective way to ensure compliance with company policies and guard against potential liability from inappropriate use. The "unreasonable intrusion upon the seclusion of another"[21] is the invasion of privacy tort most likely to be used by employees in cases against their employers. This tort holds that "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[22] Cases involving such questions are most often resolved in favor of the employer because the information passing through company computing and communication systems is generally not considered private, and the monitoring of such systems is usually not found to be highly offensive.

{10} In Smyth v. Pillsbury, the defendant repeatedly told employees that e-mail communications would

remain private[23]. Despite these assurances, the court found that the plaintiff did not have "a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system."[24] This case resulted from the discharge of an at-will employee as a result of threatening comments he made about management over the company's e-mail system [25]. The court also held that "even if . . . the employee had a reasonable expectation of privacy in the contents of his e-mail communications over the company e-mail system, . . . a reasonable person would [not] consider the defendant's interception of these communications to be a substantial and highly offensive invasion of his privacy."[26] In addition, the court applied a balancing test, finding that the company's interest in ensuring proper and appropriate usage of its e-mail system outweighed any interest an employee may have in the privacy of his own e-mail sent or received by the company server. [27] This case and others illustrate the courts' willingness to justify monitoring of employee's e-mail.

{11} As a result of these potential dangers, employers must have a policy addressing Internet and e-mail usage in the workplace. Difficult decisions must be made concerning personal use of these communication mediums and whether or not monitoring of employee e-mail and Internet usage is necessary. Companies must also develop a policy for retention and storage of electronic communication, and perhaps even set parameters for what types of information can be communicated via e-mail. E-mail sent and received on an employer's computer system is subject to discovery and can often be accessed even after it is deleted. Employers must also clearly state their rules for employee's personal web sites. If such a site contains questionable material, such as pornography, it would be wise to ensure that the company's name is not mentioned on the web site. Many companies utilize firewall software that blocks certain websites [28]. While this is a useful tool, it does not completely eliminate problems. Certain sites are missed, and tenacious employees can find ways to circumvent the blocking program. They can also send pictures and programs to their work computers from a computer not connected to the company system. These are complicated issues that an alarming number of employers have yet to address.[29] In order to avoid litigation, it is imperative that employees have a clear understanding of company expectations regarding e-mail and Internet use.

B. Federal and State Laws

{12} Federal and state laws are changing as rapidly as computer technology to keep up with the demands of the electronic world. Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act in 1968 to prevent unlawful telephone wiretapping. The Electronic Communications Privacy Act (ECPA) of 1986 [30] amended Title III to include all forms of electronic communication, including e-mail. However, the Act has provided little protection to employees concerned with the privacy of workplace e-mail. The ECPA provides that a person may not "intentionally intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral or electronic communication.[31]" This blanket statement is followed by a number of exceptions.

{13} The "Ordinary Course of Business" exception states that an employer may intercept an employee's e-mail in the ordinary course of business using equipment or facilities furnished by the provider of electronic communication service.[32] As long as an employer can show that the interception occurred in the ordinary course of business, the employee has no grounds to challenge the interception. While "ordinary course of business" has not been defined in the context of e-mail interception, it is likely that the capture of e-mail sent and received on company systems will easily fall into such category. This would include monitoring the system to ensure proper management and routing of messages, inevitably resulting in the observation of employee e-mail messages. In cases involving workplace telephone calls, courts have held that monitoring is allowed as long as the call is business-related.[33] This standard will

likely apply to e-mail monitoring as well.

{14} Title II of the ECPA addresses stored communications. [34] Violation occurs if a person "intentionally accesses, without authorization a facility through which an electronic communication service is provided."[35] There are also exceptions that apply to this section. The first is the provider exception, which holds that a violation of the ECPA does not occur if "the person or entity providing a wire or electronic communications service" authorizes the access. [36] The second exception, which also applies to Title I, is the user or prior consent exception. [37] This exception provides that the ECPA does not apply when one party to a communication consents to monitoring. While express consent affords an employer the greatest protection against privacy violation suits which stem from the monitoring of employees, the employer may also argue that such consent is implied from the nature of the employer-employee relationship and the work environment.[38].

{15} These three exceptions to the ECPA address most challenges that an employee can present regarding privacy of workplace e-mail. If a company serves as the e-mail provider for its employees, Title II authorizes access to stored communications and Title I allows the company to intercept e-mail messages as long as the interception occurs as part of the normal course of business. E-mail messages, even once deleted, are often stored on backup servers and central hard drives. As a result, employers may have access to communication believed by employees to be no longer in existence. In this manner, employers can monitor exactly what enters and leaves their system via e-mail. Even if an outside entity provides online service, an agreement signed by employees acknowledging that their e-mail can be accessed would indemnify companies in most states from liability by invoking the prior consent exception.

C. Constitutional Concerns

{16} Two constitutional issues have been raised with little success in defense of employee's privacy. The Fourth Amendment of the United States Constitution protects against unreasonable search and seizure. This protection applies only to public employees working for a government actor [39]. However, courts have upheld even the government's right to engage in workplace surveillance for legitimate business reasons.[40] As such, private-sector employers likely will not face Fourth Amendment claims. In ambiguous cases courts have applied a balancing test, weighing the importance of the employer maintaining control of the work environment against the public interest in the activity of the employee.[41] The second constitutional consideration addresses Congress' power to regulate private corporations. Congress' authorization to govern private entities stems from its commerce power granted in Article I, § 8, (3). If the electronic communication sent and received within a particular company does not cross state lines or impact interstate commerce in any other way, Congress may not regulate it. Neither of these Constitutional arguments is likely to benefit an employee arguing for privacy of workplace communication.

{17} Most state's laws concerning electronic communication mirror the federal laws. Florida laws protect the privacy rights of employees a bit more strongly than federal law. [42] However, even the Florida Constitution can only protect privacy rights against governmental intrusion in areas where an individual has a legitimate and reasonable expectation of privacy. Florida also narrows the scope of the exemptions listed in the ECPA in its Security of Communications Act.[43] In order for the consent exemption to apply in Florida, all parties to the communication must consent to employer monitoring, not just one as required by the ECPA. This more stringent standard could present a problem for a company if a Floridian is a party to a message intercepted or monitored by an out-of-state employer.[44]

In order to avoid potential lawsuits stemming from variations in state's laws, an employer should be conscious of with whom his employees communicate via e-mail.

IV. Corporate Strategies for Liability Avoidance

A. Inappropriate Use of E-mail and Internet Systems

{18} Most companies have policies addressing many issues regarding e-mail and Internet use[45]. While these guidelines provide a good starting point for avoidance of liability, they must be closely examined to ensure they achieve the intended result. E-mail and Internet use policy statements must be consistently worded each time they are stated. It is important for different departments or work areas to maintain the same policies within the same company. And company directors should consider the impact of their workplace policies on employee morale.

{19} Many employees log onto their computers immediately upon arriving to work, which usually enters them into a company Intranet system. This provides a good opportunity to greet employees with a warning message stating that "[Company] computing and communication resources are provided for business-related purposes. [Company] will monitor system use and inappropriate activity will subject users to appropriate disciplinary action, which may include termination." The use of the word, "will" is important in the warning message. If this language reads, "may," the company could potentially be liable for claims of discriminatory application of the policy. Although it will be difficult to catch and punish every misuse of the e-mail and Internet system, notifying employees that such activity *will* be monitored and violators *will* be subject to disciplinary action relieves the employer of some of the dangers that can be caused by discretionary enforcement[46]. Employees often overlook boilerplate warnings such as this[47]. However, should problems arise, it will be more difficult for an employee to claim ignorance of the policy's applicability, particularly if this message is posted in the same spot everyday[48].

B. Policy Guidelines

{20} There are a number of other measures employers can take to minimize problems with electronic communications. First, companies should reconsider their position on personal use of e-mail and the Internet. Studies have shown that workers with on-line access spend up to 10 hours per week sending personal e-mail or visiting Internet sites unrelated to work It is unrealistic for a company, particularly a large company, to expect all employees to refrain from any personal use of communications systems. It is also difficult to enforce a policy prohibiting all personal activity on such systems. Punishment for violation of this rule would not be consistent unless each employee's Internet and e-mail use is monitored equally. Employees may claim discrimination if one person is reprimanded for personal use of e-mail and another is not. Employees may also be more compliant with usage policies if guidelines for e-mail and the Internet include allowances for a small but realistic amount of personal use. For example, a policy stating that "Company computing and communication resources are provided for business-related purposes and any personal use must be kept to a minimum and may only be done during non-work periods (i.e. lunch breaks)," may help to foster cooperation and lower resentment among employees. However, if the company chooses not to allow any personal use of its computing and communication systems, this should be clearly stated in the warning message posted on computer start-up screens. Every other statement addressing e-mail and Internet use should also contain this strict policy. Such message could read, "Company computing and communication resources are provided for business-related purposes only and personal use is prohibited. Violation of this policy will result in disciplinary action." Policies such as this must be consistently reiterated to ensure that employees are

aware of the strictness of the standard and the potential for disciplinary action if the guidelines are not followed.

{21} Second, e-mail and Internet usage and monitoring policies are also frequently listed in the company's human resources communications guidelines, which are often available on the company Intranet[49]. While these policy statements often specifically address the issues this paper discusses, they may be contradictory and a bit unclear at times, and all employees may not read them. For example, company policies may state the rule using language similar to, "all use of company assets should relate to valid business purposes." First, many employees may be unaware that the company computing and communication systems and all data transmitted or stored on them is company property and is considered a company asset. A statement clarifying what is included in the definition of "company assets" would help eliminate confusion. Second, the use of the word "should" (all use of company assets *should* relate to business purposes) implies flexibility and leniency in the policy, which conflicts with the statement "all use." Statements such as the one above sentence should be modified to eliminate confusion. A statement that the use of company assets should relate to valid Company business purposes should also be added to modify "Business purposes" in the above example. Otherwise, personal business not related to the company could arguably be conducted using the company's resources.

{22} Guidelines may also frequently state that "Excessive 'browsing' [of external public networks] leading to unproductive or lost work time is inappropriate." This sentence suggests two things: 1) that a certain amount of browsing is allowable as long as it is not "excessive," and 2) excessive browsing is acceptable as long as it does not lead to unproductive or lost work time. Such interpretation contradicts the previous assertion that "all use" of computing and communication systems must relate to valid business purposes.

{23} Third, policy statements should address the content and recipients of e-mail. This warning is necessary to prevent employees from creating an implied agency relationship between the company and a third party. Such warnings also provide a defense for the company in the case of erroneous third-party assumptions regarding agency relationships between the corporation and its employees. The section should caution that "Diligent care is required when your use of public networks may result in actual or perceived action or commitments on behalf of the company." These commitments may arise through employee's personal web sites, e-mail sent from the company server, or potentially even employee postings on an anonymous chat site[50]. Guidelines for personal web pages should be listed here. The company name should not be used in association with any web page or other Internet site that contains information that could be viewed as offensive or questionable, or even information that is in no way related to the business. Examples of such material should be listed, and employees should be instructed that questions may be directed to their supervisor or human resources department and will be kept confidential. Employers would be wise to require any use of the company name on personal e-mail or websites be prohibited unless the human resource or other appropriate department grants permission. This policy will be difficult to enforce, but it will eliminate the company's name from at least a few private sites and will therefore reduce the possibility for litigation.

{24} Similarly, e-mail containing personal or other inappropriate material should not be sent or received using company computers. Employees should be cautioned in posted communications guidelines to keep in mind that "Communications can be easily forwarded to others with or without your knowledge or consent." This section should stress that problems are likely to arise if inappropriate e-mail messages or proprietary information inadvertently ends up in the wrong hands. This policy should also state that disciplinary action up to and including termination and legal action will be taken if an employee engages in such activity. It is important to warn employees of the danger of casually sending information via e-

mail or the Internet without regard to where that information could ultimately end up[51]. The company should also indicate in this guideline that simply having an unsuitable image or message displayed at any time on a computer monitor could lead to disciplinary action by violating the company's sexual harassment policy.[52]

{25} Fourth, communication guidelines should address monitoring of communications. Monitoring warnings on company Intranet screens and in other locations should be displayed prominently. A random survey shows that most employees simply ignore warning screens[53]. When asked what standard warning messages prohibit, most employees believe they caution against visiting improper Internet sites[54]. While many company policy statements do contain such guidelines, they often include other important information as well[55]. By including a large amount of important information in policy statements, employees who fail to read closely may bypass reminders that their company monitors system use. As a result they may not realize that their communications may be intercepted or retrieved from storage. Courts would likely find that any expectation of privacy held by employees regarding e-mail communications is not reasonable, particularly if the employer has posted warnings. However, in order to avoid potential litigation it would be prudent to ensure that this message is clearly and concisely posted on a warning page seen by the majority of employees every day.

{26} Company policies should clearly state that all data and information on company systems is the property of the company and is subject to access by the company. This is a complex rule and it is important that it be worded concisely and be easy to understand. The most important sentence in this section should state, "The Company reserves the right to access any information contained in company computing and communication systems, and the company may, at its sole discretion, disclose this information to third parties." The next step is to ensure that employee reads this statement in order to guarantee awareness of company procedures and expectations. It may be wise in this section to clarify what information may be stored in such systems. Employees may not realize that e-mail may be accessible even once deleted from their personal computers.

{27} And finally, proprietary information should be addressed in Internet and e-mail policies. Guidelines should caution against the use of electronic communication for the transfer of certain material. Because e-mail passes through a number of computers before reaching its destination, it is possible that information could be intercepted during transmission. This can be avoided through prudent use of electronic communication for transfer of company-private information, and also through the use of encryption software. The company should be aware of an important issue raised by the use of personal passwords. Employees should be reminded that their password does not block the company from accessing their computers to monitor Internet or e-mail use. It merely prevents another user from signing onto the system as that particular employee and accessing personal files and other stored information. Again, a court probably would not find that an employee had a reasonable expectation of privacy resulting from the use of a password[56], but clearly stating the policy will eliminate costly litigation.

{28} Companies must clearly establish their policy for personal use of company communication and computing systems. This policy should then be stated simply and boldly in communications guidelines that are accessible to every employee. Employers should give an explicit yes-or-no answer when addressing the question of whether personal use of e-mail and the Internet is allowed. They can then go on to clarify or limit their response, but a clear policy must be firmly established and articulated. The goal of most employers is to limit use of company-provided electronic communication systems to legitimate company business purposes. It is often unreasonable, however, to expect employees to strictly follow this policy. Just as employees will pick up the phone to make a doctor's appointment or

phone home, they are likely to send a quick e-mail to a friend or check their stock prices during the workday. Disallowing minimal personal use may result in resentment and abuse of company systems. Employers must decide if completely disallowing personal use of e-mail and the Internet is worth alienating the workforce.

{29} If the company determines that no personal use is to be allowed, the policy should be clearly stated and reiterated using the same terms every time the subject is addressed. The language of these communication guidelines should be chosen carefully to avoid confusion and to ensure that the proper message is being conveyed. If the policy is not clear and an employee is reprimanded or terminated for a violation, such as excessive personal use of company systems, it would be difficult for the company to support its position and defend its actions concerning such employee. For example, using the word "encourage," as in "the company encourages use of the Internet for business purposes," implies leniency in the company standard. Similarly, by stating that the company "reserves the right" to monitor system use, there is no indication whether or not such monitoring will occur without employee knowledge. Maintaining different policies for various divisions of the same company can also lead to litigation.

{30} Many companies have gone as far as having each employee sign a form acknowledging their awareness and acceptance of e-mail and Internet monitoring[57]. While this is certainly not necessary, it can help reduce misunderstandings based on erroneous perceptions of privacy. This acknowledgment also serves to avoid litigation and other conflicts related to use of company communication and computing systems. I would recommend, going forward, that all employees be required to read and acknowledge such policies. Having e-mail and Internet policies stated regularly in common locations, such as computer start-up screens can likewise reduce the chances for litigation by implying constructive notice of policies.

C. Information Security and Storage

{31} Companies must be aware of problems that may arise from the storage of information. Employees should be alerted that any e-mail that passes through their computer can be accessed and may be stored on company systems. When an employee deletes a message from his own computer, it often still exists on a central server. Policy statements should warn employees that any information stored on company communication systems can and may be accessed by the company, even if it is personal in nature. Companies' positions regarding "ownership" of such personal material should be clarified in order to avoid confusion among employees. Employers must also address which computer systems are subject to the company's policies. For example, if information about the company is sent from one home computer to another home computer, would it be included in this category? If so, it seems impossible to keep track of all such communications. Does the company intend to retain the right to monitor or access employee's home computers to search for such information? While this may seem a bit far-fetched, the potential ambiguities found in policy statements make this a possibility. Companies should also communicate a policy regarding employees that telecommute. Does all information on their personal computers become subject to review by the company simply because the computer serves a work function? These issues should be clearly explained in information security policies made available to every employee.

{32} Procedures for electronic data retention and central storage must also be developed. If a company is not aware of exactly what information is stored on its hard drives and back-up servers, it may find itself in court defending or explaining documents it thought had been erased. Conversely, a company may find itself accused of spoliation for deleting items, whether intentionally or not, pending litigation. Employees must have guidelines for how long to retain e-mail before deleting it from their computers. These guidelines should mirror policies for keeping data in hard-copy form. The same standard should apply for data stored on the company server or back up computers. A uniform length of time should be

established for erasing and reusing space on such systems. Strictly following such procedures can help avoid penalties, even when relevant documents are destroyed.[58] Measures should also be taken to ensure that deletions do not occur when the company is facing litigation concerning a particular issue. It must be established exactly what data is to be kept, in what form, and for how long. This will reduce the opportunity for "litigation minefields"[59] arising from discovery of documents unwittingly retained on computers, and will help avoid sanctions for destroying relevant evidence. The importance of such procedures is increased in light of some court's standards that inadequate records keeping is the equivalent of destroying records.[60] The data-storage policy should reiterate the importance of choosing the language and topics of e-mail carefully.

{33} Companies should review all policies concerning Internet and e-mail use to ensure consistency and conformity with company objectives. Stating policies in different locations is wise to put employees on notice of monitoring and other procedures. However, it is important that these different statements to complement each other and company goals.

{34} The benefits of using e-mail and the Internet in the workplace generally outweigh the possibilities for abuse of such systems. However, the issues addressed above must be addressed in any employment setting to avoid later problems. Companies may face a myriad of problems including lawsuits from employees and customers, release of proprietary information, and loss of productivity if firm policies for use of these company assets are not established and enforced. This is a complex area, and although many problems are just now being discovered, there are precautions that a company should take to avoid these and other problems. First, the company must decide what position to take on e-mail and Internet use. Whether some personal use will be permitted or whether such systems are provided strictly for business use, the company must choose a policy and consistently follow it. Second, all policy bulletins, manuals and alert messages must communicate this guiding principle in a standard manner using consistent terms. It is wise to have alert messages in a number of locations, but there must be no room for misinterpretation of such warnings. If two employees read two different messages, they should each have the same understanding of the company policy. Third, employees must be aware of the potential security risks of sending information via e-mail. They should be alerted to the possibility that their Internet use can be traced back to the company. Most employees will not intentionally disobey company policies, as long as they are reasonable and serve a valid purpose. A consistent, reasonable and realistic e-mail and Internet use policy should result in compliance and satisfaction in the workplace.

---

[1] See Bruce Schneier, E-Mail Security: How to keep your Electronic Messages Private, 1995.

[2] See Susan E. Gindin, *Guide to E-Mail and the Internet in the Workplace,* The Bureau of National Affairs, 1999 <http://www.info.law.com/guide.html>.

[3] See id.

[4] See Mark S. Dichter & Michael S. Burkhardt, *Electronic Monitoring in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age* (last modified June 1999).) <http//www.mlb.com/speech1.htm>

[5] See id.

[6] See Randolph A. Kahn and Robert F. Williams, *Responding to the New Legal Landscape Created by Technology*, 3 The Corporate Counselor 1 (1999).

[7] See id.

[8] See Leyla Kokmen, Firms E-Mull Computer Policies: Employees' Personal Use a Concern, Denver Post, Mar. 22, 1999, at E01.

[9] See Kokmen, *supra* note 8.

[10] See Kokmen, *supra* note 8.

[11] See Kokmen, *supra* note 8.

[12] See e.g. McVeigh v. Cohen, 983 F. Supp. 215, 219 (D.D.C. 1998).

[13] See Kokmen, *supra* note 8.

[14] See Society for Human Resource Management (SHRM), *Technology Raises Legal Questions*, May/June 1996.

[15] A firewall is a special type of gateway that's used to connect an internal network to the Internet. Its purpose is to prevent unauthorized intrusions into the network, which it does by connecting only a 'boundary' machine to the Internet, then selectively forwarding only approved types of traffic between the internal network and the boundary machine. *See* G. Burgess Allison, *The Lawyer's Guide to the Internet,* 133 (American Bar Association 1995).

[16] See Gindin, *supra* note 2.

[17] See Pitney, Hardin, Kipp and Szuch, *Legal Strategy Relating to Internet Bulletin Board Postings, June 15 1999* <http://www.phks.com/newslett/corp_may99.html>.

[18] See id.

[19] See Gindin, *supra* note 2.

[20] See e.g., Smyth v. Pillsbury Co., 914 F. Supp. 97, 98 (E.D. Pa. 1996).

[21] See Restatement (Second) of Torts § 652B (1977).

[22] See id.

[23] See Smyth , 914 F. Supp. at 98.

[24] See id. at 101.

[25] See id.

[26] See id.

[27] See id.

[28] See Allison *supra* note 15.

[29] See Kokmen, *supra* note 10.

[30] 18 U.S.C. S 2510-2520

[31] 18 U.S.C. § 2511

[32] See id.

[33] See, e.g., Epps v. St. Mary's Hosp. of Athens, Inc. , 802 F.2d 412, 417 (11th Cir. 1986).

[34] 18 U.S.C. S 2701-2710

[35] 18 U.S.C. § 2701

[36] See id.

[37] 18 U.S.C. § 2511

[38] See Jarrod White, Email@work.com: *Employer Monitoring of Employee E-mail*, 48 Al. L. Rev. 1079, 1084 (1997).

[39] See e.g. Vega-Rodriguez v. Puerto Rico Tel. Co., 110 F.3d 174, 178 (1st Cir. 1997).

[40] See id. at 181

[41] See e.g., Connick v. Meyers, 461 U.S. 138, 152-53 (1983) (holding that the content, context, manner, time, and place of the employee's expression must be considered in balancing the employee's rights against the employer's interests).

[42] See U.S. Const. Art. I, § 23

[43] See Fla. Stat. Ann. §§ 934.01-934.43(1991).

[44] See White, *supra* note 38, at 1090.

[45] See Gindin, *supra* note 2.

[46] See id.

[47] Based on an informal poll conducted 6/24/99 by the author

[48] See Gindin, *supra* note 2.

[49] See, e.g., <http://www.corp.harris.com/harris/Directory/qa.htm>.

[50] See Gindin, *supra* note 2.

[51] See id.

[52] This guideline should comply with the language and regulation of company sexual harassment policies.

[53] Survey conducted 6/24/99 by the author

[54] Survey conducted 6/24/99 by the author

[55] See Gindin, *supra* note 2.

[56] See e.g., Smyth, 914 F. Supp. at 101.

[57] See Gindin, *supra* note 2.

[58] See Randolph A. Kahn and Kristi L. Vaiden, *If the slate is wiped clean: Spoliation: What it can mean for your case*, 8 JUN Bus L Today13, 13 (1999).

[59] See id.

[60] See id. at 14.