J. INDIVIDUAL EMPLOYMENT RIGHTS, Vol. 10(4) 337-347, 2002-2003

EMPLOYER AND EMPLOYEE RIGHTS AND RESPONSIBILITIES IN A NETWORKED OFFICE

RONALD R. TIDD

NANCY GRABER PIGEON

Central Washington University, Ellensburg

ABSTRACT

Internet-connectivity is having a profound impact on the workplace. Employees use it to access data and information from global sources, communicate with others instantaneously regardless of physical proximity, work anytime, anywhere, so long as they have a digital device connected to the Internet. Alternatively, the technology can be used to subject coworkers to objectionable material, violate workers' privacy, and convey the appearance of working when actually abusing Internet resources. This article discusses the existing laws regarding employee usage of an employer's Internet resources and employer monitoring of that usage. Thus, it provides a foundation for understanding a body of law that is bound to evolve at an increasingly rapid rate and must be used by every organization to guide its employment and IT policies.

The Internet may not be fueling a revolution in the marketplace, but it is certainly fueling an evolution in the workplace. More and more organizations are discovering the power of networked computers and connecting employees to each other and to the Internet. In this connected work environment, employees can:

- access data and information from around the world;
- communicate instantaneously with each other regardless of physical proximity; and
- work anytime, anywhere, as long as they have a digital device that connects to the network.

This seems like heaven to Type A personalities, but like all technologies, it is a two-edged sword. The results of the annual UCLA Internet Project Survey show that a majority of employees use their employer's Internet and e-mail resources for personal purposes, although almost half of them also believe that the employer monitors their activities (Table 1).

These network technologies alter the interaction between employees and workflow as well as the interaction between employees and employers. They make it more difficult for managers to monitor, control, and direct employee productivity and activity. Telecommuting employees work at home in relative autonomy. Technology-enabled employees in the office are not as autonomous, but they may be able to obscure their activities from managerial scrutiny. Thus, employees may be using company technology for personal purposes during company time and may even access and disseminate material that creates a hostile workplace. Without proper precautions and controls, management may not discover those activities until charges of sexual harassment are levied or decreasing profits are reported. Consequently, it is imperative that employers and employees understand the legal environment and how to manage the risks associated with this constantly changing environment of networked computers.

THE CHALLENGES OF A NETWORKED WORKPLACE

As a computer network evolves into a mission-critical channel for exchanging business information and communications, the legal system must also evolve. Unfortunately, it cannot do so at "Internet speed" and the issues related to

Table 1. Internet Usage Survey

	2000	2001	2002
Employee Internet usage at work			
For business purposes	83.7%	89.7%	90.2%
For personal purposes	50.7%	60.7%	60.5%
Employee e-mail usage at work			
For business purposes	79.7%	85.5%	83.5%
For personal purposes	52.4%	58.1%	57.1%
Employee perception about employer monitoring			
Employee Internet usage monitored	N/A	44.6%	45.1%
Employee e-mail usage monitored	N/A	45.7%	44.9%

Source: Surveying the Digital Future: The UCLA Internet Report, Year Three, UCLA Center for Communication Policy, February 2003.

employees' use of employers' network resources (technology and time) remain unresolved. This article provides guidance with respect to two related issues: 1) Can and/or should employees have unrestricted use of employer resources (technology and time)? and 2) Can and/or should employers restrict employee use of employer resources (technology and time)?

The proper management of the risks associated with these issues involves a cost-effective combination of technology, policies, procedures, and practices (policies) that should be tailored to meet the unique environment of each organization and help it fulfill its mission.

Within this framework, an organization has three main risks. First, in the absence of a usage policy, the inappropriate use of its resources may impair employee productivity, create a hostile workplace, or allow confidential information to be communicated to unauthorized individuals. This may leave the employer with limited legal recourse against employees. Second, with a policy that employees view as too *Orwellian,* the workplace will become more unfriendly and potentially unstable. A poorly written policy may even violate employee rights to privacy and provide them with legal recourse against the employer. Finally, with a policy that is inappropriately enforced, the employer may become an unwitting accomplice of employees committing inappropriate acts. Again, the employer may become a defendant in a legal action.

THE LEGAL FRAMEWORK

The proper management of these risks must comply with federal, state, and local laws as well as help an organization fulfill its objectives. Four federal statutes have potential application:

- Title VII of the Civil Rights Act of 1964 (hereafter, Title VII)
- National Labor Relations Act of 1935 (NLRA)
- Fair Labor Standards Act of 1938 (FLSA)
- Electronic Communications Privacy Act of 1986 (ECPA)

Each of the first three applies to a specific area of employment law and relies on a different definition of employee.

Title VII

Title VII of the Civil Rights Act prohibits discrimination in the workplace. It defines employee as "an individual employed by an employer," including those subject to civil service laws but excluding elected officials and those that they choose or appoint to policy making positions [1]. Discrimination can occur under this statute through the misuse of Internet resources to engage in sexual harassment. This form of discrimination can involve e-mail transmissions of, for example, pornographic messages, pictures, and sexually charged jokes, from

one employee to another or from someone outside the company to an employee. With respect to the later, the employer of an aggrieved party is responsible for contacting the instigator's employer to stop the offending behavior.

Title VII can also involve browsing pornographic Web sites if that activity creates a hostile work environment for employees who are nearby and see or hear what is on an offending employee's computer. Such behavior could be costly, as indicated by recent settlements for sexual harassment.

The NLRA

Section 8(A) of the NLRA protects an employee's right to organize or not organize collectively and prohibits certain employer actions that constitute unfair labor practices. It specifies that the term employee shall include any employee, and shall not be limited to the employees of a particular employer unless this subchapter explicitly states otherwise [2]. This statute could be applied when employees use an employer's Internet resources (e-mail and Web pages) to solicit participation in an unionizing activity. Employers can implement and enforce policies that prohibit employees from using those resources for non-business purposes (including unionizing activities). However, employers can not implement and enforce policies that prohibit only unionizing activities. Unless the employer's policy officially and effectively prohibits all non-business activity, it is unlikely to survive a review by the National Labor Relations Board [3].

The FLSA

The Fair Labor Standards Act ensures that all covered employees are paid the minimum wage and are paid overtime for all hours worked over 40 hours in a workweek. Employees are defined as "any individual employed by an employer" [4]. Computer technology complicates application of this law by making it more difficult to determine when covered employees are working. Whether the employee is a telecommuter or confined to a cubicle, employers need to know that compensation paid for overtime hours is for hours actually worked.

The ECPA

Because the application of the Electronics Communications Privacy Act is not restricted to employee-employer relationships, it does not define the term, employee. This Act prohibits the "interception, recording, disclosure of any wire oral or electronic communication," with two notable exceptions:

- A provider of an e-mail system may intercept electronic communication on the system incident to rendering the service or to protect the rights or property of the provider [5],
- A party to the e-mail communication or a participant in the communication may consent to the monitoring [6].

The first exception gives employers who provide workplace e-mail systems the right to monitor employee e-mail if such communications threaten the employer's rights or property. Clearly, terms like threaten, rights, and property are subject to interpretation and uncertainty. Since the second exception is not subject to similar interpretation and uncertainty, it is a safer strategy. However, as is mentioned in the next section, consent should be in writing to remove as much uncertainty as possible.

Network usage policies must also consider state and local laws. Some states have laws patterned after the ECPA, which protect against the interception of electronic communications [7]. In addition, many state constitutions have privacy provisions, although their application is generally restricted to the violation of employee rights by public sector employers. In an attempt to extend application to private sector employers, an argument has been made that the state constitution provides for employee privacy [8]. In two notable cases, the courts have held that employees should have no expectation of privacy when using e-mail systems used by all company employees [9]. If that privacy is violated, an employee may have a claim for wrongful discharge based on a violation of public policy [10].

There is still uncertainty about whether an employee has an expectation of privacy in the private sector given constitutional limitations. Generally, if an employee in the private sector is using company equipment, the employee has a lessened expectation of privacy under the Smyth and the McLaren cases. But every jurisdiction is different, so it is imperative that employers seek assistance from those with legal expertise in each jurisdiction.

USING TECHNOLOGY TO MEET THE CHALLENGES OF THE NETWORKED WORKPLACE

As noted, any strategy for managing the risk that IT resources will be used inappropriately involves some combination of technology, policies, procedures, and practices that are designed to prevent, detect, and correct inappropriate activities. Prevention relies on a blocking strategy that prevents employees from accessing and sending inappropriate information. Detection uses a monitoring strategy that discovers violations in process or after the fact. Correction requires policies and procedures that remedy violations by modifications to the technology, the policies, and employee behavior. It is common to use all three, but necessary to emphasize prevention where the risks are greatest.

Implementing Technology

It is possible to implement the technology component for prevention and detection strategies with hardware or software, and a prevention system can be administered by an organization's system administrators or outsourced to a service provider (see Table 2). To distinguish between acceptable and unacceptable uses

Table 2. Technology Solutions

	Strategy		
	Prevent	Detect	Correct[a]
Hardware			
NetSpective WebFilter	X		X
iPrism	X	X	X
Software			
Internet Manager	X	X	X
Pearl Software		X	X
SuperScout Filters	X	X	X
Symantec Mail Gear	X	X	X
Websense	X	X	X
WebWasher	X		
WinWhatWhere	X	X	X
Service Providers			
Cerberian	X	X	X
FastTracker	X	X	X

[a]A correction strategy is implemented primarily through the use and analysis of log files generated by the technology or the service provider.

of network resources, the technology commonly uses filtering methods that can prevent access to Web sites based on:

- their uniform resource locator (URL) address;
- text that contains pejorative/offensive words; and
- patterns in digital photos that suggests pejorative/offensive topics (e.g., a high incidence of flesh tones suggesting pornography).

Filtering methods also are used to monitor e-mail by examining content and information about its source and subject, and to prevent downloads of certain types of files (e.g., pictures, music, videos, and executable files) (see Table 2).

Filtering methods compare the characteristics of a requested Web page (its URL, the presence of pejorative/offensive terms and graphics) to a list (database) of offensive URLs and inappropriate Web-based material that might violate usage policies, including the Internet (unless everything outside of the organization's intranet is considered off-limits and filtered out). Consequently, the filtering methodology is only as effective as that list (database) is complete and current. Maintaining currency and completeness is a dynamic game of cat-and-mouse since new potentially offensive Web sites emerge on a daily basis, plus those who

create such Web sites continuously adjust the content and presentation to circumvent the latest filtering techniques. Employers should verify that the vendor providing the hardware, software, or filtering service, also provides continuous updates to combat the latest stealth techniques.

Employers also need to be aware that employees have strategies and tools to circumvent employer restrictions. For example, employees can use Web-based e-mail services during work hours (e.g., Hotmail and Yahoo), and it will be difficult to monitor the content of the e-mail. However, filtering can make it impossible to access the Web sites that offer such Web-based services. Employees also can acquire software that thoroughly removes the remnants of prohibited browsing and downloading from their desktop and laptop computers, but cannot remove the tracks left on the employer's server that is used as the gateway to access the Internet. Of course, employees can use dial-up modems to circumvent the employer's server.

The activity logs and records generated by the server that connects an organization and the Internet are an extremely important part of detect and correct activities. They provide, in part, information about:

- where office employees are going on the Internet, how long they are there, and what they are downloading; and
- where telecommuting employees are connecting from, how long they are connected, what computer-based tasks they are doing while connected, and where they go to through the server.

When analyzed properly and on a timely basis, such records provide information that can help identify problems and patterns. They might also be important as evidence in court cases. The preferred hardware, software, and service providers provide these log files and perhaps the necessary analysis. Otherwise it is necessary and possible to buy software that performs the analysis.

Embedding Policies

No matter which way hardware and software is used to implement a network usage policy, there must be a complementary set of policies. The consensus is that employers have a legal right to monitor and restrict employee use of the Internet and e-mail. There also is some consensus about what the content of the related policies should be and what the best practices are for developing them. Generally, employers should:

1. involve employees in the development process, perhaps in a task force that has a representative cross-section of employees from different functional areas and different levels;
2. implement policies that respond to the business risks associated with the use of the technology and are linked to an organization's mission; and

3. educate and inform all employees about those risks to the bottom line, business continuity, and concomitantly career continuity.

These steps help ensure that employees will link the resulting policies, procedures, and practices to business mission rather than to a witch-hunt. Employee buy-in is more likely. (See the Privacy Exchange.org Web site listed in Table 4 for links to the policies of various corporations.)

In addition to implementing the policies in a manner that conforms to sound business practices, employers must implement policies that comply with the employment laws. Table 3 presents some suggestions for policy provisions that respond to the legal requirements under the federal acts. Probably the most important provision is that every policy must be enforced consistently among all members of the workforce. This prevents claims of discrimination and (inadvertent) employer complicity.

Table 3. Policy Provisions

Federal Act	Suggested policy
Title VII of the Civil Rights Act of 1964	Prohibit use of resources for accessing or transmitting materials that could create a hostile work environment (e.g., pornographic and racist materials).[a]
	Enforce usage policies consistently for all employees.
National Labor Relations Act of 1935	Enforce usage policies consistently for all employees so as not to discriminate against those involved with unionizing activities.
Fair Labor Standards Act of 1938	Require covered employees who work without direct supervision (i.e., telecommuters) to "clock in" via e-mail, employer's Web site, or telephone.
	Allow only employees not covered by the FLSA to work as telecommuters.
Electronic Communications Privacy Act of 1986	Require explicit employee consent to usage policy, especially monitoring activity. Written consent is preferred.[b]

[a]Sexual Harassment can occur when the conduct has the purpose or effect of creating a hostile work environment for another employee. The harasser does not have to intend the consequences of his/her actions.

[b]*Steve Jackson Games, Inc. v. United States Secret Service,* 36 F.3d 457; *Konop v. Hawaiian Airlines, Inc.,* 2001 U.S. App. Lexis 19206 (9th Cir. August. 28, 2001).

In addition, the policies should include specific provisions regarding attempts to circumvent the usage policies. As noted, modems can be used to establish dial-up connections to the Internet that do not use the organization's network. Thus they circumvent the network's controls and protection and expose it to security breeches and viruses. Employees also should not be allowed to download and install any software on a desktop or laptop computer, especially software that is used to erase or disguise prohibited activities. Any exceptions to this policy should require proper written authorization and supervision, and have a clear connection to personal productivity and business purpose.

Finally, and perhaps most importantly, the policies must address the proper management of e-mail. The initial concern is with e-mail content and the goal is to reduce the risk of disclosing sensitive information to inappropriate parties. (Remember that unencrypted e-mail is like sending a postcard through the mails.) It is important to reduce the size of e-mails, too, by prohibiting the inclusion of unnecessary attachments and multimedia content (music, photos, and animation). A second concern is with e-mail retention. All documents and the information that they contain have a useful life and should be destroyed when it is over. Good practices will free up valuable network resources and may prevent embarrassing disclosures. While it is illegal to "shred" e-mail in anticipation of a grand jury investigation, it is not illegal to dispose of information that no longer has any purpose in organizational communications.

Once the policies are developed, it is important to document them and convey them to employees. Again, there is a lack of consensus about the most effective and appropriate way to do this. In the 2001 AMA survey, over 80% of employers indicated that they had written policies regarding e-mail use. Most often, firms with policies used memos, company-wide e-mail, oral communication by

Table 4. Online Resources for More Information

FindLaw Cyberspace Law Center, Privacy, http://www.findlaw.com/01topics/cyber/privacy/workplace.html
GigaLaw.com, http://www.gigalaw.com/
Privacy Exchange.org, Codes & Policies of Individual Companies and Industries, http://www.privacyexchange.org/buscodes/icp/icp.html
Privacy Foundation, Workplace Surveillance Project, http://www.privacyfoundation.org/workplace/index.asp
UCLA Internet Report: Surveying the Digital Future, 2000 and 2001, http://www.ccp.ucla.edu/pages/internet-report.asp

supervisors, postings of notices in offices and notices, which appear on the individual employee's computer [1]. Some organizations use network login procedures that require an employee to explicitly respond that they understand and agree to comply with the organization's network resources policy every time they access the network. If the employee does not agree, then access is denied.

Clearly the most appropriate method for communicating the policies depends on the organization's culture and traditional communications channels. But best practices and common sense suggest methods that create an atmosphere of openness and trust, rather than one of stealth and fear. The selected method must also emphasize employee education about the risks and threats of misuse, rather than the punishments for misuse.

CONCLUSION

Networked computers are an essential component of the 21st century office environment. They are dramatically changing the relationships of employers and employees at a time when employment-related lawsuits are becoming the fastest growing type of civil cases [11]. To avoid the devastating impact that such lawsuits and their attendant publicity can have, employers and employees must be proactive and cooperative in the design, implementation, and enforcement of Internet usage policies. They also must stay abreast of current developments (see Table 4).

ENDNOTES

1. Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000 *et.seq.*
2. National Labor Relations Act, 29 U.S.C. Section 152(3). See also, Sharlene A. McAvoy, "Timekeeping Systems, Inc.: Protecting Employee Expression by E-Mail Under Sections 7 and 8 of the NLRA," *Journal of Individual Employment Rights,* Vol. 10, No. 1, 2002-2003, pp. 59-64.
3. For example, Honeywell Inc. 262 NLRB 1402 (1982).
4. Fair Labor Standards Act, 29 U.S.C. Section 203(e)(1).
5. 18 U.S.C. Section 2511(2)(i).
6. 18 U.S.C. Section 2511(d).
7. CT Public Law 98-142; NJ Wiretapping and Electronic Surveillance Control Act, NJSA 2A:156A-1; MD Code Ann Section 10-4-01-08 and others.
8. *Ryan v. Sara Lee Corp.,* No. S031479, 1993 Cal. LEXIS 2464 (Cal. Dist. Ct. App. April 29, 1993); *Semore v. Pool,* 266 Cal. Rptr. 280 (Cal. Dist. Ct. App. 1990); *Luck v. Southern Pac. Transp. Co.,* 267 Cal. Rptr. 618.
9. *Smyth v. The Pillsbury Co.,* 914 F. Supp. 97 (E.D. Pa, 1996); *McLaren v. Microsoft Corp.,* No. 05-97-00824-CV, 1999 Tex. App. LEXIS 4103 (Texas Ct. App., May 28, 1999).
10. *Luedtke v. Nabors Alaska Drilling, Inc.,* 768 P. 2d 1123 (Alaska, 1989); *Hennesey v. Coastal Eagle Point Oil Co.,* 609 A. 2d 11 (NJ, 1992).

11. Protecting Your Company Against Employee Lawsuits, HR One at SmartPros, http://www.smartpros.com/x32722.xml. Viewed May 23, 2003.

Direct reprint requests to:

Dr. Ronald R. Tidd
Associate Professor, Accounting
Central Washington University
400 E. 8th Ave.
Ellensburg, WA 98926-7484
e-mail: Ron@rrtidd.com