Communications of the IIMA

2005

Workplace Surveillance and Employee Privacy: Implementing an Effective Computer Use Policy

Scott Cox
Georgia College & State University

Tanya Goette
Georgia College and State University

Dale Young
Georgia College & State University

Follow this and additional works at: http://scholarworks.lib.csusb.edu/ciima

Part of the Management Information Systems Commons

Workplace Surveillance and Employee Privacy: Implementing an Effective Computer Use Policy

Scott Cox

Tanya Goette
Tanya.goette@gcsu.edu

Dale Young
Dale.young@gcsu.edu
Georgia College and State University
Information Systems, Communications, and Marketing
Campus Box 012, Milledgeville, Georgia 31061
Phone: 478.445.5721
Fax: 478.445.5249

ABSTRACT

Organizations face growing liability with regard to employee use of electronic resources. To mitigate the risk of liability, companies must develop and implement a computer-use policy outlining proper use of organizational electronic resources. This paper examines critical aspects of computer use policies, including: clearly explaining reasons for the policy, applying the policy to all employees including all levels of the organization, and indicating zero tolerance for offensive, harassing or discriminating communications. Finally, the paper identifies the implications of a computer usage policy.

Key Words: employee privacy, surveillance, acceptable usage policy.

INTRODUCTION

In recent years, issues related to workplace privacy and how organizations address privacy, have brought unwanted, costly litigation. In an effort to prevent such litigation, organizations are monitoring employee communications carefully. Employee surveillance and email monitoring in the workplace present a number of sometimes conflicting issues regarding an employer's need to protect its property and itself against liability and an employee's right to privacy (Adams, Scheuing & Feeley, 2000). Martin and Freeman (2003) examined key arguments for and against employee monitoring, including productivity, security, liability, privacy, creativity, paternalism, and social control. Although none of the arguments is conclusive, each outlines specific concerns brought forth by groups on all sides of the workplace privacy/email monitoring issue.

Should private organizations have the right to monitor employee communications? According to the courts, the answer is yes, and with good reason. In 1996 for example, an analysis of the computer logs by Neilsen Media Research Inc. of employees at IBM Corporation and Apple Computer Inc. found that employees of both companies had visited Penthouse Magazines' Website almost 13,000 times in a single month. They estimated this to be equal to 350 eight-hour days (Kovach, et al., 2000). This example did not lead to any litigation, however the potential certainly existed.

This paper examines the legal liability and possible financial consequences specifically related to employee privacy and email monitoring, the balance between employee rights and employer interests, and the development of an effective computer-use policy. Reasonable business judgment dictates it is legally and ethically prudent for the employer to create a written workplace privacy policy which includes monitoring of computer use while at the same time providing adequate protections for employee privacy rights in order to survive legal scrutiny. This paper provides guidelines for formulating an appropriate computer-use policy. It also identifies the implications of such a policy.

PRIVACY DEFINED

Privacy has become an extremely important part of American culture. Prior to the terrorist attacks of September 11, 2001, workplace privacy initiatives were gaining momentum. This momentum was driven by pressure from legislators and employee lawsuits (Sproule, 2002). Current fears over terrorism and homeland security have led to laws many fear will promote the deterioration of civil liberties and create a society where everyone is continually under surveillance of some kind. An example is the controversial law known as the Patriot Act. This law, enacted shortly after the terrorist attacks in 2001, gives the government sweeping power to look into a person's private life and communication regardless of the medium used for the communications (Sproule, 2002).

Privacy is freedom from unsanctioned intrusion (American Heritage Dictionary). It is an implied right based on the Fourth, Fifth, and Ninth Amendments of the Constitution (August, et al., 2001). Privacy may be invaded in four ways. The first is unreasonable intrusion upon a person's seclusion. Appropriation occurs when the use of a person's name or likeness is used for economic benefit. Third is public disclosure of private facts. Finally, false light is publicly characterizing or placing a person in a false light (Chieh and Kleiner, 2003). Most cases concerning invasion of privacy by employers involve intrusion upon seclusion.

TECHNOLOGY AND THE WORKPLACE

Employees are accustomed to using the technology made available in the workplace for purposes other than job duties. Although generally discouraged by employers, checking news headlines, doing some on on-line shopping, or sending personal emails while at work are everyday occurrences. Many still feel as though these actions go unnoticed by employers and assume, incorrectly, that their activities remain private.

Most (75 percent) medium and large companies use technology to monitor employees' email and Internet activities (George and Jones, 2003). Conversely, only 57 percent of employees think employers should have the right to monitor their email at work (Muhl, 2003). Despite employee concerns, sales of email monitoring software are expected to grow significantly, from $139 million in 2001, to an estimated $662 million in 2006 (Wakefield, 2004). Reasons cited for monitoring include: potential legal liability (68%), security concerns (60%), and employee productivity concerns (45%).

The ease of use, and the speed at which information can be sent and received, causes difficulty for managers and technology professionals. Email, for example, sometimes lacks the formality a phone call or traditional letter has. The lack of formality can cause the sender to pay less attention to the content, which may include items of a personal nature, sensitive information, or information that could be considered offensive. Add to that the possibility that a message sent in confidence may be viewed by others, or the risk of uncontrolled distribution, and serious problems could occur for both employer and employee (Adams, Scheuing, and Feeley, 2000).

LEGISLATION

One of the first and most substantial pieces of legislation relating to electronic communication and privacy is The Electronic Communications Privacy Act (EPCA) of 1986. It prohibits the interception and disclosure of wire, oral, and electronic communications. It also protects stored wire, transactional, and electronic communications from being disclosed without consent. Violations of either can result in criminal or civil liability (Kovach, et al., 2000).

There are three exceptions to the ECPA that give employers a means of bypassing personal privacy rights. The first, known as the "business exception," allows an employer to intercept communication, if done in the ordinary course of business, using a qualified device. The second, called the "consent" exception, states an employer may monitor communication if at least one individual consents to the interception. Finally, the "service provider" exception states that an employer providing a wire or electronic communications service (e.g., email, voicemail) may retrieve information maintained on that person's system in order to protect the employer's property rights. ECPA is the basis upon which right to privacy cases regarding electronic communications in the workplace are judged.

LITIGATION

Two important cases concerning privacy and the workplace are *Smyth v The Pillsbury Company* and *Bourke v Nissan Motor Corporation. Smyth v The Pillsbury Company (1996)* was significant because it was the first federal decision to state that a private sector, at-will employee has no right to privacy with regard to the content of email when it is sent over an employer's email system (Smith and Faley, 2001). An employee of Pillsbury was terminated

following the interception of an email containing statements deemed inappropriate by the company. The company had issued assurances to employees that email communications would be confidential, and would not be intercepted or used as grounds for termination or reprimand. The employee received email from his supervisor on his home computer. He exchanged emails with his supervisor. At some later date, contrary to the assurances of confidentiality made by Pillsbury, the private e-mail messages were intercepted. Shortly thereafter, the employee was terminated for transmitting inappropriate and unprofessional comments over the e-mail system. The court found that no reasonable expectation of privacy existed and the termination was upheld.

In *Bourke v Nissan Motor Corporation (1993)*, a state judge in California upheld the termination of two employees whose email messages contained what were deemed inappropriate remarks concerning their supervisor. The judge ruled the company had a right to read the email because it owned and operated the computer equipment. During the demonstration and training session of the company email system, the trainer randomly selected a message sent by Bourke to another employee. The email selected was of a personal, sexual, nature and not business related. The trainer reported the incident to her supervisor. Management authorized a review of all email messages, finding additional emails from Bourke containing similar messages. Bourke resigned following threat of termination. The employee with whom she communicated was terminated. Each eventually filed suit for wrongful termination as a result of invasion of privacy. The courts found in favor of Nissan.

The theme for both of these cases, and the basic test for cases where workplace privacy is concerned, is "reasonable expectation of privacy." As a result of the ambiguity of privacy law, courts must decide on a case-by-case basis whether an employee has a reasonable expectation of privacy. Courts must balance the invasion of privacy claim against the need for supervision and control of the business (Adams, Scheuing, and Feeley, 2000).

Employers are being held liable for the atmosphere in the workplace. They can be liable for harassment (e.g., sexual, racially discriminatory) that creates a hostile work environment. Employers have been found liable for failing to monitor and prevent inappropriate e-mail once put on notice by employees. In *Blakey v Continental Airlines (2000)* the court ruled that an employer had a duty to remedy electronic harassment because it had received notice that the employees were posting defamatory and harassing messages on the company's electronic bulletin board.

A company can incur financial liability when IT resources are misused. Female employees sued Chevron alleging it allowed its internal email system to be used to transmit sexually offensive messages. They cited a joke sheet circulated by email. The company settled when a copy of the email was located on its email server, paying more than $2.2 million in damages (Soewita and Kleiner, 2000).

More recently, the CEO of Boeing, Harry Stonecipher, resigned following a tip that he was having an extramarital affair with a coworker. The issue was brought to the company's attention in a letter, to which was attached an excerpt of a sexually graphic email sent by Stonecipher. The actions of Stonecipher violated the firm's strict code of ethics policy, of which he was a proponent. This case reinforces the idea that email is not private (Richman, 2005). The sexually graphic content of the message sent by Stonecipher, although intended to be private, could result in internal harassment or discrimination claims by employees involuntarily subjected to offensive content. This case is an example of the relationship between privacy and sexual harassment as it relates to digital communication and technology resources in the workplace.

SURVEILLANCE METHODS

Firms should carefully consider electronically monitoring employee e-mails and Internet activities. There are delicate issues of trust and loyalty that should be addressed in order to preserve the culture of the organization. Monitoring requires proper planning, clear policies, and detailed procedures (Arendt, 2004). Both opponents and proponents of monitoring agree that organizations need clear and definitive policies on electronic surveillance, and that these policies should be frequently and clearly communicated to employees. They also agree that employees should undergo formal training on e-mail and Internet policies, proper usage, and conduct (Agarwal and Rodhain, 2002). Given the potential liability facing organizations as a result of the misuse of technology resources by employees, steps must be taken by managers and IT departments alike to mitigate the risk involved in allowing employees unfettered access to the Internet and company email systems.

Email Monitoring

The number of U.S. firms that monitor e-mail usage has tripled in the last few years (Segarnick, 2002). Proponents for e-mail monitoring maintain that employers must take proactive steps to insure business interests are protected,

such as making certain the work environment is free from hostile and harassing activity. Organizations must secure sensitive company information, including trade secrets, intellectual property, and customer, employee, and financial data (Miller and Weckert, 2000). Proponents also believe monitoring ensures that employees maintain efficient and productive work habits, which should boost efficiency, increase productivity and improve customer service.

Some of the arguments against email monitoring include the loss of respect and trust for the employer, which result in higher turnover, loss of productivity, and decay in a positive work culture. Opponents of monitoring also believe that monitoring costs the company more than it saves, because it is a distraction from getting the business of the business done.

Internet Monitoring and Filtering

The Internet can be a tremendous distraction to employees with Internet access. Just like email, when it comes to potential employee abuse of the Internet, employer concerns are related to loss of productivity, degradation of available IT resources, and the high risk of liability (Lim, 2002).

Organizations that provide their employees Internet access expect some personal use. This usage is really no different than allowing some "reasonable" amount of personal calls using company telephones. However the Internet poses a much greater opportunity for abuse. An employee checking the stock market may seem harmless, but what if that employee expands their activities to continual tracking of stock quotes, in-depth research and online day trading? Now suppose many employees exhibit this same behavior. Company IT resources could potentially be slowed enough to affect productivity.

Firms employ filtering or blocking systems to prohibit access to certain Websites. When a user clicks a link or enters a Web site address, it is matched against a database of inappropriate sites. If the requested site is found on the list of blocked sites, the user gets a message that access to this site is contrary to company policy and who to contact if they think they have a legitimate reason for accessing the site (Lichtash, 2004).

COMPUTER USE POLICIES

Ensuring proper use of organizational technology begins with outlining what is proper and what is not. "Apathy towards e-mail and Internet policies is the biggest mistake an employer can make" (Adams, Scheuing, and Feeley, 2000). Outlining proper usage provides a tremendous advantage to employers should litigation over privacy issues become necessary, in that it lays the foundation for a business to employ surveillance technology to protect company interests. Properly documented and implemented computer usage policies provide employees the knowledge to use company resources without subjecting themselves to possible embarrassment or disciplinary action. An example of a computer use policy is detailed in Table 1. This guide comes from a report issued by The U. S. Government Accounting Office detailing the computer use monitoring practices of selected companies (GAO, 2002).

Monitoring Practice	Key Elements
Monitoring use of proprietary assets	Statements that company computing systems are provided as tools for business and all information created, accessed, or stored using these systems are the property of the company and are subject to monitoring, auditing, or review.
Establishing no expectation of privacy	Statements about the extent or limitations of privacy protections for employee use of e-mail, the Internet, and computer files.
Improper employee use described	Statements that some uses of company computers are inappropriate – including specific notice banning offensive material (e.g., obscenity, sexual content, racial slurs, derogation of people's personal characteristics).
Allowable computer use by employees described (i.e., what employees are, and are not allowed to do with computers)	Statements explaining proper or acceptable uses of the company systems, including whether or not personal use is permitted.
Protecting sensitive company information	Statements providing instructions for handling proprietary information on company systems.

| Disciplinary action | Statements that there are penalties and disciplinary actions for violations of company usage policy. |
| Employee acknowledgement of policy | A statement requiring that employees demonstrate they understand the company policy and acknowledge their responsibility to adhere to the policy. |

Table 1: Key Elements of a Computer-Use Policy. Source: GAO (2002).

A starting point for any organization should be consultation with their legal counsel and other relevant parties (e.g., human resources, employees, and, if applicable, union representatives) to determine what type and scope of policy would be best suited for the organization. Organizational culture must be given consideration in such discussions. The end result should be a policy that balances the employer's right to protect its interests with the employee's right to privacy (Kovach, et al., 2000). This balance between interests and privacy is of great interest given recent increases in cyber attacks (Evers, 2005) and the potential for misuse of electronic identification (Gilbert, 2005).

An acceptable computer use policy includes the following items (Policy, 2000; Adams, Scheuing, and Feeley, 2000).
- Reasons for the policy should be clearly explained.
- The policy should apply to all employees including all levels of the organization.
- Employees should be informed that company equipment belongs to the company and is to be used for business purposes only; some personal use might be allowed and should be specified.
- Employees should be informed that all messages and information stored on company resources become company property and remain confidential unless made public by the company.
- The policy should indicate zero tolerance for offensive, harassing or discriminating communications.
- The policy should prohibit employees from encrypting email without company permission.

POLICY IMPLEMENTATION

An organization should train employees on proper use of company computers and email. Additionally, the implementation should (Totten, 2004; Morris, 2003):
- Be in writing and placed in appropriate company employee manuals and literature.
- Be given to each employee who, in writing, acknowledges receipt thereof.
- Remind employees yearly of the existence and content of the policy.
- Let employees know their voice mail, email, or computer files and hard drive will be subject to monitoring at any time and without notice (computer screen warnings regarding proper use should flash on when employees first log-on and they should be informed if the company is employing content monitoring or blocking software).
- Indicate that password protection does not guarantee the employee immunity from employer access.
- Indicate that any violations of the policy could lead to disciplinary action up to and including termination.
- Recognize that some personal use of the company computer is going to occur and will be tolerated (in the same sense as phone calls) but that improper use (e.g., shopping or on-line gaming during working hours, or visits to offensive sites) will not be tolerated.

The implications of a computer use of policy are summarized in Figure 1. The figure notes that computer usage must balance both employer and employee interests.
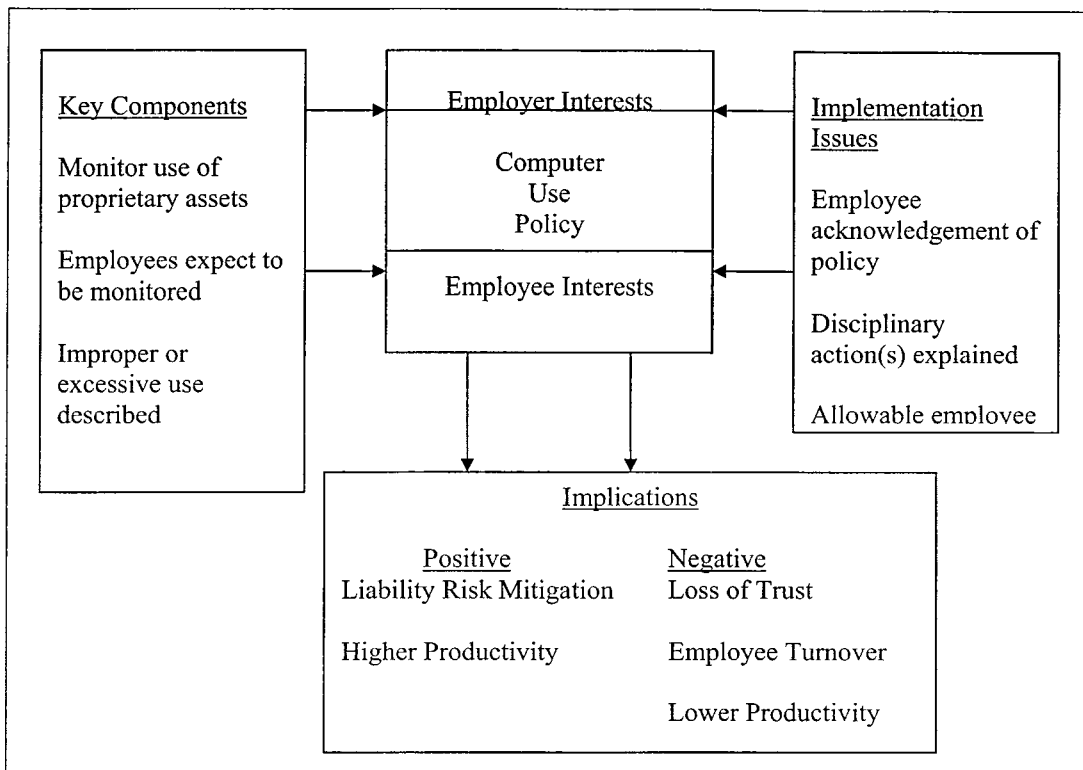
Figure 1: Implications of a Computer-Use Policy.

There are currently no state or federal laws requiring that employers adopt an acceptable computer use policy (Lichtash, 2004). There is also no guarantee that having such a policy will completely protect the employer from liability for claims of invasion of privacy brought by employees. Given that most employees will likely follow a properly designed and implemented policy, the courts will likely deny an employee's invasion of privacy claim absent a complete disregard of that right by the employer. However, employers must be careful when monitoring not to violate labor or anti-discrimination laws by "targeting" specific employees (Segarnick, 2002). In addition, it is important to establish employee trust and properly train employees before implementing monitoring technologies (Lindquist, 2005).

ORGANIZATIONAL IMPACT

Companies are developing strategies that lead to more satisfied employees and encourage employee loyalty among highly-skilled, knowledge workers (Smith and Faley, 2001). Restrictive computer use policies have the potential of negatively affecting the organization by creating an atmosphere of employee mistrust of management. "If a firm is trying to develop and transform information into a competitive advantage, a sense of loyalty is needed" (Smith and Faley, 2001). Monitoring can be seen as a sign of mistrust by employees, which could lead to a less efficient workforce and the loss of organizational talent (Miller and Wiekert, 2000). While customer data privacy violations attracts a great deal of litigation (Patton, 2004), employee monitoring also results in legal actions and labor disputes (Lindquist, 2005).

Besides the loss of productivity for the employees that are abusing their Internet access privileges, another major employer concern is clogged bandwidth, degraded system performance, and over-consumption of finite computing resources that can indirectly reduce the productivity of non-abusing employees (Liebert, 2004). In some cases, the ripple effects can be devastating. Consider the problems with PointCast's push technology that provides news and data services directly to a desktop. Businesses found significant percentages of their employees with access to the Internet were getting large quantities of real time data, such as news stories and stock ticker data, 'pushed' to their

desktops. They were experiencing an unanticipated, double-digit percentage loss of bandwidth (CIO, 1997; Information Week Online, 2000). The same risk exists with streaming audio and video. While the music may be free to those who listen to it, it's certainly not free to the employer who pays for the Internet connectivity. The defense organizations employ to stop push technology and streaming media from clogging bandwidth is blocking/filtering technology.

While the abuse of IT resources has an impact, so to does monitoring those resources. Sophisticated systems can automatically store both incoming and outgoing messages. Organizations that employ email monitoring for instance, must provide storage for the enormous amounts of email generated. Monitoring and filtering of e-mail, for example, can slow systems performance and thus generate productivity costs for an organization.

IMPLICATIONS

Employers are looking for ways to limit employees' expectations of privacy in the workplace by implementing restrictive computer use policies. The possibility of lower productivity, the temptation to use those resources for purposes other than official business, and the legal implications for the employer must be addressed (Kovach, et al., 2000). However, these restrictive policies may have a negative impact and may actually do just the opposite of what was intended. Organizations must be sensitive to the needs of employees for privacy as they implement performance measurement to develop a sustainable competitive advantage. It is conceivable that organizations could lose quality employees who do not feel trusted by their employer. Employers must differentiate between spying and legitimate monitoring in the workplace (Smith and Faley, 2001). Employers that use monitoring technology face the possibility of creating an atmosphere of distrust in the workplace. An employee who feels no sense of trust from the employer lacks the incentive to be efficient and could be less productive (Smith and Faley, 2001).

Where should an organization draw the line? What constitutes legitimate monitoring and what is simply spying? From a legal perspective, it's clear that businesses have tremendous latitude when it comes to workplace surveillance. It seems fruitless to argue or expect that privacy should prevail over management rights. Protection of organizational interest has been upheld over the individual rights to privacy in court cases to date. However, organizations must recognize that some activities have a limited investment return. For example, with the exception of support center telephone operators, few telephone conversations are monitored because some casual or personal usage is expected and tolerated.

Alternatives to active monitoring are also being used that are less invasive to personal privacy. Many organizations use passive methods such as filtering software that prohibits employees from visiting specific Websites or using third-party email programs such as MSN Hotmail. This solution is generally accepted to be the better alternative to monitoring as employees don't feel a sense of rights violation (Miller and Weckert, 2000). Employees accept that some things simply aren't accessible and therefore don't attempt to use them. System administrators use filtering software to monitor email and Internet traffic, to stem unapproved use of IT. Third-party email programs, Internet radio Websites, and many e-commerce Websites are not accessible on corporate computer networks.

Therefore, organizations have a range of options - - do nothing or monitor everything - - to balance privacy needs with unrestricted control of computer usage. Employee education, especially regarding improper or harassing content is important. Some monitoring is obviously necessary, but is not a substitute for voluntary, responsible behavior by employees. Corporate culture can help set standards and provide peer pressure for such responsible behavior as it does for basic issues such as what does and does not go on an expense report, or how employees (mis)treat access to supplies.

CONCLUSION

It seems reasonable to expect that employees should have some level of privacy at work and employers should not be allowed to open completely private emails. Any computer use policy should include a system for marking personal versus business email in order to alleviate confusion, or clearly state that all e-mail is subject to monitoring. Given the risk of legal liability, productivity loss, and drain on bandwidth, it's clear why organizations must implement acceptable use policies and monitor resource usage. Managers and technology professionals must take steps to ensure the negative impact is minimized.

Workplaces subjected to high surveillance typically are culturally troubled, where trust is missing. Data collected during monitoring is subject to misuse in ways that could subject the organization to liability. Opponents worry that, without proper checks and balances and adequate corporate governance, employers may abuse monitoring (Hodson,

Englander, and Englander, 1999). However, disgruntled employees can cause an organization legal problems and liability in other ways, such as by writing a letter, having a conversation, sending a fax or making a phone call just as easily as by sending an e-mail or misusing the Internet.

Additional research could include surveys of organizations to compare the impact of usage policies on employee behavior. Do some policies work better than others? Have some policy statements proved to be unenforceable? What types of work environments are most liable for excessive or improper usage? Are computer usage policies affected by organizational culture and an emphasis on ethical behavior by employees?

REFERENCES

Adams, H., S. Scheuing, & S. Feeley, (2000). E-Mail Monitoring in the Workplace: The Good, the Bad and the Ugly. *Defense Counsel Journal. 1,* 32-46.

Agarwal, R., & F. Rodhain, (2002). Mine or Ours: Email Privacy Expectations, Employee Attitudes, and Perceived Work Environment Characteristics. Proceedings of the 35th Hawaii International Conference on System Sciences, Hawaii.

American Heritage Dictionary. 3rd Ed. (2000). Houghton Mifflin Company. Boston.

Arendt, L. (2004). Keeping an Eye on Employees. *Corporate Report Wisconsin,* 19, 32-35.

August, R., G. Ferrera, S. Lichtenstein, Reder, M., & W. Schiano, (2001). *cyberLAW* Cincinnati, OH: South-Western College Publishing

Blakey v. Continental Airlines, Inc. (1998). 2 F. Supp. 2d 598, 603 (D.N.J. 1998).

Bouke v. Nissan Motor Co. (1993).No. B068705 (Cal. Court of App., 2nd Dist., July 26, 1993)

Chieh, C., & B. Kleiner, (2003). How Organizations Manage the Issue of Employee Privacy Today. *Management Research News, 26,* 82-88.

CIO   Magazine.   (1997).   *Pushing   It.*   May   1, Retrieved   April   10,   2005,   from: http://www.cio.com/archieve/050197/_push.html

Evers, J. (2005). Panel paints grim picture of cybercrime battle. *News.com,* June 1.

GAO (2002).Employee Privacy: Computer-Use Monitoring Practices and Policies of Selected Companies. U.S. GAO. Committee on Education and the Workforce, House of Representatives

George, J., & G. Jones. (2003) *Contemporary Management* New York, NY: McGraw-Hill.

Gilbert, A. (2005). California bill would ban tracking chips in IDs. *News.com,* April 28.

Hodson, T., F. Englander, & V. Englander, (1999). Ethical, Legal, and Economic Aspects of Employee Monitoring of Employee Email. *Journal of Business Ethics, 1,* 99-108.

Information Week Online. (2000). *Push Technology Matures – And Makes A Comeback. July 10,* Retrieved April 10, 2005, from: http://www.informationweek.com/794/portal.htm

Kovach, K., J. Jordon, K. Tansey, & E. Framinan, (2000). The Balance Between Employee Privacy and Employer Interests. *Business and Society Review, 2,* 289-298.

Lichtash, A., (2004). Inappropriate Use of E-mail and the Internet in the Workplace: The   Arbitration Picture. *Dispute Resolution Journal, 59,* 26-36.

Liebert, M., (2004). Development of a Measure of Personal Web Usage in the Workplace *CyberPsychology & Behavior, 7,* 93-104.

Lim, V. (2002). The IT way of loafing on the Job Cyberloafing, neutralizing and organizational justice. *Journal of Organizational Behavior, 23,* 675-694.

Lindquist, C. (2005). Watch Carefully. *CIO,* May 15.

Martin, K., & R. Freeman, (2003). Some Problems with Employee Monitoring. *Journal of Business Ethics. 4,* 353 – 361.

Miller, S., & J. Weckert, (2000). Privacy, the Workplace and the Internet *Journal of Business Ethics, 28,* 255-265

Morris, F., (2003). The Electronic Platform: Email and Other Privacy Issues in the Workplace *Computer and Internet Lawyer, 20,* 1-9.

Muhl, C., (2003). Workplace e-mail and Internet use: employees and employers beware. *Monthly Labor Review.* 2, 36-45.

Patton, S. (2004). Privacy is Your Business. *CIO,* June 1.

Policy, S., (2000). Employer monitoring of employee Internet and email use: An Effective Litigation Avoidance Tool. *Computer and Internet Law, 17,* 21-23.

Richman, D (2005). E-mails sent at work anything but private. (March 9) The Seattle Post-Intellgencer http://seattlepi.nwsource.com/business/215147_email09.html

Segarnick, K. (2002). Courts Say It's Ok: Peep away. *CIO,* June 1.

Smith, A., & R. Faley, (2001). Email Workplace Privacy Issues in an Information-and Knowledge-based Environment *Southern Business Review, 27,* 8-22.

Smyth v. Pillsbury Co. (1996). 914 F. Supp. 97 (E.D. Pa. 1996)

Soewita, S. & B. Kleiner, (2000). How To Monitor Electronic Mail To Discover Sexual Harassment. *Equal Opportunities International. 19,* 45-47.

Sproule, C., (2002). The effect of the USA Patriot Act on workplace Privacy. *Cornell Hotel and Restaurant Administration Quarterly.* 43, 65-73.

Totten, J., (2004). The Misuse of Employer Technology by Employees to Commit Criminal Acts. ABA Section of Labor and Employment Law Technology Committee Midyear Meeting, Miami, Fl.

Wakefield, R., (2004). Computer Monitoring and Surveillance: Balancing Privacy with Security. *The CPA Journal.* 7, 52-55.