Sacred Heart University
DigitalCommons@SHU

WCOB Faculty Publications

Jack Welch College of Business

2006

Ethical and Managerial Implications of Internet Monitoring

Andra Gumbus
Sacred Heart University, gumbusa@sacredheart.edu

Frances Grodzinsky
Sacred Heart University, grodzinskyf@sacredheart.edu

Recommended Citation

Gumbus, Andra and Grodzinsky, Frances, "Ethical and Managerial Implications of Internet Monitoring" (2006). *WCOB Faculty Publications.* Paper 129.
http://digitalcommons.sacredheart.edu/wcob_fac/129

Ethical and Managerial Implications of Internet Monitoring

Andra Gumbus
Welch College of Business
Sacred Heart University
5151 Park Avenue
Fairfield, CT 06825
(203) 396-8271
gumbusa@sacredheart.edu

Frances S. Grodzinsky
Computer Science / Information Technology
Sacred Heart University
5151 Park Avenue
Fairfield, CT 06825
(203)371-7776
grodzinskyf@sacredheart.edu

ABSTRACT

As Internet use pervades our personal and professional lives, organizations have become increasingly concerned about employee use of the Internet for personal reasons while at work. This has prompted the restriction of the Internet or the limitation of the Internet during work hours. Monitoring of employee Internet and email is another result of this trend. Legitimate business functions such as employee performance appraisal and progress toward goals are served by monitoring. However, poorly designed and communicated monitoring practices can be negative and have perverse effects on employee morale and productivity. Monitoring of employees erodes trust and may be considered an invasion of privacy. In this paper ethical issues surrounding Internet monitoring are explored from two perspectives: university and business use. Survey results from the university perspective are compared with computer monitoring in a business setting. Students feel an invasion of privacy when a university setting monitors computer use, however they consider the practice of monitoring the workplace an acceptable invasion of privacy. Reasons cited for unethical monitoring at a university or business setting include: payment for the computer, personal property and possession by the student, and limitations of personal freedom, rights, trust and privacy. Reasons cited for the ethical use of monitoring include: academic use of the Internet, workplace requirements and payment for work, discouragement of hate crimes and terrorism, and university or employer property.

Keywords

Internet, World Wide Web, Productivity, Computer Ethics, Business Ethics

1 PRIVACY AND PRODUCTIVITY

Employers have a legal right to monitor productivity of workers while workers have the right to be told how they are watched. Justification from the company perspective includes keeping employees safe and data secure (particularly after September 11). Firms can spot warnings of possible sexual harassment, corporate espionage, and flag words like bioterrorism and anthrax. However, they can also monitor job search sites that can alert the company to problems in departments or anticipated turnover. Should the firm be privy to this information or does it violate employee privacy?

In a Harris survey conducted for WebSense a majority of employees would give up coffee before Internet access. Half of 500 employees admitted using the Internet for news (81%) email (61%) banking (58%) travel (56%) and shopping (52%) (Soat, 2005).Surreptitious monitoring can and does occur when employees are on company time using company resources, with little legal protection available for employees. WebSense, the producer of the most commonly used monitoring software reports an estimated annual cost of 53 million employees cyberloafing to be $ 138 billion. A program called Investigator developed by WinWhatWhere Corporation has 100 corporate and government clients in Canada and monitors all activity including deleted or unsent messages and can scan for words such as " boss" and " union". It is installed after hours as an " upgrade" and cannot be detected by employees. President of the National Workrights Institute, Lewis Maltby stated, "Employer's efforts to prevent abuse often lead to serious invasions of privacy. People are not robots. They discuss the weather, sports, their families and many other matters unrelated to their jobs at work that can be highly personal.' (Thibodeau, 2000).

The employer has an unchallenged right to monitor the workplace virtually, but the issue of monitoring the home for telecommuters poses a different concern of invasion of privacy. The proliferation of technology at home and in the workplace will escalate the friction between privacy and productivity. " Whether it's sexual harassment, hate mail, or just goofing off, these new technologies can make it easier for workers to commit misdeeds – and to amplify their effect. At the same time, technology enables employers to monitor workplace activity and be more aware of the violations." (Van Slambrouck, 2000).

The organization has an obligation to inform employees that they have no privacy when it comes to the workplace. Many companies do not educate employees on Internet privacy issues and do not specify acceptable Internet usage and communicate it to their staff. Maltby of the National Workrights Institute (ACLU) stated, " you should take your passport when you go to work because all your rights as an

American citizen disappear the second you walk through the office door. He argues that the protections of the right to free speech, privacy, and freedom from arbitrary punishment are absent in the workplace. Ironically, these freedoms are virtually guaranteed for the top level executives who are usually immune from workplace monitoring practices. Some view Sarbanes – Oxley as the vehicle for monitoring that is needed in the executive suite. (Sandberg, 2005). Forrester Research claims a growth rate of 30% a year driven by corporate compliance to Sarbanes-Oxley as well as the need to eliminate inappropriate content. A sample of red flag words that are scanned in email include: porn, sex, promise, guarantee, exceed, beat, sure thing, easy money, medication, patient record, boss, client file, meds, SSN, ID#. (Tam, White, Wingfield, Maher, 2005). If the word is found in an employee's internet activity an alert is generated and emailed to the manager. Managers can receive summaries or log onto a web site to view real time Internet traffic. The web monitoring software StellarIM cost the company $ 8000. (Roberts, 2005).

Although monitoring the Internet has increased, the last workplace privacy law was enacted in 1986 before the proliferation of the Internet. Increasing incidences of identity theft, hackers, phishing, pharming, bot networks and other cybertricks has resulted in the Secret Service uncovering 4000 suspects, 1.7 million credit cards numbers, access to 18 million email accounts and counterfeit documents. (Grow, 2005). Identity thieves usurp personal information and it is estimated that only 1 in 700 are convicted if caught. Identity theft is lost by the neglectful practices of companies that do not safeguard personal information. Examples are: leaving unencrypted information on computers, selling it to criminals, stolen laptops, lost data, stolen UPS boxes with company data, hacking, failure to monitor employees and other cons and scams. Unfortunately, companies are not punished for the resulting identity theft. A current bill in Congress proposes fines and other penalties for companies' failure to protect personal information and would require corporations to protect customer data. (Levy and Stone, 2005). The circulation of internal emails with private payroll and benefits information have revealed weaknesses in the California privacy law. (Verton, 2004). Bills increasing employee rights have not passed Congress in 1994 and 2000 and the Notice of Electronic Monitoring Act (NEMA) would have required notification to employees. Conley argues that trusting employees and respecting individual rights is a better path than electronic surveillance. It does not invade privacy and deplete morale and productivity. He argues that if employees aren't motivated in the first place adding surveillance will only make matters worse not better. (Conley, 2004).

2 ETHICS OF PRIVACY AND TRUST

Are employers snooping unnecessarily or are they protecting themselves against legal liability? Drawing the line and maintaining a balance between detecting misconduct and protecting rights to privacy can be a difficult balancing act. The International labor Organization (ILO) reported that big brother jeopardizes employees health and welfare. Increased stress and adverse working conditions such as lack of involvement and control over tasks, reduced task variety and supervisory support, fear of job loss, and reduced social support can result from monitoring. Excessive monitoring can be ounterproductive and result in low morale and depression that affect productivity. (Hall, 2004).

The historical meaning of privacy (as the right to be left alone based on respect for the person) takes on a whole new dimension in the age of technology. Technology invades privacy because others not only have access to knowledge, but can have more knowledge than the individual (Robison, 2000). Privacy as a vehicle for respect for persons can be classified as a moral value from a deontological as well as a consequentialist perspective. Privacy can also be viewed as a virtue to be protected and defended as a moral right. (Stahl, 2004). Others view privacy as intellectual property where information about the person is that person's property and should not be violated. (Hunter, 1995). Monitoring employees violates privacy and intrudes upon the sense of security and individuality that is a necessary component of a trusting relationship. Is an employee autonomous in the workplace? Is the employee or the company responsible for balancing personal privacy and organizational security? Should an individual manager have the sole responsibility for acting on the information received from monitoring software? Stahl argues that individuals do not have the power, knowledge or intellectual capacity to objectively deal with these ethical questions involving privacy and information assurance. (Stahl, 2004). If managers are not equipped to respond to these difficult issues, who is ultimately responsible?

The issue of monitoring raises an important aspect of the employee / employer relationship with regard to privacy and trust. Employees may view their privacy being invaded by the company practice of monitoring and blocking web sites and emails. It may also be perceived as a lack of trust and can be counterproductive by causing anger among employees monitored. Does the company respect employee privacy? If the company has to restrict access should it provide Internet at all? Will the workplace relationship be compromised by tracking employee activities in virtual space? The Internet should be a positive productivity tool not a liability. In a recent study, managers expressed concern about the social costs of disrupting the relationship with employees by breeching trust, fairness and privacy. The cost spent in time and energy monitoring, interpreting and acting on data on multiple subordinates can also be a deterrent to electronic monitoring. Ethical concerns about secretly monitoring employees were also indicated. It was found that the decision to monitor secretly carries greater risk of a negative reaction of mistrust, invasion of privacy and injustice than informing employees of monitoring activity.

(Alge, Ballinger, & Green, 2004). Is the IT department acting unethically eroding human dignity and privacy by monitoring employees? Is the company acting ethically when they monitor because they own the equipment and the information is accessed through IT assets? (George, 2000).

Taylor states that we should distinguish overt and covert invasions of privacy. Employees are aware they are monitored in overt invasions and are unaware in covert invasions of privacy. Taylor argues that employees will avoid personal web surfing thereby reducing their individual autonomy if they know they are being watched. No loss of autonomy occurs when employees are free to surf the web and are unaware they are monitored. (Taylor, 2000). Passive monitoring may be a common ground between overt and covert invasions where the company records information on Internet use and email but managers access it only if a suspicion of abuse exists. One may argue that the prosperity of the business is more important than privacy and that " is the business goes well, both employers and employees benefit, no matter how much the employees' privacy rights are violated." (Petrovic-Lazarevic and Sohal, 2004).

Ladson and Fraunholz surveyed six large organizations with respect to online privacy attitudes and policies and the level of employee awareness. The importance of policies as instructional manuals and preventative documents was stressed. The organizations felt that policies on online and offline privacy and acceptable Internet use and email are important to privacy and online security. However, implementing training of employees on these policies was not considered important. (Ladson and Fraunholz, 2005). Chen and Park found that control in the electronic surveillance workplace strongly influences trust and concern for privacy. If employees have some control over the surveillance and monitoring equipment it may make up for the loss of trust when implementing monitoring technology. Control is vital to privacy and when employees have control over monitoring technology their privacy concerns are lessened. Control is recommended as a low cost and effective way to reduce privacy concerns. (Chen and Park, 2005).

3 MANAGERIAL DILEMMAS: ETHICAL ISSUES

Keeping employees focused on work related tasks and enhancing productivity are managerial responsibilities. A study of the impact of the Internet on productivity can be instructive for managers by making them aware of the negative effects on productivity and helping managers address problematic employee behavior. Employees need to feel valued for their work and that they are treated fairly and justly in the exchange process between manager and employee. Strong cultures with explicit norms of behavior and IT ethical codes of practice are conducive to curtailing cyberloafing. Norms such as reciprocity, explicitly stating tolerable behaviors and consequences in a written and well communicated policy that governs the use of the Internet will aid managers as they interpret policy. Peterson examined the influence of guidelines and universal moral beliefs on the use of computers in the workplace and found that clear computer guidelines had a positive effect on business professionals with a low belief in universal moral rules. He supports the need for ethical guidelines for computer use as a simple and inexpensive way to discourage the unethical use of computers and educate users to inappropriate use of company property (Peterson, 2002).

The ethical culture of an organization is a reflection of the ethical values of the managers and may be stated in an ethics credo or code and reinforced through education of employees to that code of ethical conduct. Ethical codes can be a deterrent to unethical behavior. The punishment of unethical behavior sets a powerful example for employees. However, managers have differing views on what constitutes a breach of ethics and differ in the interpretation of a company code making enforcement a difficult moral choice. Another difficulty is posed by the frequency of technological changes causing differing interpretations on ethical behavior in eBusiness (Petrovic-Lazarevic and Sohal, 2004).

Managers face the dilemma of needing to curtail cyberloafing and not offend or limit employee freedom. Should managers allow lapses in productivity for the sake of employee satisfaction? In order to answer this question, Urbaczewski and Jessup studied employee satisfaction with electronic monitoring. They distinguished electronic monitoring (EM) for simple feedback purposes versus monitoring for control which reports compliance with Internet acceptable use policies. They found less satisfaction with EM for control of cyberslouching and greater satisfaction with EM for feedback that was generally positive and constructive in nature. They recommend a hybrid approach that allows managers to influence employee behavior in an acceptable way that high performers will tolerate, and that low performers will dislike with desirable results for management. "Fortunately it appears positive forms of monitoring can be more instructive and acceptable to employees than negative forms of monitoring. Alternatively, managers might employ different EM techniques for different employees: using EM for feedback for high performers and EM for controlling for problematic employees." (Urbaczewski & Jesup, 2002).

4 RESEARCH RESULTS: UNIVERSITY

A survey was conducted with 173 Sacred Heart University students on the topic of internet monitoring. Both undergraduates and graduate students participated from the USA campus as well as the Luxembourg campus. Students were from the following courses: 19 graduate level Luxembourg students taking Team Management, 47 undergraduate students taking Organizational Behavior, 46 undergraduate students taking Computer Sciences, and 61 undergraduates taking Business Ethics. Of the 173 respondents 114 are male and 59 female. Students under age

21 totaled 116 and there were 57 aged 21 or over. Both Business Ethics and Computer Science students had course modules on privacy whereas the Organizational Behavior and Team management students did not. Students were asked to respond to whether they felt that monitoring was an invasion of privacy and unethical at a university setting as well as in the workplace. Qualitative results indicated an overwhelming response to the feeling that the university has no right to monitor internet use because it limits personal freedom, rights, trust and privacy. Qualitative comments fell into four different categories when analyzed for why students thought it was unethical for the university to monitor. These categories are: students pay for the computer so they feel a sense of ownership: it's assumed to be personal property or a possession of the student; it limits personal freedom (rights, trust and privacy); and the internet is needed for academic use. There were three categories identified in qualitative comments that indicate an acceptance of monitoring as ethical and needed. These are: workplace requirement; monitoring discourages hate crimes and terrorism; and the final category of the internet and all computer equipment are SHU property and the school has the right to know what students are doing.

University students were asked if monitoring Internet usage is an invasion of privacy at the university and an overwhelming 65% responded yes. For those under age 21, 67% felt this is an invasion of privacy, and for those over 21 years of age 34% responded that monitoring is an invasion. Knowing that the university monitors Internet use causes 31 % to admit that this knowledge alters their Internet behavior. When asked if they consider monitoring unethical 57% responded yes. Fifty six percent of students under age 21 felt monitoring is unethical, and 33% of those over 21 felt the same.

When asked if they considered restricting the use of their computer unethical 72% responded yes. Of the 72 % of students responding yes to the question about restricting of their computer there were only slight differences among the men and women surveyed. Seventy seven per cent of males and 61% of females felt the restriction was unethical. When the same question was analyzed by type of student the results were different and noteworthy. Computer science students who responded that restriction was unethical represent 69% of all computer science students surveyed. For Business Ethics students the percentage was 86, for Organization Behavior students the percentage was 67, and for the graduate Luxembourg based students only 37 % felt that restriction was unethical. Students who responded yes to both questions about an invasion of privacy and unethical were 48% of the surveyed population.

Out of 173 responses, 110 written comments indicate students feel their privacy is invaded by monitoring. Interestingly, invasion of privacy was more evident and important to the students who had taken course material on privacy in their business ethics and computer courses. Approximately half of the ethics students and three-fourths of the computer science students felt it was inappropriate for SHU to monitor their email and internet sites. Invasion of privacy was most important to graduate students as well. Out of 19 surveyed, 15 responded that it was unethical for the university to monitor.

5 RESEARCH RESULTS: WORKPLACE

In sharp contrast, responses to identical questions regarding monitoring at the workplace are markedly different with respect to perceptions of privacy. Only 32% of respondents feel that workplace monitoring invades their privacy. Twenty four percent of students under 21 felt monitoring invades privacy and 15% of those over 21 felt the same. This knowledge affects only 52% of employee s' behavior on the Internet. Only 34 % feel that monitoring is unethical and a mere 37% think that restricting use in the workplace is unethical as compared to 72% in a university setting. Age differences were not significant as a factor in response to this question. Twenty five percent of those under 21 and 27% of those over 21 responded yes to this question. Women and men were similar in their belief that restriction was not unethical (63%). Thirty six percent of male respondents and 39% of female respondents felt that restricting was unethical. Students believe that their employer has the right to monitor (93 out of 141) comments state that employees are paid to do a job and should be working while at work and not wasting employer resources.

Some students reflected on the extent of employer prerogative as indicated below:
"How far will I let a company go until I feel uncomfortable with their actions? If they regulate my email or if they regulate my phone calls I would be fine with it. However, once they start checking my financial background, and ask for private documents I would not feel comfortable." Most felt that employers not only have the right, but an obligation to determine if employees are productive. Out of 46 total comments from business ethics students, 34 comments were in this category. Ethics students also understood the liability of the employer to harassment law suits or other liability exposure if employees were unchecked. Some felt that the employer has an obligation to create a code of conduct regarding use of infrastructures that belong to the employer, and the obligation to educate and inform the employee of this conduct code.

Finally, the topic of disclosure was also addressed by survey respondents. Students felt that monitoring must be disclosed clearly to the employee, or it is an invasion of privacy by the employer. Five out of six comments on limitation of freedom mention the need to be informed so it is not "sneaky" on the part of the employer.

6 RESEARCH RESULTS: OBSERVATIONS AND IMPLICATIONS

The main observation is the difference in attitude regarding the right of employers to monitor but not the university. It is interesting to note that the percentage of students who felt that it was unethical to monitor Internet use in both the university setting and the workplace was only 32%. Clearly, students feel that monitoring is more appropriate at work than in an academic setting.
Questions resulting from analysis of the results that merit further investigation are why the reason of " academic use of internet by students" is cites so infrequently as a rationale for not monitoring students. Students use the internet frequently to do research, yet this category was mentioned only 22 times out of 173 responses.

Another interesting research finding were comments indicating that since radio, TV and books are not monitored – therefore, internet should not be as well. This faulty reasoning is cause for concern that students do not understand the extent of monitoring that actually does occur on these various media. Using an Ipod or cell phone our music is tracked, using cable, Netflix or a tevo, our TV habits are monitored, using Amazon to buy books, our purchases are tracked, and even the library has records of the books we read. How else could the advertising industry be successful with direct – to – consumer ad campaigns and personalized emails suggesting product for purchase. An interesting side note: the author worked at a company in the 90's Executone Information Systems that produced a product called the locator system. Employees were located and voice announced as to their location and who they were with by wearing a badge that was read by ceiling monitors. This product was also sold for tracking portable equipment needed in hospitals (portable X-ray machines) and to dissuade theft of computers and other valuable supplies. It was considered by some to be an invasion of privacy and by others to be a productivity enhancement.

7 CONCLUSION

In summary, sophisticated monitoring and blocking tools will continue to be used by organizations to solve productivity issues due to Internet misuse. Wen & Lin recommend the following minimal functional requirements for these tools: prevent web surfing that is not related to business needs and drain productivity, issue violation notices to the user who breaks acceptable internet use policy, monitor sites by time wasted, time of day and frequent users to analyze network performance. They also recommend the following components of Internet policy: determine acceptable amounts of time spent on-line, determine what should and should not be accessed, determine guidelines for downloading, determine what should be done if objectionable material is discovered, state acceptable chat room use, determine if there is an acceptable time of day to be on-line for personal use, and set rules for sending and receiving email. These should limit exposure and liability to the company caused by employees surfing the Internet. (Wen & Lin, 1998).

Introna advocates for policies associated with workplace monitoring. If an employee accepts a contract that he/she will abide by company policies, and a monitoring policy is in place, then that employee should have no expectation of privacy in the workplace. Using Rawls theory of justice, Introna advises policy development that ensures: the employer has a right to monitor and use the data for the overall good of the organization; the employee has a right to secure a regime of control that justifies all monitoring and assurances that data collected will be used fairly. (Introna, 2001).

The Internet should be a positive productivity tool not a liability. Employees and students need to feel valued and fairly treated in the exchange process between themselves and management. Strong cultures with explicit norms of behavior and ICT ethical codes of practice are conducive to curtailing cyberloafing and Internet misuse. Norms such as reciprocity, explicitly stated tolerable behaviors, and consequences, in a well-communicated policy that governs the use of the Internet can aid managers and university IT administrators in their relations with their employees and students.

REFERENCES

Alge, Bradley J., Ballinger, Gary A., Green, Stephen G. (2004) Remote control: Predictors of electronic monitoring intensity and secrecy. *Personnel Psychology*. Durham: Summer 2004. Vol 57, Issue 2. 377 – 411.

American Management Association (2005), AMA survey on electronic monitoring and surveillance www.amanet.org/research/pdfs/ems_short**2005**.pdf accessed 7/5/05.

American Management Association (2004), AMA survey on workplace email and instant messaging survey www.amanet.org/research/pdfs/ems_short**2004**.pdf accessed 7/5/05.

Anandarajan, M., Simmers, C., and Igbaria, M.(2000) An exploratory investigation of the antecedents and impact of internet usage: an individual perspective. *Behavior and Information Technology*, 19, 69 – 85.

Carsten Stahl, Bernd. Responsibility for information assurance and privacy: a problem of individual ethics? *Journal of Organizational and End User Computing.* Hershey: Jul-Sept 2004. Vol 16 issue 3, 59.

Chen, J. and Park, Y. The role of control and other factors in the electronic surveillance workplace. *Journal of Information Communication & Ethics in Society.* April 2005. Vol 3 No. 2. 79.

Conley, L. The privacy arms race. *Fast Company.* Boston: Jul2004, Issue 84. 27.

D'Antoni, Helen. (2004) E-Mail: Worker's constant companion. *Information Week*. Manhasset. Issue 979. 66 – 68, March.

Dudley, G. The cubicle walls have eyes. *Finance Week – South Africa*. Standton: Mar 14 – 18, 2005 59.

Flynn, Nancy. The ePolicy handbook. 2001 http://www.epolicyinstitute.com/d&d.html. accessed 7/5/05.

George, R.T. (2000) Business ethics and the challenge of the information age. *Business Ethics Quarterly*. Vol 10 No 1. 63.

Grodzinsky, F. and Gumbus, A. Internet and productivity: ethical perspectives on workplace behavior. 2005. unpublished paper.

Grow, Brian, Hacker hunters: an elite force that takes on the dark side of computing. *Business Week*. May 30, 2005. 74.

Hall, L. Where to draw the line. *Personnel Today*. Sutton: Jun1, 2004. 16

Hunter, L. (195) Public Image. In D.G. Johnson & H. Nissenbaum (Eds.) Computers, ethics, and social values. Upper Saddle River. Prentice Hall. 293.

Introna, Lucas.(2001) Workplace Surveillance, Privacy and Distributive Justice. *Readings in Cyberethics*, eds, Spinello and Tavani, Jones and Bartlett, 418-429..

Ladson, A. and Fraunholz, B. Facilitating online privacy on eCommerce websites: an Australian experience. *Journal of Information Communication& Ethics in Society*. April 2005. Vol 3 No 2. 59.

Langnau, L. From pirating to privacy. *Material Handling Management*. Cleveland: Oct 2004 Vol 59 issue 10. 58.

Levy,S. and Stone, B. Grand theft identity. *Newsweek*. July 4, 2005. Vol CXLVI. No 1. 38.

Lim, Vivien K.G.(2002) The IT way of loafing on the job: Cyberloafing, neutralizing and organizational justice. *Journal of Organizational Behavior*. Vol23,Issue 5, Aug..

Peterson, Dane K. Computer ethics: the influence of guidelines and universal moral beliefs. *Information Technology & People*.(2002) West Linn:. Vol 15, Issue 4. 346 – 362.

Petrovic-Lazarevic, S. and Sohal, A. Nature of e-business ethical dilemmas. *Information Management & Computer Security*. Bradford: 2004. Vol12 isue 2/3. 167.

Pomeroy, A. Business 'fast and loose" with email, IMs – study. *HR Magazine*. Alexandria: Nov 2004 Vol 49 Iss 11. p. 32

Roberts, M. Untangling web of wasted time. *Security Management*. Arlington: May 2005. Vol 49, issue 5. 26.

Robison, W.L. (2000) Privacy and appropriation of identity. In G. Collste (Ed) Ethics in the age of information technology. Linkoping: Center for Applied Ethics. 70.

Sandberg, J. Monitoring of workers is boss's right but why not include top brass? *Wall Street Journal* eastern ed. New York, NY. May 18, 2005. B-1.

Soat, J. Spamming the globe, surfing at work. *Information Week*. Manhasset: May 16, 2005. Iss 1039. 76.

Taillon, G. Controlling Internet use in the workplace. *The CPA Journal*, New York: Jul 2004. Vol 74 issue 7. 16.

Tam, P. White, E. Wingfield, N. and Maher, K. Snooping email by software is now a workplace norm. *The Wall Street Journal* eastern ed New York, NY Mar 9, 2005. B-1.

Taylor, J.S. (2000), Big business as big brother: is employee privacy necessary for a human-centered management organization? *Business and Professional Ethics Journal*. Vol 19 No 3. 13.

Thibodeau, Patrick. Employer snooping measure nears vote. Computerworld, 00104841, Sep 11, 2000, Vol 34, Issue 37.

Urbaczewski, Andrew and Jessup, Leonard M. (2002) Does electronic monitoring of employee internet usage work? *Communications of the ACM*, Vol 45 issue 1. 80 – 84, Jan.

Van Slambrouck, Paul.(2000) E-mail ethics: You've got pink slip. *Christian Science Monitor*, 08827729, Vol 92 Issue 193, August..

Verton, D. Email glitch exposes flaw in privacy law. *Computerworld*. Framingham: Jul 12, 2004. Vol38, issue 28. 1

Wakefirle, Robin. Computer monitoring and surveillance. *The CPA Journal*. New York: Jul 2004. Vol 74, issue 7. 52.

Wen, H. Joseph and Lin, Binshan.(1998) Internet and employee productivity. *Management Decision*. London: Vol 36, Issue 6.

Websites:

http://it.sacredheart.edu/webservices/policies/privacy/index.asp accessed 12/18/04.