INTERNET AND PRODUCTIVITY: ETHICAL PERSPECTIVES ON WORKPLACE BEHAVIOR

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

Andra Gumbus
Assistant Professor,
Management
Sacred Heart University
5151 Park Avenue
Fairfield, CT 06825
203 – 396 – 8271
gumbusa@sacredheart.edu

Keywords: Internet, World Wide Web, Workplace deviance, Productivity, Computer Ethics, Business Ethics

Abstract

The abuse of the Internet is real problem for organizations, with real productivity ramifications and it shows no sign of letting up. “The International Data Corp. estimated that 30% to 40% of employee Internet use isn't work related. And according to Nielsen/NetRatings, 92% of online stock trading occurs from the workplace during work hours and 46% of online holiday shopping takes place at work” [Schweitzer,2004].

Part One of this paper will examine the effect of the Internet on employee behavior in the workplace and its effect on productivity. The analysis will focus on issues of monitoring and privacy, employer/employee relationships and trust, behavioral expectations and managerial control. Part Two (section 3) will present and analyze the research of forty organizations including corporate, non-profit and academic institutions in order to gain a perspective across industries on company policy and practices regarding employee use of the Internet as it relates to productivity. Throughout the paper, we will examine the ethical issue of controlling employee behavior in the workplace.

Introduction

When Tim Berners Lee unleashed the World Wide Web (WWW) in 1990, his goals were to create “an internet-based hypermedia initiative for global information sharing” [Frauenfelder, 2004]. This accessibility to information at the click of a mouse coupled with the affordability of hardware and connectivity has re-oriented our lives. Within the past fifteen years, the Internet has made its way into our homes, schools, and workplaces changing the way we communicate, learn and conduct business. The WWW has lifted the restrictions on the Internet from a tool that could be used solely by academics and researchers, to one that can now be used by society to access popular culture. Looking back to the future, who would have dreamed that our lives would be so online in 2005?

Rapid access to data and information is essential for competitive businesses in the Information Age. Advances in information and communication technologies (ICT) have provided the tools that make this possible. Over the past decade organizations that were heavily dependent on manual processes and paper, have invested in ICT. Central servers with dumb terminals controlled by management information systems (MIS) departments have given way to distributed client server models with unlimited Internet access. While this access has made life more enjoyable for the employees, organisations are finding that time spent on personal business is eroding time spent on company business. Consequently, companies have started to rethink how much Internet access to allow employees in the workplace. Broadband access to the Internet in the workplace increased the number of web pages viewed by individuals by 55% and increased the amount of time spent online by 23%. Of the time spent online 31% is non-work related [webspy, 2004].

To counter this trend, companies today are limiting access to non-work related sites. Thin clients (computers with limited applications and no Internet access) are replacing thick clients that afforded unlimited access. Under the guise of virus control, spam control, employee safety, protection of bandwidth, companies are implementing intranets that can be controlled by management Gains in productivity are targeted, e.g., reducing the demands on the help desk, control/limiting downloads and upgrades onto company property, and centralizing access to company-wide data.

What are the ethical ramifications of controlling employee behavior in the workplace? Is the company acting ethically when spy ware or other software that monitors all employees based on the inappropriate behavior of a few is installed? Is monitoring for control eroding the employee / employer relationship and undermining trust? Does a company have the right to deny the reading of private email during lunchtime or after work hours? Are companies realizing the anticipated results gained from the switch from thick to thin client terminals? This paper will explore these questions using survey results from forty companies across industries. Part One will examine the effect of Internet on employee behavior in the workplace and its effect on productivity. The analysis will focus on issues of monitoring and privacy, employer/employee relationships and trust, behavioral expectations and managerial control. Part Two will present and analyze the research of forty organizations including corporate, non-profit and academic institutions in order to gain a perspective across industries on company policy and practices regarding employee use of the Internet as it relates to productivity.

1. Internet and Employee Behavior

The pervasiveness of the Internet and email over the last decade has led researchers to study the Internet, email addiction and other problematic behaviors associated with its constant use in the workplace. There is a continuum of employee Internet abuse ranging from employees who exhibit high comfort and use to those that are adverse to computers and do very little personal business online. The following statistics demonstrate the rampant abuse of Internet privileges:

- 80% of companies reported that employees had abused Internet privileges, for example by downloading pornography or pirated software [Fox, 2002].
- 70% of all Web traffic to Internet pornography sites occurs between 9 a.m. and 5 p.m., according to SexTracker, a porn industry consultancy.
- 92% of online stock trading occurs from the workplace during work hours and 46% of online holiday shopping takes place at work according to Nielson/NetRatings.
- 25% of employees felt they were addicted to Internet usage [Fox, 2002].
- Online gambling was rated as the fifth most addictive activity (by eight percent of respondents) behind shopping (24 percent), news (23 percent), pornography (18 percent), and ahead of auctions (six percent) [Fox, 2002].

In addition, Information Week estimates that large companies with revenues of over $1 billion receive 2.4 million email messages and send 1.6 million daily. Small companies of less than $100 million receive 82,000 messages and send 100,000 daily. Workers surveyed by Osterman Research reported checking email continuously at work (68 %) a few times an hour (17 %) and several times a day (13 %). Weekend and vacation are not exempt from the habit of email (only 2 out of 5 don't check until they return to work) [D'Antoni, 2004].

The explosion of the Internet and its use in organizations has affected productivity positively and negatively. On one hand, companies have harnessed the Internet to perform tasks such as analysis and research and have shortened cycle times, marketed products and reduced costs associated with doing business [Anandarajan, Simmers, and Igbaria, 2000]. On the other, the Internet has also affected productivity negatively by allowing employees to shop, email friends, plan vacations and otherwise eat up company time and resources for personal gain. Vivien Lim [2002] defines this behavior as "cyberloafing". "Cyberloafing" is a voluntary act of employees using company Internet during office hours to surf non-job related web sites for personal purposes and to check personal email. Lim equates "cyberloafing" to a form of production deviance, under the broader rubric of workplace deviance. Robinson and Bennett define workplace deviance as acts that violate organizational norms and adversely affect the organization and its members [Robinson and Bennett, 1995]. Lim credits the Internet with the creation of an easy and convenient new form of production deviance allowing employees to remain invisible, and loaf while still being present at work looking busy and efficient. She refers to cyberloafing as the " IT way of idling on the job." Lim suggests cyberloafers pose an even greater threat than regular loafers. While both groups cost the company money based on lost productivity, the cyberloafers might unintentionally put the company at risk if their virtual explorations incur computer viruses or open the company up to legal liabilities [Lim, 2002]. So while cyberloafing may be undertaken as a personal response, as we will demonstrate below, its repercussions may affect productivity on more than just a personal level.

Why do employees cyberloaf? Lim studied employees in the context of exchange relationships where employees and employers exchange time and effort for compensation, and in terms of organizational justice that refers to how fair an organization is to its employees. She indicates that simple exchange relationships have become more complex when social goods such as information, respect and status may be exchanged. Has the Internet added to this complexity? The results of Lim's study show that unhappy employees who feel they have been unjustly treated by management might feel entitled to cyberloafing as perceived additional compensation. Lim refers to this technique as neutralization. Neutralization is a response to an imbalance in employer/employee relations by which employees rationalize why their deviant behavior is justifiable [Lim, 2002]. The metaphor of the ledger is used to describe this rationalization: deviant behavior is balanced out against past good acts. The goal is to alleviate guilt that may be associated with the deviant act. The employee's consequentialist analysis that cyberloafing really does "reinstate a sense of justice into the relationship" [Lim, 2002] from the employee perspective raises questions as to how it is viewed by management. We suggest that cyberloafing could lead to mistrust on the part of management that might result in workplace monitoring.

2. Monitoring

The American Management Association [2001] reported that 78% of all firms monitor employees electronically, 62% track Internet use, and 54% track email. Technology enables employers to monitor workplace activity and be more aware of violations." [Van Slambrouck, 2000]. Research on electronic monitoring primarily focuses on employee reactions and less on the managerial decisions that result in monitoring. However, in their study, Alge, Ballinger and Green, found that managers increase monitoring activity when they have a high level of dependence on subordinates and also when employees have performance problems. They report that problems with past and future performance trigger monitoring of employees. In addition, 95% of managers interviewed identified lack of productivity, abuse of the system and failing trust as cause to monitor. Past performance is a predictor of future performance; therefore, a slip in performance can create the need for additional information. This could be an unanticipated result of Lim's neutralization. Their study also found that the more important the employee is to a critical task or project the greater the likelihood of monitoring [Alge, Ballinger & Green, 2004].

2.1 Managerial implications

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? Will tracking employee activities in virtual space compromise the workplace relationship? In order to answer this question, Urbaczewski and Jessup [2002] 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, which was viewed as infringing on privacy and trust, and greater satisfaction with EM for feedback that was generally positive and constructive in nature. Monitoring and blocking may also be counterproductive to productivity by causing anger among monitored employees. 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. Managers expressed ethical concerns about secretly monitoring employees. Alge, et al. 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].

To address these concerns, Alge, et al. recommended 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].

Lucas Introna [2001] also 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. Unfortunately "the issue of workplace privacy is not merely a matter of 'bad' employees wanting to hide their unscrupulous behavior behind a call for privacy… it is rather a legitimate concern for justice in a context in which the employees, for the most part, are in a relationship of severe power asymmetry" [Introna, 2001]. Using Rawls theory of justice, Introna advocates for 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.

The Internet should be a positive productivity tool not a liability. Keeping employees focused on work related tasks and enhancing productivity are managerial responsibilities. Employees need to feel valued for their work and fairly treated in the exchange process between manager and employee. Strong cultures with explicit norms of behavior and ICT ethical codes of practice are conducive to curtailing cyberloafing. 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 in their relations with their employees.

3. Research Results

Forty organizations were surveyed in order to determine company policy and practices regarding employee use of the Internet. In order to gain a perspective across industries, organizations included corporate, non-profit and academic institutions. Twenty-eight companies had similar themes in their responses to the following research questions:

1. What practices and/or policies has the company implemented to limit or control unlimited Internet use among employees?

2. What policies are ethically problematic to enforce? What policies reflect gray areas?

3. What specific Internet sites has the company blocked for employee access? Example: www.ebay.com

4. Why were policies implemented to limit employee access to unlimited Internet resources?

5. How is the company monitoring employee usage and/or time online? Example: spam filters, firewalls, and Internet access controls.

6. What cost and/or productivity savings are incurred? How are savings measured?

7. What productivity results have been achieved due to limiting Internet access for employees?

Twenty-two companies used Websense to monitor employee usage of the Internet, and categorically block sites that promote pornography, shopping, gambling, music downloads, politics, and hate. Many also prevented access to Yahoo, hotmail and other email providers to discourage online chat. Many have policies that leave enforcement to the discretion of the manager and will monitor employees only when and if abuse is suspected. An additional twelve organizations were either too small or had not yet considered the negative effects on productivity of unrestricted employee access to the Internet.

3.1 Small Organizations

In small organizations (classified as under 50 employees), policies regarding Internet access ranged from no policy in place (i.e., unlimited access), to those that totally restricted Internet access. Twelve of the companies had not yet implemented policies regarding Internet usage and provided unlimited access. They stressed the idea of community and trust. "In order for a community to exist there must be some degree of shared beliefs, values and goals among members who share a common vision and who desire to perpetuate it through the socialization of new members" [Grodzinsky and Tavani, 2004]. However, two of those surveyed responded that investigations were under way and felt that the investment to restrict access would be worth the productivity gains. At a law firm the culture was described as a "sort of honor system where employees are free to do what they want as long as the work is done on time. Monitoring is done by eye if need be; it is an unspoken rule that employees don't use the Internet unnecessarily." The CEO at another small firm recently discussed Internet abuse with employees and said the idea of controls was not necessary at this time. "It is looked upon here as a trust issue. We are a close-knit group of people that don't really work normal office hours. That leads to many of us being here later or earlier than we should sometimes. If we have to go on the Internet to get something done, we trust we will use our heads and do it during some down time, on our lunch hour, or after hours."

Finally, one small company adopted a strategy of allotting company computers to designated jobs. No computers with Internet access are available for general staff. Only managers and those who need full Internet access have it. No policies have been implemented because " by not having the temptation the company is avoiding the issue all together."

3.2 Large Organizations

Of the 28 large firms surveyed, Internet access is restricted. Over two thirds mentioned the legal protection provided by blocking offensive or inflammatory sites and email providers. Over 95% of large firms block sites that include music downloading, pornography, gambling, adult themes, shopping, games, military and extremist, violence, racism and hate sites. Email is blocked by over two thirds of large companies to prevent private mail or junk mail from taking server and bandwidth space. Websense software is used by over 80% of large firms that track usage through an outside vendor. In these firms, policies exist but over half have not had to implement the policy unless management noticed a suspected abuse. One manager noted, "We have policies in place but have not had to implement them because the company works on a trust factor and has not run into any issues with employees abusing policy. Internet use is also controlled by open work spaces and locating computer screens so the monitors can be seen from the door." Larger firms cite productivity gains of between 15 – 20% due to restrictions of Internet access.

In other firms, however, Internet access is a necessity for work. “ Internet access helps conduct research that results in increased productivity. The IT person would have to unblock computers when employees need to do research and this would take more time than it is worth. Employees stay productive even with unlimited access to the Internet.” A computer technology business that sells a variety of product needs the Internet to conduct research. “ The only way to know your product is to research it. Therefore going online and retrieving free samples and doing research before recommending it to a customer is necessary. We need to see it for ourselves using the Internet.” A good faith policy is in place in a large firm to intentionally discourage abuse. “The nature of the work at this company is such that our clients include Playboy, eBay, and HBO making it necessary for our employees who are working with the client at any given time to access their Internet sites. Therefore, blocking Playboy even though it might be considered an inappropriate work site would not be smart business practice in our company. Regular checks are run in this company to ensure employees are not visiting offensive sites unnecessarily. Our policy was also implemented to negate legal implications of subjecting employees to offensive material. For instance, if an administrative assistant walks in on her boss who might be viewing pornographic material, it might give her reason to file a legal complaint.”

3.3 Internet Usage Policies and Productivity: Emergent trends

In terms of Internet usage policies, organizations divided into three areas: those with no policies (see section 3.1), those that were proactive in establishing policy and those that were reactive. Excerpts from our case studies illustrate these trends.

3.3.1 Pro-Active Policy Development

In a university setting as opposed to corporate environment the restrictions are less intrusive to student and faculty, giving them the freedom to engage in research and use the Internet without constraints. However, the issue of file sharing is broad based in the academic world. Students often use software to download music that uses bandwidth at the expense of legitimate university business. At one university, the web was virtually inaccessible for a few days two years ago because file-sharing applications were hoarding bandwidth. This seriously impacted the productivity of the entire university. By installing the PacketShaper device, the university can reserve bandwidth by limiting traffic by port type. The university network engineer is able to ensure that all types of traffic can function at a good level of operation at all times. The issue of organization justice is addressed in the following manner: The software shuts down at 10:00PM each night to allow unrestricted downloading from the university Internet. An interesting side note is that peak Internet usage hours on campus are between 8:00PM and 4:00 AM.

A large tobacco company was proactive. Policies were implemented to limit abuse and address productivity concerns. The philosophy adopted was that strong controls from the start are easier than loose controls that may have to be strengthened. To that end, their written policy entitled Information Technology General Usage Policy includes sections on Internet usage and Electronic Mail. A training class is mandatory for employees before an Internet logon is established. This one-hour class explains Internet limitations and why the firm has implemented these policies. Their monitoring implementation uses a third party vendor. While it is easy to monitor volume by sender, content monitoring is more problematic. Of concern to the company is the content of email as this poses the biggest risk to the company if proprietary information is sent unencrypted. Internet browse time for the second quarter of

2004 illustrated a steady trend from March until June with a severe drop in June after an abuse was discovered and investigated. The abusers were released from employment and a reminder memo issued by senior management regarding Internet usage. The memo caused a sharp drop in usage. This trend of outsourcing monitoring to a third party that tracks productivity and reports to the company emerged in several company responses.

An international publishing company also took a pro-active approach. It has an official Electronic Communications Policy that is in the employee handbook. It clearly states that the electronic communications systems (Internet, telephone, fax, and copy machine) are solely for business purposes. The senior network administrator revealed that the company is lenient when interpreting this policy. They leave it up to the individual manager to monitor employee usage. Managers are coached to look for productivity changes with a reduced performance level, a possible indicator of excessive usage. One instance led senior management to issue an email warning employees that the Motion Picture Association had notified them that employees were downloading files from illegal websites. The email reemphasized the policy and warned that tracking systems were being installed to monitor illegal usage.

The city of Stamford, CT instituted a policy in May 1999 regarding proper usage of the computer by city employees. The policy states that the computer is to be used for city business only; however, incidental or minimal use is tolerated due to the difficulty of enforcement. The city does monitor if and when individual performance is not met. The policy states that “ each user is responsible for using the city’s technology systems, resources, and services in an efficient, effective, ethical and lawful manner and in accordance with applicable statutes… violations of this policy will not be tolerated and may result in disciplinary action up to and including termination.” Although no blocks are in place, the City of Stamford policy articulates a clear mandate about productivity, privacy and Internet usage.

At a large personal care product division of an international conglomerate the company policy states that minimal personal Internet use is acceptable. Inappropriate sites are restricted including joke sites, day trading, Victoria Secret and pornography. A policy of restricting web sites can be problematic for employees who need to access sites that contain company products. In one instance employees could be researching a product on the Target site in order to gain information on how Target markets their brand; in another, they could be ordering merchandise and doing personal shopping. It is important not to target employees who are doing legitimate research. Those who monitor the system look for red flags such as a keyword that is deemed unprofessional. The system will report the search and the employee will be monitored for additional offenses. After supporting documentation is prepared the employee will be issued a warning. If the problem is not corrected, termination proceedings will be started. The company currently uses Lotus Notes but anticipates a system update in order to support Outlook 2003 that has many more spam filters, firewalls and pop- up ad blockers.

3.3.2 Reactive Policy Development

At a large copier and mail service firm policies were implemented because employees were spending too much time on the Internet and not being productive. The IT department was also concerned about the ability of junk mail and viruses to come through while employees were on various sites. The company uses spam filters, firewalls and customized software to monitor employee’s usage and time online. They have instituted the automatic downloading

of spy ware software into employee’s personal computers when certain Internet sites are visited. This enables the company to monitor keystrokes and inappropriate time spent online. They use an outside vendor to track productivity and report to the company.
At a large commercial finance division of an international company the policy regarding use of e-sources was implemented in order to eliminate or reduce the improper use of company e-sources which include computers, computer software, email internet access wireless devices, intranet, telephones, voicemail, fax machines and photocopiers. The company experienced substantial increases in the downloading of unauthorized software that resulted in computer malfunctions, server problems and productivity lapses. Downloading software is a violation of company policy and in response, the IT department has blocked many websites from employee access. The company monitors Internet access by the use of firewalls and programs downloaded onto the employee’s hard drive. At the discretion of the company, management can review, audit, and access files or information from any of the e-sources at anytime. Employees are permitted a reasonable non-business use of e-sources as long as the communication is not abusive, sexually explicit or offensive or time intensive. If misconduct is recognized, disciplinary action can be taken.

The Director of Information Technology at a small privately held health care provider responded that policies were implemented to restrict employee usage of the Internet after personal studies of individual usage on company time were conducted at the practice. He stated another benefit of the restrictive policy is the ability to limit the liability of illegal activities that may be conducted by employees. Since the company started monitoring usage by running reports, Internet usage has gone down considerably. Employees are aware that unacceptable Internet usage is grounds for termination. The executive team recently ran reports for every employee in the business office and is determining what productivity losses and costs have been incurred for time wasted on the Internet. The data will be shared with each department manager to be made a part of the employee performance evaluation process.

3.3.3 Observations

In terms of productivity, similar themes in both small and large companies surveyed emerged in three areas: trust, time limits on Internet use, and managerial level responsibility for monitoring and/or implementing policy. The issue of trust between management and employees surfaced in surveys from both small firms that do not monitor (see section 3.1) and large firms that monitor and block Internet usage. It was encouraging to discover that many companies proactively set policy and inform their employees of expectations, then trust employees to abide by these policies. When trust was violated, surveillance was in place to verify the abuse. This substantiated our view that in most cases monitoring was used for the good of the organization.

Both large and small firms put time limits on private use of the Internet. Some have an unstated policy that implies access before work, during lunch and after work hours. Others limit employees to one hour per business day. Some provide levels of access. A mid-sized electronics manufacturer provides three levels of computer access. The default level is 300 minutes per month for all employees. If the job description requires use of the Internet employees are allowed 1000 minutes. The third level is unlimited access requiring the immediate supervisor’s written permission.

All companies surveyed rely on management to interpret policy or enforce discipline if abuse is suspected. A large global company with offices throughout the world replied that at any given time a manager can view the top 10 sites employees are accessing enabling management to react and further investigate if suspicious looking sites are listed and/or if excessive time seems to be spent online. A large technology company retains records of employee online activity for 6 months. “ Internet usage is treated the same as phone usage; if it is not abused then no action is taken. Other large firms do not monitor productivity loss but rely on local management to discipline. One firm stated that its philosophy is to let the managers and supervisors police their own departments and people. Comparative Internet usage figures are often more meaningful to managers because they are monitoring locally rather than unilaterally. The downside to this distributed approach is that with no clear company directive, discipline may vary from department to department. Based on the response from both large and small companies surveyed, the important role of management cannot be overstated in the study of Internet and productivity.

Because more and more companies are using monitoring tools, Wen & Lin [1998] recommend the following minimal functional requirements for these tools: prevent web surfing that is not related to business needs and drains 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.

Conclusion

We believe that because: the organization owns its network, the Internet has become part of daily life for employees, sophisticated monitoring and blocking tools will continue to be used by managers to solve productivity issues due to Internet misuse, companies should develop usage policies that embody fairness for all concerned. Employees, when hired, should be made aware of what the company expects of them concerning Internet usage. Win and Lin [1998] also recommend the following components of Internet policy in order to support fairness: 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] and should inform employees as to what is expected of them. If they do not support the organizational policy, employees could choose to work elsewhere.

References

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

American Management Association (2001), AMA survey on workplace surveillance and monitoring www.amanet.org/research/pdfs/ems_short2001.pdf accessed 12/18/04.

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.

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

Fox, M., Phillips, L. Vaidyanathan, G. (2003) Managing Internet Gambling in the Workplace, First Monday, volume 8, number 4 ,
URL: http://firstmonday.org/issues/issue8_4/fox/index.html. Accessed 12/18/04.

Frauenfelder, Mark, (2004) Sir Tim Berners-Lee: He Created the Web, Now He's Working on Internet 2.0. MIT's Magazine of Innovation Technology Review. Vol 107. No 8. 40 – 45.
Grodzinsky ,F, Tavani,H. (2005) The Internet and Community Building at the Local and Global Levels: Some Implications and Challenges, ICIE 2004, Karlsruhe, Germany forthcoming in Johannes Frühbauer, Rafael Capurro, Thomas Hausmanninger (Eds.): Localizing the Internet. Ethical Issues in Intercultural Perspective. Munich: Fink Verlag.
Introna, Lucas.(2001) Workplace Surveillance, Privacy and Distributive Justice. Readings in Cyberethics, eds, Spinello and Tavani, Jones and Bartlett, 418-429..

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..

Nielsen//Netratings, 2002. "Online Usage at Work Jumps 17 percent year-over-year, driven by female office workers," at http://www.nua.org, accessed 15 February 2003.

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.

Robinson, S.L. and Bennett, R.J. (1995)A typology of deviant workplace behaviors: a multidimensional scaling. Academy of Management Journal, 38, 555-572.

Schweitzer.D. "Workplace Web Use: Give Em an Inch", 27 Sep 2004 | SearchSecurity.com
http://searchsap.techtarget.com/originalContent/0,289142,sid21_gci1009417,00.html, accessed 12/18/04.

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..

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.

http:// www.ci.stamford.ct.us accessed 12/18/04.

http://www.webspy.com/files/articles/WebSpy%20Ltd%20-%20Internet%20Use%20Statistics.pdf accessed 12/18/04.

http://searchsap.techtarget.com/originalContent/0,289142,sid21_gci1009417,00.html accessed 12/18/04.