Online Journal of Applied Knowledge Management
A Publication of the International Institute for Applied Knowledge Management

Volume 1, Issue2, 2013

Legal and ethical issues of employee monitoring

Johnathan Yerby, Middle Georgia State College, Johnathan.Yerby@maconstate.edu

Abstract

Many questions about employee workplace monitoring produce complex answers. For example, what is employee monitoring, who is doing it, and why are employers doing it? This paper will explain what employee monitoring is, how organizations can learn what types of activities users need, and why there is a need for the monitoring. This paper will also discuss one or two types of employee monitoring. This paper addresses the legal and ethical issues involved when observing someone in a work environment. The paper will give employers strategies and practices for monitoring employees for improved organizational performance.

Keywords: Employee monitoring, legal, ethical, management.

Issues of Employee Monitoring: What is Appropriate?

Should companies monitor employees while at work? What actions should the companies monitor? What types of monitoring are acceptable? A report by the U.S. Office of Technology Assessment, defines computerized performance monitoring as, "the computerized collection, storage, analysis, and reporting of information about employees' productive activities" (Peters, 1999). The practice of monitoring a company's workers is a controversial practice that is undeniably on the rise (AMA, 2008). When it comes to the subject of employee monitoring there is a grey area; current laws mandate that monitoring is legal, yet the questions of effectiveness and ethics arise. Organizations must monitor employees to protect both the company as well as the employee, but organizations must also give diligent attention to the ethical treatment of employees (Bezek, Britton, 2001). Bhatt (2001) describes employee monitoring and knowledge management by pointing out that many organizations "believe that by focusing exclusively on people, technologies, or techniques, they can manage knowledge." Such a strategy will not allow a firm to maintain a competitive advantage. Organizations must create an environment of accountability and transparency to operate effectively (Bhatt, 2001).

At the beginning of the 21st Century, the world and more specifically the United States has gone from an Industrial Age to an Information Age (Hart, 2000). At the dawn of the Internet Age, employers face serious risks from employee abuse of this relatively new communication medium. To limit these risks, Frayer (2002) suggests that employers are using innovative monitoring technology, which enables them "secretly to view, record, and report literally everything employees do on their computers." Nowadays, increasing numbers of employees use computers to perform work tasks. Of the 50% to 75% of workers having access to a computer, approximately 85% have internet access (AMA, 2008). With computers being so regularly available to such a wide spectrum of people with a diverse sense of work ethics, knowledge, and varying intentions, employers feel forced to monitor the activities of their employees.

E-mail and the Internet are integral parts of the typical worker's daily routine. Because of its speed and overall convenience, e-mail has replaced the inter-office memorandum as the preferred method of communication in corporate America. Therefore, many employees are using e-mail and the Internet for just business. However, the problems arise when employees use business resources for non-business related tasks. Therefore, businesses are responding to legal risks by proactively combating problems of employee non-work Internet use. The proactive step that businesses are taking is to monitor the activities of their employees, more specifically monitoring employees' electronic activities (Bezek, Britton, 2001). As reported by Court (2004), numerous employers across the nation utilize some form of employee monitoring. Court cites statistics of Internet and e-mail misuse by workers, and potential liability traps, as the main reasons for employee monitoring. The employee monitoring in many cases is there to protect the business from legal liability, as well as to produce a more efficient employee.

An article, discussing citizen's privacy, reports that over three-quarters of major U.S. corporations collect information on employees by various means: videotaping, monitoring Internet and e-mail use, or hiring outside investigators (Marshall, 2001). As of January 2008 only two states, Delaware and Connecticut, require employers to notify employees of monitoring, the remainder of the nation does not have specific laws requiring employee notification. According to the 2007 American Management Association survey (AMA, 2008) 83% inform workers that the company is monitoring content, keystrokes and time spent at the keyboard; 84% let employees know the company reviews computer activity; and 71% alert employees to e-mail monitoring.

As described by McEvoy (2002), one problem with workplace monitoring is that despite employers informing employees about monitoring, many employees still let their guards down and commit acts subject to disciplinary action. Companies provide more employees with Internet access and e-mail at work, which gives them a new way to cause potential problems for their employers. To address the problem on employee computer misuse, many businesses implement systems to monitor the actions of their employees. The 2007 Electronic Monitoring & Surveillance Survey (AMA, 2008) cited some reasons for firing employees including violation of company policy (64%); inappropriate or language (62%); excessive personal use (26%); breach of confidentiality rules.

The Technology: How Are Employees Monitored

There are hundreds of software and hardware solutions available on the market to monitor a vast array of activities. The price of monitoring or surveillance software ranges from several thousand dollars down to free. Most solutions can log keystrokes typed, application and website usage, detailed file usage, incoming and outgoing chats and e-mails, internet connections, windows interacted with, internet packet data, desktop screenshots, software installations, and much more. The software can present all activities logged in easy-to-read graphical reports. Employers can set specific alerts to notify management when an employee performs a certain action or is perhaps not meeting productivity goals. Keystroke monitoring is perhaps one of the most invasive types of monitoring. There are programs that generate reports detailing every key pressed on a keyboard. The companies that make the appliances to monitor employees cite uses for their products to stop leaking sensitive information, stop breaking laws, stop violating company policies, limit legal liability, and to monitor and recover lost crucial communications to

name a few. Companies can implement easily and stealthily the advance monitoring systems allowing the employer to monitor workers without their knowledge. The corporation may install hardware devices at the firewall that will track all electronic transactions or can remotely install software made invisible to the computer user. The technology to monitor an employee's activities is extremely sophisticated and fully capable of exposing any action taken on a business computer. The practice of employee monitoring is in practice by large and small businesses throughout the world.

It is also very important to note that employers are monitoring more than just computer usage, many also employ telephone and video monitoring. According to California state law on California Public Utilities Commission, organizations monitoring phone calls are required to inform participants of the recording or monitoring of the conversation by either putting a beep tone on the line or playing a recorded message (1983, General Order 107-B). Many companies also observe employees using video surveillance equipment. Over the last couple of decades, devices that they are completely oblivious to are recording an increasing number of events in every citizen's daily lives. There is an all-out assault of tools including hardware, software, telephone systems, and video recordings that organizations are using to protect themselves and work to increase productivity.

The Dilemma: Employee Monitoring

Employers can create complex problems when they monitor employees. Should employers be able to monitor their employers? If so, what should they be restricted to monitoring, and do the employees have the right to know that employers are monitoring them. Each of these questions creates a multifaceted response from both the employer's side, as well as the viewpoint of the employee. As Frayer (2002) notes, increased employee use of the Internet created opportunities for several companies to produce sophisticated monitoring software, which enables employers to peer into literally everything employees do online. According to Frayer, organization created employee monitoring because there was a substantial need for organizations to monitor their workforce.

If a business owner does nothing to stop these counter-productive activities, then it is not likely the owner could stay in business. Workplace monitoring can be beneficial for an organization to obtain productivity and efficiency from its employees (Bezek, Britton, 2001). The enormity of potential productivity loses, as reported by Court (2004), is approximately one million dollars annually for a company with 500 employees surfing the Internet for just a half hour a day. Using these facts, if an employee spends two hours per day on the Internet, and the organization has 500 unmonitored employees, the potential annual loss could be nearly $4 million.

While computers are often essential work tools, giving employees open, unmonitored, computer access causes productivity and efficiency to suffer. There has to be a balance between protecting the company's information assets without going overboard to the point where employees feel alienated. Education and communication are the best tools to attain this balance. Educate workers to let them know what monitoring is, what it will monitor, and convey the message that this monitoring is not due to lack of trust, but is being used to protect the company. The main disconnect between the organization and the employees interpretation is poor communication or training (Duffy, 2003). Lawyers generally advise that one way for businesses to avoid liability

for monitoring employees' online activities is to take all necessary steps to eliminate any reasonable expectation of privacy that employees may have concerning their use of company e-mail and other communications systems (Duermyer 2007).

People, the employees, by nature generally tend to desire more freedom and less monitoring. Many people and organizations are against monitoring the activities of people in the work place. Opponents include civil liberty groups, privacy advocates, and many employees themselves. Among the major criticisms of electronic employee monitoring, as noted by Watson (2001), are increased levels of stress, decreased job satisfaction, decreased work life quality, and lower levels of customer service. Monitoring can create a hostile workplace, possibly eliminating the whole point of monitoring in the first place (i.e., to increase efficiency).

Watson (2001) continues to say labor unions and other advocacy groups have complained exceedingly about electronic monitoring – charging that it invades employees' privacy, causes work-related stress, and low morale, and employers can use it unfairly. It is possible that employees will feel like their employers are treating them unfairly - resulting in the employees taking less initiative, and perhaps do only the bare minimum just to keep their job. Therefore, from an employee stance, workplace monitoring could be detrimental to productivity and efficiency

Many articles from Management and law journals such as the American Management Association and Mealey's Cyber Tech Litigation Report support a perceived need for employers to monitor their employers. The need comes from more than just a desire to increase productivity, but there are also issues relating to protection from potential legal liability.

Court (2004) discusses a two-year marketing research study indicating that "sex" was the most popular search term on the Internet. That study also revealed that "Porn" was the fourth most-searched term, with "nude," "XXX," "Playboy," and "erotic stories" all being among the top-twenty Web search terms. More disturbing is the fact according to the cited study, that 70% of this traffic occurs Monday through Friday, 8am until 5pm. Court further writes that more than 60% of companies report having disciplined employees for inappropriate use of the Internet, with more than 30% of companies having terminated employees for Internet misuse. Court cites specific examples of employees at major corporations using work computers for sex-related purposes:

(1) Dow Chemical Company firing fifty workers and suspending 200 more for sending and storing pornographic and/or violent e-mail messages;

(2) The New York Times terminating over twenty employees for sending inappropriate and offensive e-mail messages.

(3) Employees of IBM, Apple Computer, and AT&T were among the most frequent visitors to Penthouse Magazine's website, spending the equivalent of over 347 eight-hour days in a single month.

These cases are but a few of the numerous incidents that give reason for companies to monitor employee computer use. Any of the companies discussed above could have been subject to lawsuits for, among other grounds, hostile environment sexual harassment.

Security is yet another reason that gives rise to an organization's need for employee monitoring. Woodbury (2003) explains that opening unsolicited e-mail at work creates danger because attached files could contain a virus, wreaking havoc on a workstation hard drive and then spreading through a business' entire computer network. With more monitoring, a business could perhaps prevent, or at least detect sooner, a computer network vulnerability created unknowingly by employee e-mail. Managing the knowledge of an organization could also help catch employees who may be giving away a business' trade secrets, designs, or formulas, to a competitor (Oprea, 2012). Whether it comes to an issue relating to productivity, sexual harassment, hostile workplace, or protecting the security of the company and its computer network, there is a need for businesses to screen the activities of their employees.

The Question: Should Employees Have a Right to Privacy?

Whether an employee should have the right to privacy in the workplace is an issue mentioned briefly above. There are many arguments in favor of employee privacy, but there are also strong reasons why an organization simply cannot grant this right to its workers. Groups such as the American Civil Liberties Union, Workplace Fairness, and National Work Rights Institute argue that that secret monitoring infringes on protected workplace rights. Under that logic, it would seem that employee monitoring should not exist at all. Yet, Frayer (2002) responds by saying it would be "absurd" never to permit employer monitoring of an employee's online activities. For example, Frayer notes that monitoring employee computer use would be an effective way to confirm or alleviate an employer's suspicion of an employee who might be using the Internet to reveal trade secrets.

Employee e-mail use creates other workplace privacy problems. As discussed by McEvoy (2002), even though e-mail is ubiquitous, and makes employees more efficient, it hangs around on workstation and network server hard drives – leaving behind evidence of all employee communications. McEvoy further states that employers should advise employees to think seriously before clicking the send button with work e-mail. One nasty joke about a supervisor, or a lewd joke or image, can create problems in the workplace. Even if an employee thinks, he or she deleted an e-mail message someone may retrieve it later since organizations save almost all e-mail on a network server. According to a 2008 article by Tangent Inc, an organization performs approximately 90% of the day's business communications via e-mail or by way of unsecured instant messages (Alexi, 2008). Communications, including unstructured data, can clog up an organizations network bandwidth and take up great amounts of storage space. The volume of e-mails and similar data forms in most businesses double every 12 to 18 months. Federal Rules of Civil Procedures passed in December of 2006, state that organizations cannot delete or overwrite any e-mails, communications, files, directives, or requests that may be relevant to current or future litigation. The company must be able to produce necessary data and to produce it because that is the law (Alexi, 2008). In addition to the Federal Rules of Civil Procedures, there are other governing policies such as Sarbanes Oxley, HIPPA, Gramm-Leach-Bliley, and about a dozen others that require organizations to preserve and protect data in very specific ways.

As an example of how employees have few electronic privacy rights at work, Collins (2002) discusses the case of an insurance company senior executive given two company computers - one for the office, and one for home use. The executive signed a computer use agreement stating

that he would not go to any pornographic website, or misuse the company computers in any way. The insurance company later fired the executive for violating the company's computer use policy, after the executive admitted to repeatedly accessing pornographic websites during work. Collins further explains that the executive claimed he did not intentionally visit the porn sites, but that the sites simply "popped up" on his work computer's display. Therefore, the executive sued his former insurance company employer, alleging that the company had wrongfully terminated him.

During the litigation, lawyers for the employer wanted to get access to the company computer the executive used at home to show that he frequently visited pornographic websites. Collins explains that the trial court denied the employer's motion to search the executive's home computer, but a court of appeals disagreed. The court of appeals held that evidence of the executive's Internet-use history, stored on his home computer's hard drive (including the length of time spent at particular Web sites) could be used to impeach the executive's claim that porn sites just "popped up" on his work computer's display.

Therefore, in that case, the employee ultimately did not have a right to privacy for information on an employer-supplied computer, even when used at home – a place most would believe to be private. Employees do enjoy a true right to privacy in their everyday lives outside of work, and workers may desire that right to extend to the workplace, too. Nevertheless, the reality is that when an employee is at work, the right to privacy is either nonexistent, or significantly less than the one enjoyed after-hours.

Legality of Employee Monitoring

As mentioned earlier, new technologies often create the need for new rules. Marshall (2001) uses the example of the U.S. postal system to show how laws change to address new technologies. In 1825, Congress enacted mail anti-tampering laws in response to increased reliance on the mail system, brought about because of growing literary in the young nation. However, it was not until 1877 did the Supreme Court extend Fourth Amendment Constitutional protection to mail, requiring government officials to get a court order to open mail.

Marshall's postal system example shows how laws often lag behind technological development. Moreover, e-mail is like a new version of postal mail. While laws currently protect someone from opening or tampering with postal mail, the same type of laws do not currently (and may never) protect e-mail.

Frayer (2002) writes that the type of employer may dictate which laws (if any) potentially protect employees. If the employer is a government entity, then the Fourth Amendment may protect employee's right to privacy. If the employer has a collective bargaining agreement with a labor union, then the National Labor Relations Act (NLRA) and the bargaining agreement may protect a covered employee's privacy interests. The NLRA may also protect non-union employees' privacy interests under certain circumstances.

Different types of employers and employees - with different applicable laws - further complicate the legal issues. Current laws do not specifically state that monitoring employees is illegal. In fact, some organizations have used information obtained from monitoring employees as key evidence in many legal cases. An article by Meade (2001) on workplace privacy notes that e-

mail and Internet-use evidence has been used to prove critical legal issues in a wide variety of lawsuits, including race and sex discrimination, trade secret theft, and even the Microsoft antitrust case.

Another legal issue arising from employee monitoring is an organization's legal obligation to do so. Court (2004) discusses a recent survey reporting that 68% of employers who monitor employees' computer activities cite legal liability as their main motivation. Although Court writes, no court of law has ever ruled that an employer is required to monitor employees' electronic communications; some have suggested that such monitoring would be wise.

The courts can hold companies liable if they do not seek to prevent other employees from creating a hostile work environment. Employers may face liability for not only what someone communicates over the Internet, but also for what someone sees on workplace computer displays. For example, several Minneapolis Public Library staffers filed a complaint in 2001 with the U.S. Equal Employment Opportunity Commission stating that the library subjected them to a sexually hostile work environment after exposing them to hard-core pornography left on computer displays by library patrons *American Libraries* (2003).

Court (2004) describes other legal issues involving employee monitoring. For example, he discusses a case where a female employee sued her employer for allegedly creating a hostile work environment by, among other things, forcing her to look at sexually explicit websites. Besides web-based pornography, other electronic communications can create a hostile workplace. An e-mail may contain racist jokes or derogatory statements about males or females. Employers should take action against this type of harassment. Organizations are monitoring e-mail, blocking websites, tapping into phone conversations, and even tracking employees via GPS combining technology with policy to manage productivity and minimize litigation, security, and other risks. Organizations utilizing knowledge management techniques seek to monitor the environment and promot efficient transmission of knowledge (April, 2002; Bhatt, 2001; Keh-Luh & Chiu-Mei, 2012). To communicate the vitality of compliance with rules and policies, more than one fourth of employers have fired workers for misusing e-mail and approximately one third have fired employees for misusing the Internet, according to the 2007 Electronic Monitoring & Surveillance Survey from American Management Association (AMA, 2008) and The ePolicy Institute.

As mentioned above, laws governing employees depends on the employment relationship. For the most part, private employees have no right to privacy. Nevertheless, the Fourth and Fourteenth Amendments of the U.S. Constitution protect government employees from unlawful searches and seizures. Before the government employer can search a government employee's records or online activities, there must be reasonable cause for the employer to conduct the search. Court explains that reasonableness depends on whether an employee has a reasonable expectation of privacy with certain property, or in certain workspace areas. That may depend upon whether the work area is for the employee's exclusive use or whether office regulations placed employees on notice that certain areas were subject to employer intrusions. This interpretation of the law leaves the situation open for a case-by-case analysis. What one employee may consider reasonable a judge or the person's supervisor who conducted the search may not consider reasonable. After reviewing a large number of cases where the employee claimed Fourth Amendment protection, most courts seemed to rule in favor of the employer.

Currently, California is the only State with laws to protect the privacy of private employees. Some other States have similar bills in legislation with mixed support. Taking away a person's right to privacy at work is a controversial practice. A citizen of the Unites States of America has Constitutional rights to privacy in their normal daily life, yet if they go to work for a private business these rights no longer apply. Employers must maintain control over their workers to protect themselves, because if they do not monitor their employees then they could be liable for not doing so (Bezek, Britton, 2001).

Ethical Issues

Monitoring the actions of employees creates a debate about whether an employee should have the right to privacy. However, employee monitoring also brings up ethical questions. Woodbury (2003) explains that some of the ethical issues involve employees downloading pornography, putting personal web pages on company owned machines, or displaying offensive images on computer monitors. Employees have spent hours of their workday playing games on their computers, sending personal e-mail, or gambling. Two large problems are day trading and shopping online. (Woodbury, 2003) The ethical issues that an employer looks at may differ from what an employee considers ethical. It all goes back to a point of view on what is permissible and what is right or wrong. Woodbury continues that from the employee's point of view, businesses might act unethically while monitoring keystrokes, looking at private e-mail, or providing inadequate equipment that leads to vision, neck, hand, wrist, or arm damage. The keystroke monitoring is particularly invasive, because any time an employee rests, perhaps stretch for health or having a short chat for sanity's sake, the person is off task (Woodbury, 2003). Such strict monitoring can create rulings or workplace decisions that could discipline the employee for simply taking a legitimate break. The monitoring programs cannot know when an employee has an upset stomach and needs to be away from their desk - it just senses that the employee is not currently working. The employers get, in a sense, biased and incomplete data.

In addition, monitoring programs such as key loggers can be extremely invasive. Rosen (2000) describes a sophisticated monitoring program called Assentor that screens every incoming and outgoing e-mail for evidence of racism, sexism, or certain body parts. Assentor assigns each e-mail an offensiveness score and forwards messages with high scores to a supervisor for review. The program in this case is not another person, but it is able to calculate a formula to send the e-mail to a human supervisor to read the e-mail. Rosen writes that courts have ruled that government employers are free to search the offices of their employees for work related misconduct (when they have clear suspicion of wrongdoing), because people expect less privacy in workplaces shared with other employees. Some may view that as being unethical. A government employee assume that they are protected by the Fourth Amendment, but then a supervisor is able to search through the worker's e-mails, Internet history, or whatever else they may decide needs to be investigated. Looking at employee monitoring from an ethical standpoint, the practice should be subject to regulation. Yet current laws and standards provide few guidelines for regulating employee monitoring. There are several hundred programs similar to the one discussed. The newer programs are more robust, more available, easier to use, and can be completely invisible to the end user.

Solution

From the employer's perspective there are immense benefits to monitoring employees. Employers must have a thoughtful strategy to address scope of what they will monitor, how they will monitor who will perform the task, and how it will be funded (Bezek, Britton, 2001). Most workers would prefer that there be no monitoring, but employers need to have a system in place to ensure productivity and limit the risk of legal liability. Knowledge management systems put into place can effectively help an organization monitor users and provide benefits of improved performance, and increased organizational awareness (Oprea, 2012). Acceptable Use Policies are one of the most common company policies that outline how employees can use company systems and what they can expect as privacy. The task of creating and updating Acceptable Use Policies to address employee monitoring and privacy issues should not rest on the IT Department alone according to Duermyer (2007). Instead, policy writing, policy updates and compliance needs to be a cross-functional team effort that includes, representatives from human resources and if available, legal counsel, along with input from the IT group, who can best council on how monitoring can be accomplished, which activities will be monitored, who will be monitored, and what data will be available in monitoring reports. If an organization already has a policy in place, the company should audit the policy at least annually to determine if the policy is in step with current procedures. As with any corporate policy, an e-mail/Internet usage policy needs to be concise, easy to understand and consistent with the other business policies.

Employers must be especially mindful that many employees mistakenly think personal computer use at work is private. A computer usage policy needs a clear statement that employees should not expect privacy with anything they put on the company computer network. Employers should also state that they cannot "guarantee privacy" of e-mail communications, or indicate that employees with e-mail access automatically waive any right to privacy in their electronic communications.

Organizations should have the right to monitor their employees to maintain productivity, protect the company and the fellow employees. Even strong opponents to workplace monitoring, American Civil Liberties Union, agrees that the employer does have the right. The ACLU understands the necessity for some monitoring. The organization calls for fair standards such as employers notifying the employee, give the employee access to information being collected, and give the employee the right to dispute evidence. A computer usage policy needs to be clear so that an employee knows that the computer is property of the employer. If an organization is going to monitor its employees, then the company should give every employee a document explaining the policy to read and sign. It would also be prudent for the employer to create a training session to describe exactly what the policy does or does not allow. A training session would allow employees to ask questions about what is acceptable computer use, instead of having them disciplined for a violation. Different types of work would require different types (and amount) of monitoring. There is not a standard solution for every organization wishing to consider employee monitoring. As a part of the solution, the company should have safeguards in place to protect the well-being of the company as well as the employee. One reason employers need to protect themselves is that the a court may hold a company vicariously liable for failing to discover discriminatory or threatening e-mails sent over company computer systems. Anti-discrimination policies should blend readily with e-mail and Internet policies. Organizations

should reiterate their policies prohibiting discrimination and violence in the workplace when formulating e-mail and Internet policies. An e-mail and Internet policy should be included with a new employee's hiring package. Rosen (2002) recommends that employers warn employees about monitoring. Then employer surveillance could become a tolerated (but still intrusive) condition of employment. Clearly, there is a need for organizations to monitor their employees' computer usage. However, larger questions lie in what to monitor, when to monitor, whom to monitor, and even how to monitor. Each of the questions about who, what, when, and how must be answered on a company-by-company basis.

Conclusion

Maintaining a safe and efficient workplace requires organizations to keep a watchful eye on employee activities, which could pose harm to others or create liability for the company. One way for a company to maintain efficiency and lower liability is for the employer to monitor its employees. Monitoring, however, is only the first step. Employees must be educated about monitoring so that they can understand the lack of privacy that currently exists at work. Employees need to be educated to understand how technology works, to understand capabilities and limitations. Employers who monitor must be responsible and reasonable. Employers must explain to workers what they monitor. There must be a disciplinary plan to punish employees for computer-usage policy violations. As the law slowly catches up with technology, many questions remain. Privacy advocates will likely continue to push for reforms that would offer greater protection for employees. If history is any judge, these efforts will likely fail. It is likely that laws will grant organizations and even the government additional permission to monitor more facets of every citizen's daily life, inside and outside of the workplace. Organizations will need actively to train employees to correct the problems and misperceptions that currently exist with employee computer usage. If a business must monitor the activities of their employees to create a safe work environment, then so be it. Although some people and organizations believe that employee monitoring is wrong or unethical, there is a clear need for such practice. Employee monitoring is here to stay. The status of employee monitoring may change if laws tailor to the always-changing computer technology - but employee monitoring will not go away.

References

(2008). 2007 Electronic Monitoring & Surveillance Survey. *American Management Association*, Retrieved Feb 28, 2008, from http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey/

April, K. A. (2002). Guidelines for developing a k-strategy. *Journal of Knowledge Management*,6, 445-456.

Bezek, P.J., & Britton, S.M. (2001). Employer Monitoring Of Employee Internet Use And E-Mail: *MEALEY'S Cyber Tech Litigation Report*, *2*, Retrieved April 7, 2009, from http://www.foleybezek.com/art.InternetFile.pdf

Bhatt, G. D. (2000). Organizing knowledge in the knowledge development cycle. *Journal of Knowledge Management*, 4, 15-26.

Alexi, Edward (2008). The Law Requires Email Archiving. *IT Solutions, Tangent Inc.*

Collins, Z. (2002). No expectation of privacy on company computer used at home. *The Computer & Internet Lawyer, 19*(5), 35-37.

Court, L., & Warmington, C. (2004). The workplace privacy myth: why electronic monitoring is here to stay. *Employment and Labor Law, 1*(1), 1-20.

Crampton, S., & Mishra, J. (1998). Employee monitoring: privacy in the workplace? *Advanced Management Journal, 63*, 17 - 21.

Duermyer, Randy (2007, Sept 25). Balancing Employee Monitoring and Privacy Laws. *CopiaTech*, from http://www.copiatech.com/balancing-employee-monitoring-and-privacy-laws/

Duffy, Daintry (2003, Feb, 1). Employee Monitoring: Watch This Way. *CSO Online*, Retrieved April 21, 2009, from http://www.csoonline.com/article/print/217419

Frayer, C. (2002). Employee privacy and internet monitoring: balancing workers' rights and dignity with legitimate management interests. *Business Lawyer, 57*(2), 857 - 878.

Hart, Keith (2000). *THE MEMORY BANK: Money in an Unequal World*. Cambridge, England: Profile Books Ltd.

Hipple & Kosanovich, Computer and Internet Use at Work in 2001, *Monthly Labor Review*, U.S. Bureau of Labor Statistics, February 2003, 26-35.

Keh-Luh, W., Chi, C., & Chiu-Mei, T. (2012). Integrating human resource management and knowledge management: from the viewpoint of core employees and organizational performance. *International Journal Of Organizational Innovation, 5*(1), 109-137.

Marshall, P. (2001). Are tougher laws needed to protect citizens? *Privacy under Attack, 11*(19), 1-30.

Meade, M., ed., (2001). I've Got My Eye on You: Workplace Privacy in the Electronic Age, in *Practicing Law Institute Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series* (pp. 1 - 10). Practicing Law Institute - Thomson/West.

McEvoy, S. (2002). E-mail and Internet Monitoring and the Workplace: Do Employees have a Right to Privacy? , *Communications and the Law, 24*(2), 69-84.

Oprea, M. (2012). An Agent-Based Knowledge Management System for University Research Activity Monitoring. *Informatica Economica, 16*(3), 136-147.

Peters, Thomas A. (1999). *Computerized Monitoring and Online Privacy.* Jefferson, North Carolina: McFarland & Company.

Rosen, J. (2000). *The Unwanted Gaze, the Destruction of Privacy in America*. New York: Random House.

Staffers sue Minneapolis public library over hostile workplace. *American Libraries*, (2003), 34(5), 23.

Watson, N. (2001). The private workplace and the proposed "notice of electronic monitoring act": is "notice" enough? *Federal Communications Law Journal, 54*(1), 79-104.

Woodbury, M. (2003). *Computer and information ethics*. Champaign, IL: Stipes Publishing LLC.

Biography

Johnathan Yerby has been a Lecturer at Middle Georgia State College's School of Information Technology since 2009. His educational background includes degrees in Information Technology and Business, a Master of Management Information Systems, a Master of Business Administration, and he is currently pursuing a Ph.D. in Instructional Technology at Georgia State University. Prior to teaching, Professor Yerby held positions in technology management, network & systems administration, project management, financial lending, Mercer School of Law, print fulfillment, insurance software development, and payment processing services. Johnathan also successfully ran his own consulting firm for over ten years where his work included consulting for small business owners, medical, legal, and financial providers.