

SHOULD EMPLOYERS HAVE THE ABILITY TO MONITOR THEIR EMPLOYEES ELECTRONICALLY?

Danielle Dorval
University of Rhode Island

The purpose of this paper is to answer the question of whether or not employers should have the ability to electronically monitor their employees in the workplace. It stresses both the monitoring of computers, and also telephone wiretapping. The topic is examined through a legal, behavioral, and ethical perspective, to gain a more complete idea of the extent of the concern with electronic monitoring. Court cases were used to explain the different facets of the legal struggle between the employer's right to monitor and the employee's right to privacy. Several theories, including panoptic theory, were used to explain the behavioral effects of employer surveillance. Finally, the ethical issues with regards to electronic monitoring were explained through the idea of social control, and the balance of the needs of the employer and the needs of the employee.

Surveillance, in the workplace and in general, has a very important role to play in society. The main role is that of the power-generator (Lyon, 1994). Surveillance allows for people in control to keep a constant eye on those they are supervising. Instead of watching every person one at a time, but not seeing everyone at the same time, some types of surveillance can allow the supervisor to watch all of his employees at all times, or at least give those employees reason to believe that they may be constantly monitored. The usage of surveillance in the workplace is a very controversial subject, because monitoring an employee borders on a possible invasion of that employee's personal privacy. While there have been legal and ethical discussions regarding possible implications of using workplace monitoring, many employers still put these practices into use because they feel as though they have a right to be able to run their own workplace, and there is no legislature specifically forbidding the employer from utilizing certain types of monitoring under certain circumstances in their own business environment. Also, many behavioral issues have arisen from the usage of monitoring in the workplace, and in many other environments. Surveillance has been used a great deal by people in the position of power stretching far back in history, while electronic surveillance has grown in popularity during the last few decades.

The usage of surveillance began with the Israeli people back in the 15th century B.C. The Israelites created a census to be used for the

purpose of dividing the lands which they had conquered (Lyon, 1994). The census was studied by the people controlling the division of land, and the Israeli people were given a certain amount of land based on the findings of the study. This instance was the first in a long string of people in power monitoring their subordinates in order to control the masses. Some time after the Israelites had developed their census and used it to distribute property, new methods of recording data were developed, which led to increased levels of surveillance. The people in positions of power idolized the efficiency of military practices, and so they dreamt that their ideal workplace would operate similar to a military organization (Lyon, 1994). It was in response to the idea of this ideal workplace that employers developed a system of management in order to monitor their employees with greater efficiency. In another effort to control their employees, many managers took on the idea of Taylorism, or scientific management (Lyon, 1994). The practice of scientific management involved the breaking down of large tasks into fragments, or specific tasks performed by specific workers. This meant that the workers would no longer be able to have any autonomy with regards to their work, because they were acting as if they were different gears in a machine. Management was able to control its employees further by breaking down these tasks because they brought specialists into the company who watched the employees and determined how much time each task should take an employee. The employees' performance measure was based on

whether or not they could keep up to the standards set by the scientific management experts. This was the beginning of the practice of employers controlling their employees even down to the amount of time it takes the employee to complete a task, which is still prevalent in today's workplace.

In the computer age, surveillance, which was already occurring, was facilitated by the ease of using the computer. Computers made it easier for the employers to continuously monitor their employees for several reasons. The computer takes much of the mental burden of monitoring the employee off of the shoulders of management because the computer has the ability to monitor employees in certain ways that would be very tedious for management to monitor, including counting keystrokes to ensure that employees are being productive, and having the ability to monitor the content of e-mails and Internet usage (Lyon, 1994). Also, computers are more efficient than other types of monitoring equipment. Some reasons for this efficiency of computers are that information is easily deleted or altered if necessary, and they take up less space than most paper-based systems of surveillance and information keeping. The relatively easy deletion of information can be related to the idea of the Ministry of Truth in *1984* by George Orwell (Lyon, 1994). In *1984*, the job of Winston, who is the main character, is to delete past information from newspapers and other written materials and replace it with updated information, which makes it look as though the leader of the Party is always correct and never makes bad predictions (Orwell, 1949). A computer-based system of surveillance can erase information as quickly as the workers at the Ministry of Truth. Also, since a good deal of information can fit on a computer disc, the times of keeping all of the information written down on paper are over. Instead of the cabinets filled with paper, the company could have a drawer in a file cabinet with computer discs containing the same amount of information, which can be obtained by the use of different methods of monitoring.

Although there are other means by which employers are able to monitor their employees, the majority of the monitoring is done by computer and telephone monitoring. Employers have the ability to monitor their employees by recording the

amount of time the employee spends using the computer, recording the amount of time spent using the phone, and several other means of monitoring about which the employee may or may not know. In the past, employers have monitored the websites which employees visit, the content of e-mails written by employees, telephone calls which may or may not be business-related, and the number of keystrokes done by employees (in order to measure productivity) (Wood, 2001). In order to monitor the websites that employees may visit, the employer may put up a firewall in order to block the employee from visiting sites that the employer does not deem necessary for the completion of business. Several ways in which an employer can monitor e-mail usage are: spot checks of e-mail, looking at e-mail from a specific employee, or flag e-mails which include terms for which the employer is looking (Wood, 2001). Employers may be able to listen in on telephone calls made by employees by way of attaching recording devices to the phones and then listening to the conversation at a later time, or by listening to the conversation via another phone extension. Also, employers can monitor their employees' productivity by the usage of software which has the ability to count the number of keystrokes that they make (Wood, 2001). The number of employers using these methods of electronic monitoring has increased in the past few years.

Electronic monitoring has seen an increase in usage, and generally, a decrease in the cost to the company (Wood, 2001). For example, in a study conducted by the American Management Association, it was found that at least 20 percent of employers use e-mail monitoring systems in their workplace, which when compared with a study done in 1997, shows an increase of 5 percent (Adams, 2000). When one imagines the number of employees working for that 20 percent of companies, this monitoring of e-mail and/or computer usage affects around 14 million workers in the United States (Wood, 2001).

WHY DO EMPLOYERS MONITOR EMPLOYEES?

There are a number of reasons why employers desire to monitor the behavior of their employees. Some of these reasons have existed long before the use of computers in the workplace became

commonplace. Others emerged with the widespread use of electronic communication and data storage. It is important to note, that the answer to my research question often depends on the purpose for surveillance. The following sections describe some of functions of electronic surveillance

Employer Liabilities

An important purpose that electronic monitoring serves the employer is that of protection from various legal issues which could arise through employee use of the Internet and/or the e-mail system which is owned by the employer. Some of these legal issues are: accusations of harassment, copyright infringement, the protection of important company information, and a possible loss of productivity (Hubbart, 1998).

Harassment. Electronic communications have been permitted as evidence in harassment cases. E-mail communications, even if they have been deleted by the recipient of the message, still remain on the hard drive of the computer, and may be accessed by the employer (Place, 2000).

Software Copyright Infringement. If the employee disobeys the copyright laws while operating the employer's computer system, the employer is at fault and could be penalized for the breaking of these laws. This is because the employer owns the operating system and is liable for anything that is done through that system. The employer is technically only legally liable if they are aware of the copyright violation and they do not do anything about the violation (Place, 2000).

Information Theft. E-mail is a very easy mode of sending private company information to persons not operating within the company. From that point, the information, either a purposeful sharing of company secrets or not, can be forwarded to other unauthorized parties, or otherwise used against the company (Place, 2000).

Employee Productivity

Since employees spend a good amount of their workday on the computer, they may feel that they have the right to take care of their personal computer use on company time. This time spent on personal computer usage subtracts from the time that the employee has available to serve the

employer. Employers are more concerned with productivity in the current workplace than they have been in the past, mainly because the labor market pushes the businesses to be more competitive, and many company owners feel that the only way to be more competitive is to increase the production levels. Since personal computer usage during the workday is so rampant, employers feel as though they must crack down on e-mails and Internet usage (Place, 2000). Also, the expansive amount of time that employees spend on the Internet leads to large costs for employers, taking into account both production costs, and the amount for which the employer is paying wages while the employee is not reciprocating with their labor. For example, 96.5 hours are spent per 100 employees every day using the Internet. Not all of these Internet hours are spent taking care of non-work related business, but the great majority of employees spending time surfing the Internet is non-work related (Wood, 2001)

ALTERNATIVE SOLUTIONS TO ELECTRONIC MONITORING

There are some potential alternative methods that employers could use to combat some of these issues for which they are implementing electronic monitoring procedures. In the instance of accusations of harassment, in which the employer would red flag e-mails containing keywords which could be alarming, they could implement a zero-tolerance policy instead of the monitoring. Since most action is taken after several inflammatory e-mails, the zero-tolerance policy would stop the harassment after the first instance. Therefore, it would operate faster and be more effective than the e-mail screening policy. In the case of copyright infringement, electronic monitoring is really the only effective method of preventing the employee from breaking copyright laws. With regards to the protection of private company information, there are several methods that could be used by the employer. The employer could implement a need-to-know policy with company information, and only let employees who are beyond a certain level know the private information that could be damaging if leaked to an outside source. Also, the employer could only provide e-mail and Internet access to those employees who require the use of these amenities for their job. In this way, the employer would not

have to implement a company-wide electronic monitoring policy. With the issue of employers worrying that the employees are not being as productive as they would like them to be, the employer could set goals which are attached to incentives, either group-based or individual-based in order to induce the employees to respond with higher productivity levels. These goals should create enough of an incentive so that the employer does not have to implement a policy regarding electronic monitoring.

POSSIBLE WAYS EMPLOYEES COULD AVOID BEING MONITORED

The employee could attempt to avoid electronic monitoring by the employer in several ways, including taking a privately owned laptop computer to work, or by accessing the Internet via a cellular phone (which would also avoid instances of wiretapping) (Class discussion 4/19/04). The employee could also plan to take care of any personal business about which they would not want co-workers to know, either outside of the workplace while on breaks, or before or after leaving work for the day. One complication with the idea of the employee bringing a personal portable computer to work is that they will most likely have to access the Internet through the employer's computer server, so they would have the capability of being monitored regardless if they were using company property to do so or not. The only way that the employee could avoid scrutiny by using a laptop computer is to have a wireless Internet connection. The most effective method of obtaining a wireless Internet connection is to use a cellular phone to link up to the Internet. The employer has no effective method to monitor the employee's use of their cellular telephone, but they can implement a policy either banning cell phones from the work environment or allowing people to have cell phones, but not allowing the employees to use the cell phones during their work time (Class discussion 4/19/04). In general, if the employee were using the Internet for personal use during the work hours, they would be just as able to use the Internet in the privacy of their own home for that same purpose. Many companies make the employees aware that they are being monitored during their use of the Internet by placing a disclaimer as the employee logs onto the Internet. If the employee is planning on spending

time on an activity of which they do not want the employer to be aware, they should save that activity until they are logging onto the Internet under their own privacy at home. If the employee needs to take care of personal telephone business during the workday, they should be able to take their cellular phone outside in order to make sure that their phone call is a private call. These are methods in which employees can avoid the constant eye of the employer.

LEGAL PERSPECTIVE

Legal Risks of Monitoring to Employers

The risks to employers of monitoring their employees are negligible based on the legal perspective. Most courts will side with the employer if a case of workplace monitoring and an employee's right to privacy is brought to the courts. Since the courts generally side with the employer, the legal risks to the employer should not be a large factor in the decision whether or not to monitor the employees.

Fourth Amendment to the Constitution.

The 4th Amendment to the Constitution states that American citizens can enjoy freedom from unreasonable searches and seizures by the government. Many people believe that their workplace privacy rights are protected by the Constitution of the United States, but this amendment only covers workplace privacy rights for employees in the public sector. Also, as with the other laws concerning privacy in the workplace, the 4th Amendment right to privacy is weighted against the interests of the employer (Hubbarrt, 1998). Based on the *O'Connor* case, a search by a public employer will be examined to determine reasonableness based on whether the employer has created a reasonable expectation of privacy for their employees (Place, 2000). In general, in cases where the employee is bringing a case against the employer over their right to privacy, the court will tend to side with the employer (Colucci, 2002).

Electronic Communications Privacy Act.

The main purpose of the Electronic Communications Privacy Act (ECPA) is the protection of electronic communication systems from access that is not authorized by the user and it also protects the privacy of public service e-mail

systems, such as AOL. This Act does not, however, protect employees from having their e-mail monitored by their employer (Hubbartt, 1998). Since the e-mail system used in the workplace is owned by the employer, and is not a public system, the ECPA does not cover e-mail systems in the workplace. The ECPA “prohibits the interception and monitoring of electronic communications” (McKelway). However, the Stored Communications Act (SCA) allows the employer to have access to stored electronic communications, including e-mail. An employer can monitor e-mail if the contents relate directly to the business. Also, if the employee gives consent to the employer, the employer generally has the ability to monitor the electronic communication. Consent may sometimes be implied, but it must be under very specific circumstances. For example, if the company has a policy that they might monitor any telephone calls for a time to determine whether they are personal or business related calls, any employee who chooses to make or receive a telephone call will be considered by the courts as having given implied consent (McKelway). Court cases have determined that access to electronic communications by persons other than the addressee are only prohibited if the communication is in storage prior to the delivery of the communication to the recipient (King, 2003). The ECPA also only covers “the interception of wire, oral, and electronic communications” (Schnaitman, 1999).

Omnibus Crime Control and Safe Streets Act. This law covers invasion of privacy claims that are brought on by instances of telephone monitoring. This act only covers private employers, and it prohibits intentional interception and disclosure of telephone communications. In order for employers to comply with this act, the FCC requires that the parties involved give their consent to the monitoring prior to the start of the monitoring, or the employer must have a tonal indication of monitoring sounded at intervals (Hubbartt, 1998).

Tort Laws and Invasion of Privacy. Invasion of privacy is a right that most people believe is a constitutional right. However, it is not mentioned in the constitution and has only been developed through the outcomes of court decisions. Therefore, it is a common-law right,

and not a constitutional right (Hubbartt, 1998). Employees have four basic bases for tort claims of privacy invasion: intrusion upon seclusion, public disclosure of private facts, publicity placing the person in false light, and the appropriation of the employee’s name or likeness (Hubbartt, 1998). In cases of electronic monitoring, we are mainly interested in claims of invasion of privacy under the basis of intrusion upon seclusion. In order to claim invasion of privacy under the base of intrusion upon seclusion, the employee must prove that they had a reasonable expectation of privacy in the workplace. If the facts of the claim do not meet the court’s requirements, the court will rule in favor of the employee (Hubbartt, 1998). In a civil case, which a tort case of invasion of privacy is, the plaintiff (employee) always bears the burden of proof. The employee must prove that it was the intent of the employer to intrude upon their privacy rights. They must show that the employer knowingly, not necessarily intended for, but knew that their action may have caused the invasion of privacy (Bible, 1990). The employee must also show that there is a reasonable privacy expectation in the workplace, that this expectation was held, and the employer did not have a true purpose for the invasion of privacy (Schnaitman, 1999). Most of the time, when an employee brings a tort claim against their employer regarding an invasion of privacy, the court rules in favor of the employer. Employees who work beneath an employment-at-will agreement do not enjoy a right to privacy which limits the employer’s ability to monitor their employees electronically (King, 2003).

One important issue with respect to invasion of privacy claims is that of the employee’s expectation of e-mail privacy. Even with the action of having the employee create a password to enter his or her own e-mail account, the employee still may not have a reasonable expectation of privacy with regards to their work e-mail account. In order to avoid complications with the issue of the expectation of privacy on the employee’s behalf, the employer must create a policy regarding e-mail and Internet usage, and also abide by that policy (Bible, 1990). Many employees believe that they are safe from being monitored and used in the incorrect manner because they are under the impression that e-mail is non-permanent, and also confidential. E-mail is

actually stored in the computer even after the employee believes that it has been deleted. Also, once the employee sends the e-mail to another person, they have no control over whom the recipient of the e-mail might forward the e-mail, and the e-mail could just keep being sent out to an ever-widening area of people. E-mail can be very effective evidence in litigation suits on the side of either the employer or the employee (Smith, 2001).

Examination of Court Cases

In *Simmons v. Southwestern Bell Telephone Company*, the plaintiff brought a case against his employer stating that the employer had been monitoring his private telephone conversations. The plaintiff had worked for the employer at the “testdesk”, a help-desk for customer questions. Simmons was aware that the company had a written policy stating that the employees were not allowed to have personal phone calls while at the testboard (1978). The plaintiff claimed that the employer violated his 4th Amendment rights when the employer monitored his telephone calls. In this claim, the courts argued in favor of the defendant, stating that the plaintiff’s 4th Amendment right was not violated because that right is not protected unless the claim is against a government intrusion into the person’s privacy (1978). Also, the Constitutional right only protects a reasonable privacy expectation, and the plaintiff knew that there was a policy against personal phone calls at the testboard. Simmons also argues that the company only has the right to monitor telephone calls if fraud against the company is suspected. However, the Omnibus Crime Control Act allows for the company to monitor phone calls for the means of any activity which is necessary for service (1978). The plaintiff also had prior knowledge that there was a telephone available for personal use, and he chose to make his personal phone calls at the testboard. Since the plaintiff knew that his calls from the testboard would be monitored, he was unable to show a reasonable expectation of privacy for his phone calls (1978).

In *Watkins v. L.M. Berry & Company*, the plaintiff brought a complaint against telephone monitoring because her employer had monitored a personal phone call that she had received. During

this phone call, she had discussed an interview that she had had with another potential employer. In this case, the monitoring was accomplished using a normal extension telephone from the supervisor’s office. The defendant had a policy that the employees were allowed to make personal phone calls, and those calls would not be monitored longer than was necessary to determine whether they were personal calls or business calls (1983). The employer argues that the plaintiff had granted consent by using the employer’s phone and knowing that it was possible that her call might be monitored. One issue is “whether the monitoring of this call was in the ordinary course of Berry Co.’s business” (1983). The consent granted by the plaintiff was only for the employer to realize that the call was a personal call, and any monitoring beyond that point was not something to which she had consented. Since implied consent of telephone monitoring has to be under explicit circumstances and the plaintiff did not know that her phone call was going to be monitored, the court found that the knowledge that her employer was capable of monitoring her phone calls did not mean that she had consented to the monitoring (1983). The second issue in this case was “whether the interception of this call was in the ordinary course of business” (1983). The employer must show that any monitoring beyond discovering what type of call was being made was necessary in the course of business. For the phone call to be important in the course of business, the company must have some sort of legal interest in the topic of conversation. While the company may have had an interest in the topic of Watkin’s conversation, they did not have any legal interest in that conversation. In this case, the court ruled that “a personal phone call may be intercepted in the ordinary course of business to determine its nature but never its contents” (1983).

In *Bohach v. City of Reno*, the plaintiffs, two police officers, brought a claim of invasion of privacy to the courts to stop an investigation into their usage of the department’s paging system. The Chief of the Police Department had issued an order stating, among other things, that the messages sent through the paging system would all be logged onto the network. Every message that was sent through this system was stored in a server file and then sent to the receiving party (1996b). The officers claimed that the monitoring

of the paging system had violated their 4th Amendment right to privacy. They claimed that their messages had been wiretapped when they had sent them through the system. The problem with this claim is that the messages are normally recorded and stored in the paging system because it is necessary for the operation of the system. Since all of the Police Department had access to the paging system and the messages were stored in the computer file, the officers did not have a reasonable expectation of privacy (1996b). Also, it is common knowledge that police departments keep a record of all incoming and outgoing phone calls to the station. Therefore, the practice of monitoring the phone calls that go into the pager system is simply done in the course of everyday operations. The pager messages were not intercepted during the transmission of the message to the recipient, but they were monitored while they were in storage after the transmission. Since the ECPA only protects messages which are in transmission from one party to another, the person who intercepted these pager messages while they were in storage did not violate the ECPA (1996b). Also, the City of Reno is the provider of the pager service, and therefore, has the legal authority to access communications which are in electronic storage (1996b).

In the case of *Steve Jackson Games, Inc. v. U.S. Secret Service*, the plaintiff brought a case against the U.S. Secret Service because they feel that the government violated statutes while seizing materials from the plaintiff's property. Steve Jackson Games ran an electronic bulletin board with information regarding role-playing games, which also allowed users to communicate using an e-mail system run through the website. The users could also receive private e-mail through this website. The e-mail would be stored on the main computer's hard drive until the users logged on to the website in order to read their mail (1994). One of the files that was included on a website run by an employee of the plaintiff contained information regarding a private emergency call system. The FBI was informed of this publicized private information by the owner of the private company that owned this information. A Secret Service agent applied for a warrant to search both the company and the home of the employee who had this information on his website. During this search, the main computer was seized from the

business location, which at the time had e-mail messages, that were unread by the intended recipient, stored on its hard drive (1994). The district court held that the government was not in violation of the ECPA because the e-mails were not intercepted while they were in transmission to the recipient. The e-mails in question are in electronic storage, albeit temporary electronic storage, but they can be legally intercepted at any point that they are in storage (1994).

In the case of *Fowler v. Southern Bell Telephone and Telegraph Co.*, the defendant brought a claim of invasion of privacy by wiretapping against his employer. The plaintiff alleged that two special agents and her employer had placed a wiretap on her telephone at work, and had monitored her personal phone calls. The special agents denied having placed a wiretap, but argued that such a procedure would have been within their rights as government agents (1965). However, there were no actions taken by the special agents that created proof that they were in fact federal agents and were in possession of these governmental rights. In the state of Georgia, where this case is being argued, eavesdropping is considered to be a misdemeanor. An eavesdropper is "one who peeps through windows or doors, or other like places, on or about the premises of another, for the purpose of spying upon or invading the privacy of the persons spied upon, and the doing of any other acts of a similar nature, tending to invade the privacy of such persons" (1965). Even if the information discovered is kept only to the knowledge of the person discovering the information, according to the state statutes, the person who was spied upon still suffered from an invasion of privacy. In this case, the agents, providing they had delivered the proof that the government in fact employed them, may have had the ability to place a wiretap on the plaintiff's telephone. Since they were unable to show proof of their government employment, this case falls under the jurisdiction of the Georgia state statutes, and federal agents are guilty of eavesdropping and causing the invasion of privacy suffered by the plaintiff (1965).

In the case of *Briggs v. American Air Filter Co., Inc.*, the plaintiff brought a case against their employer alleging that the employer and branch manager violated wiretap laws and caused an

invasion of privacy. The manager had been suspicious about possible company information being discussed with employees of another competing company. The plaintiff kept contact with a former employee of the defendant who currently worked for a competing company. The manager suspected that the plaintiff was disclosing private information regarding the company plans to competitors (1980b). It was due to this suspicion that the phone calls between the two parties were being monitored, but neither party had been informed of the monitoring, and neither had given their consent to the manager, or the employer. This interception of an electronic communication, wire communications are included in the definition of electronic communications with regards to the ECPA, occurred during the transmission of the communication, which is generally prohibited by the ECPA. The question before the courts in this case is “whether the act of listening-in was ‘in the ordinary course of business’” (1980b). As a general rule, the courts have decided that the use of an extension telephone to monitor a private phone conversation cannot be considered to be part of the ordinary course of business. However, the plaintiff has agreed that this particular telephone call was a business call, not a personal one, so this issue of whether or not the monitoring is authorized is out of the question. In this case, the court decided that “when an employee’s supervisor has particular suspicions about confidential information being disclosed to a business competitor...and knows that a particular phone call is with an agent of the competitor, it is within the ordinary course of business to listen in on an extension phone for at least so long as the call involves the type of information he fears is being disclosed” (1980b). In short, if the telephone call, or electronic communication, involves the transfer of private information to a competitor of the business, the monitoring of the telephone call is within the ordinary course of business.

In the case of *Awbrey v. Great Atlantic & Pacific Tea Company, Inc.*, the plaintiff filed a case against the employer alleging that a wiretap had been placed on the telephone at the workplace. The employer argued that the employees could not produce any evidence that there was such a wiretap placed on the telephone and that they

could not confirm the monitoring of telephone calls. In actuality, the plaintiffs could not specify any particular phone call which had been tapped by the employer (1980a). This is not to say that the employees could not allege that there was in fact a wiretap placed on the telephone line. It would be a rare allegation of wiretapping if anyone other than the defendant had knowledge of the specific wiretapping incidents. This is because “the more successful the tortfeasor is, the less likely it is that plaintiff will know of it” (1980a). Therefore, the plaintiff does not have to be able to point to any specific instance of wiretapping in order to bring a complaint of wiretapping to the courts. Also, the employer argued that the employees had passed the statute of limitations with regards to court cases about wiretapping. The federal wiretapping laws do not specify any statute of limitations for this type of accusation, so the employer does not have an argument which will cause the courts to dismiss the case (1980a).

In the case of *Konop v. Hawaiian Airlines, Inc.*, the plaintiff brought a suit against his employer alleging that the employer entered onto a website of which he was not an authorized user by gaining access through another employee. The website contained critical postings regarding his employer and the union of which he was a member (2002). Konop had determined certain co-employees who would be able to access this site; managers were not included on this list of co-employees. When the authorized users first logged onto the website, they had to put in their user name, and then create a password for themselves. After this step, they had to read and then show acceptance of the terms and conditions of the site, which included a statement denying the entrance of any of the company’s management (2002). In electronic terms, “a website consists of electronic information stored by a hosting service computer or ‘server’” (2002). Based on this information alone, it would seem that anyone would be able to monitor the goings-on of this website because the electronic communication would be in storage, and not in the middle of being transmitted. The only problem with restricting the users of this website is that it is not possible to know if an unauthorized user is logged on to the site if that user knows the information, such as user name and password, to log on as someone who is thus authorized. “The SCA makes it an

offense to ‘intentionally access without authorization a facility through which an electronic communication service is provided ... and thereby obtain ... access to a wire or electronic communication while it is in electronic storage in such system’” (2002). This means that since the management of the company was not authorized to access the website, they cannot claim that they legally obtained the stored electronic communications which are located on the website. The SCA enables authorized users to permit unauthorized users to view the electronic communication, in this case, the website. Under the assumption that the authorized employee had been a user of the website, that employee would have been able to allow the manager to view the website. However, the employee who permitted the manager to log on to the website using their name had not previously used the website, so that employee was not an authorized user who would have the ability to permit a third-party user to view the website (2002).

In the case of *Ali v. Douglas Cable Communications*, the plaintiffs brought a suit against their former employer for monitoring and recording their workplace telephone calls. The employer monitored the telephone calls in order to train the customer service representatives and to improve the customer service being exuded by the representatives. Regular business extension telephones were used in the monitoring of these telephone calls. Some of the employees were aware that there was monitoring of telephone calls, while others were not aware of this practice (1996a). The manager stated in front of the court that she would stop monitoring a telephone call once she realized that it was a personal phone call. There was no policy forbidding the customer service representatives from making personal calls at their own desks and the managers were aware that such calls were being made at those locations. In the beginning of April 1993, a memo was handed around to the representatives stating that the phone calls of some of the employees, including Jan Ali’s calls, would be recorded for the training of effective techniques. The plaintiff was made aware of this memo about three days later than it had gone around to most of the employees. Prior to that date, some of the telephone calls made by the plaintiff had been recorded pursuant to the procedures outlined in the

memo (1996a). A phone for personal calls was not installed for another ten days. Although the plaintiff made personal calls from her phone located on her desk after she was aware of the memo, the fact that she had knowledge that her phone call could be monitored does not give the employer her implied consent. In this case, the plaintiffs have compiled enough evidence that they did not have enough knowledge or notification of the monitoring for the employer to have implied consent from the employees. In order for the employer to prove that the extension telephones are regular business equipment and they are used in the ordinary course of business, two different tests must be met (1996a). The first test is whether the telephone provider furnishes that type of equipment in their ordinary course of business. The company that provided the telephone system for the employer is in the business of generally providing that type of extension telephone. The second test is whether the employer used that equipment in the ordinary course of business. Since the employer was using the extension phones in order to monitor the customer service representatives' telephone calls for quality control, the employer did in fact use the extension telephones in the ordinary course of business (1996a). Although the employer can show an adequate reason for monitoring the business calls of the employees, there is no reason shown for the monitoring of the personal phone calls of the customer service representatives. The original practice of only monitoring personal telephone calls until the nature of the call was discovered is allowed under the business exception. However, the employer does not offer an adequate reason for the recording of all telephone calls, including personal phone calls (1996a). The plaintiffs also allege that the employer committed an invasion of privacy, and that plea of invasion of privacy includes the theory of intrusion upon seclusion. In order to prove that there was intrusion upon seclusion, the plaintiff must show that the intrusion is intentional interference, and that the whole idea of the intrusion would be “highly offensive to a reasonable person” (1996a). It is possible that a reasonable person would be highly offended if their personal telephone calls were being recorded if they were allowed to make phone calls at their desk, and they were not informed of the monitoring (1996a).

BEHAVIORAL PERSPECTIVE

Behavioral Risks of Employee Monitoring

Although the legal response to the question of whether or not electronic monitoring should occur in the workplace is important to employers, they should also be concerned with how the monitoring will affect the behavior of the employees. Employees are bound to have a reaction to the monitoring of their behavior and it may not be worthwhile for the employer to set up monitoring efforts if that would eventually be counterproductive for the employer. The behavior of the employee could at least affect the methods of monitoring used by the employer. Some theories that are useful when examining the behavioral perspective of electronic monitoring are: equity theory, resistance theory, and panoptic theory.

Equity Theory

Using this theory, we can explain the relationship between employee and employer as a relationship of the balance of inputs (generally created by the employee) and outputs (what it put out by the employer). The employee perceives this balance as equal if they think that the inputs are balanced out by the outputs which the company gives back to the employee (Vorvoreanu, 2000). If the employee believes that the exchange of inputs and outputs is not equal, they will feel a psychological drive to rebalance the equation. The single method that can be used by the employee to rebalance the inputs and outputs is by changing the amount of inputs, or the amount of productivity, in order to alter the ratio of inputs and outputs for the company. One way that the employee can change their productivity is by changing the amount of work that they provide for the company (Vorvoreanu, 2000). While equity theory is generally related to the balance of labor and extrinsic rewards, it can be extrapolated to relate to the balance of power between the employee and the employer. When the employer decides to monitor the employee electronically, the balance of power becomes tilted in favor of the employer. With this imbalance of power, the employee feels a psychological motive to take back some power. Since the employee can only change what they put into the relationship, they must change their rate of

productivity, showing that they still retain some power. This is counterproductive to the employer because they are monitoring the e-mail and Internet usage in order to increase productivity (Vorvoreanu, 2000).

Resistance Theory

With regards to this theory, employees are thought to be rebelling against the electronic surveillance in the workplace. While many employers seek to bring discipline into the workplace, the presence of electronic monitoring may cause the opposite reaction in the workers. Since workers are under the power of the employer, any action of the employer will cause a reaction in the employee. Sabotage is seen as a type of resistance because it is defined as a type of action, or thought process which the employee uses to try and diminish the goals of the company (Vorvoreanu, 2000). Some motives behind these acts of rebellion are: a decreased amount of control held by the employee and a negative sociological affect. Electronic surveillance leads to a decreased amount of control because the employee has the feeling that every moment of their day is being watched by the employer and they must obey the wants and needs of the employer at all times, since there is a possibility that they will be caught in the process of doing something which is not work-related (Vorvoreanu, 2000). Since the employee has lost some of their former control over their actions, electronic monitoring is a means of the employer gaining more control over the employees. A negative affect occurs when the person in question has a type of monotonous feeling about them, and they do not really show their emotions or thoughts regarding a situation. Negative affect in an employee can be caused by electronic monitoring because the employer has effectively removed any feeling that the employee is anything more than another "gear in the machine". Electronic surveillance can cause employees to perform their work to the letter of the procedure, and not really own their own thoughts or methods of doing things (Vorvoreanu, 2000). It is almost as though the electronic monitoring has taken away the employee's sense of self. Therefore, the employee is figuratively similar to a part of a machine. There is a strong connection between the ideas of power and resistance. Resistance is always

present in employee/employer relations, and this is shown because there is a history of the exercise of power in this relationship. There is no need for the exercise of power if the employer is not running into any resistance from the employee (Vorvoreanu, 2000). Electronic monitoring is a means of the employer exercising power over the employee, and therefore, the employee is resisting the entrance of electronic surveillance into the workplace in the same fashion that they would resist any type of power exercised by the employer (Vorvoreanu, 2000).

Panoptic Theory

This theory is in conjunction with the ideal of the panoptic prison, designed by Bentham. As a result of the design of the prison, which has, at the center, a station designed for the guards which allows the complete view of whichever inmate the guard is monitoring at the time, the inmates have an instilled idea that they are in a constant state of being watched (Lyon, 1994). Even though the guards do not have the ability of watching every single inmate at the same time, the inmates never know when they are being monitored because the setup of the prison does not allow the inmates to see which inmate the guard is in the process of watching. This is similar to the monitored employee who assumes that they are always being monitored because they have no way of knowing which employee the boss is watching, or if the software in the computer will catch on something that they wrote in an e-mail (Lyon, 1994). Since the employee is not sure whether or not they are being watched at any given time, they will consistently act in the manner in which they believe the manager would like them to act. In this way, the employer can insure that the employees are complying with the standards of the company. Panoptic theory leads to the notion of electronic surveillance as a means of social control (Lyon, 1994).

Social Control

Although social control has been rampant in today's society for longer than electronic surveillance has been a controversial issue, people have not reacted to other forms of social control that have been forced upon themselves from other forces than the workplace. An example of a type of social control that has been streamlined into the

thoughts and minds of people for a long time is the commercials that are aired on television. Although we may not think of television commercials as a form of social control, they do shape our thoughts as to what products we as a society should purchase (Lyon, 1994). All businesses know that the more advertising that they put out for society to view, the more people will buy their product. One of main components of being able to sell their product is to have enough advertising so that consumers are aware of the product. The volume of television viewers watching particular channels at particular times is monitored electronically, as are the employees who are being monitored by the employer. Just as commercials manipulate the minds of the television viewers, the supervision and monitoring by managers manipulates the minds and the actions of the employee (Lyon, 1994). Another form of social control used in the workplace is the idea of Taylorism, or scientific management. Scientific management is the idea of breaking down a larger task into smaller pieces, and assigning an employee to each of the smaller tasks. This process induces social control in the workplace because the workers have decreased, if any, autonomy, and the management completely controls the production process. In this case, the worker is manipulated by the employer into performing that one task, becoming highly skilled at that task, and still not understand the whole process involved in producing the product. Since the worker may not understand the entire production process, the employer still has control over the ins and outs of the process and the employee is unable to offer suggestions which may make the process more efficient (Lyon, 1994). Most people are not aware as to how much surveillance they are under in a day-to-day basis. They have the opportunity to be scrutinized every time they use a credit card, show a form of identification, or ask for information regarding an account of any type. The type of monitoring which takes place in daily life today could lead to more stringent and constant monitoring in the future (Lyon, 1994). This possibility of increased monitoring could lead to undesirable effects on the people living in the future.

Comparison with *1984*

In the novel *1984* by George Orwell, the main character lives in a society where he is being constantly monitored in every way, even his thoughts are monitored. In every apartment in this world, there is a screen that covers almost the entirety of the place and the leader of the ruling party can monitor any move that the citizens make, if he decides to do so at that moment (Orwell, 1949). This is similar to the theory of the panoptic prison, in which the guards have the capability of monitoring any of the prisoners at any given time, and the prisoners will not have the ability to tell whether or not they are in the process of being monitored (Lyon, 1994). However, the prisoners have complete control over their personal thoughts, while the characters in Orwell's *1984* have no control over anything that they think or do. Some of the most important trends in *1984* relating to workplace monitoring are those of oppression and resistance to the idea of surveillance. In *1984*, the leader of the party, Big Brother, determines not only how the citizens will act in the future, but also punishes those who do not act exactly as he wishes by exterminating them. The newspapers are altered in order to create the idea in the minds of the citizens that Big Brother is never wrong in his predictions. Big Brother creates an oppressive feeling in the people of the society because he appears to be omnipresent, and always watching (Orwell, 1949). In the workplace, the manager seems to be omnipresent because it is part of their job description, and because the employee has knowledge of the capability of being electronically monitored (Lyon, 1994). Even though the manager may not always be present in physical form, the employee is aware that the computers contain software with the ability to monitor not only their keystrokes, but also the content of the e-mails that they may write (even to other employees), and the employer has the ability to access any information which is captured by that software (Wood 2001). Also, the peer pressure of other people who are part of the same society helps to contribute to the oppression. In *1984*, all of the citizens who are part of the "Party" join together once a day for the "10 minute hate", after which they all join in screaming at people who oppose Big Brother and everything for which he stands. If one person does not participate in this screaming and yelling, they are thought to be

against the concept of Big Brother. Since opposing the concept of Big Brother will bring about a sure extermination, it is important to every citizen that they act appropriately in response to his ideas (Orwell, 1949). In some workplaces, employees are empowered to act upon what they know to be right if they see another employee going against the system. It is in the hopes of managers that the employee who is going against the oppression will be set straight by the actions of their co-workers. This may not always occur the way that the managers would like because if there are no employees who feel as though they should do as the managers say, there will be no example for the wayward employees to follow.

In *1984*, Orwell seems to be concerned with the idea of behavior modification and what lies in store for society in the future. At the end of the novel, the main character undergoes behavior modification in order to make him believe fully in Big Brother before he is exterminated (Orwell, 1949). Workplace monitoring is related to the idea of behavior modification because the employer is attempting to alter the work behavior of the employees by creating the impression that they are constantly being monitored. The employer is trying to modify the original behavior of the employee into behavior that is more desirable to the employer (Lyon, 1994). This behavior modification is similar to the idea of Skinner's box. Skinner's box is a psychological idea in which an animal is placed in a box where it can see food, and must modify its behavior in order to figure out how to obtain the food. It is an illustration of the connection between behavior and reward (Lefton, 1997). This extends to the workplace where employers will tend to reward those employees who present the behavior that is the desired end result of the behavior modification. A problem that the link between behavior modification and reward causes is that of employees pretending to embody that desired behavior in order to obtain the reward offered by the employer. While the employer is hoping that the employee is transforming their old behaviors into new, more desirable behaviors, the employee is only acting in the way that the employer expects in order to get the reward. If the employer were to stop giving the reward in response to the behavior that they would like to get from the employees, the employee who was only acting in the desired way

for the reward will revert to their former behaviors. The best way to avoid this problem with behavior modification attempts is to give out the reward at variable intervals, instead of giving it out every time the employee shows a desired behavior. As a result of giving out the reward for behavior at variable intervals, the employees who were only acting in the desired fashion will not do so because they are not guaranteed a reward, while those employees who had embodied the desired behaviors will continue exuding those desired behaviors without the promise of a reward (Lefton, 1997).

In 1984, Orwell develops a theory of resistance to surveillance with regards to the main character attempting to combat the oppression of constant surveillance brought on by Big Brother. In the novel, the main character falls in love with a girl who is in the same predicament that he is, namely silently opposing the ideas of Big Brother. He goes so far as to rent a room above a shop that he is pretty sure is not monitored by Big Brother. He and the girl have meetings in that room during which their relationship grows stronger. At the end of the novel, the pair ends up being caught in that room, and sent off to have their behavior modified and be exterminated (Orwell, 1949). The idea of renting a room which is supposedly not monitored and going there to be able to think about opposing Big Brother is the main character's act of resisting surveillance. In the workplace, the employees do not have the ability to go somewhere during the day to think about going against the wants of the managers. They would only be able to do so after they have gone home at the end of the day. However, employees do have the ability to think thoughts without those being monitored, and they have other methods of dealing with their oppression. Unlike the "Thought Police" in 1984, the manager is not capable of reading the thoughts of the employees. Another method that is used by employees as a way to resist the surveillance is by sabotage (Vorvoreanu, 2000). By sabotaging the efforts of the employer to monitor their employees, the employees may dissuade the employer from any attempts of a continuation of monitoring. Also, the employee has the ability to slow down their own productivity in response to a possible power imbalance between the employer and employee (Vorvoreanu, 2000).

ETHICAL PERSPECTIVE

In contrast to the analysis of workplace surveillance based on a legal perspective (what is or is not legal), if we examine electronic monitoring from an ethical point of view, we have to determine whose needs, employer or employee, should be met in this situation. Instead of basing the outcome of the situation on the letter of the law, an outcome based on an ethical decision will be based on the social responsibilities of the involved parties. In order to make an ethical decision in either direction with regards to workplace monitoring, the employer must understand the needs of the employees and also know the limits to which he is able to monitor the employees. While the law is on the side of the employer, the employer must understand the implications of surveillance as employees feel them. For example, the Electronic Communications Privacy Act allows the employer to access e-mails sent by the employee because the operating system is owned by the employer, but the employees may feel as though the employer is invading their privacy (White, 1994). Since the e-mail communication is a potential liability for the employer, the management feels as though it is a business necessity to be able to read the e-mails that are being sent through the system. However, the employee may believe that e-mail is a private form of communication and the employer is encroaching upon their private space. In this situation, the employer does not understand how the employee can think that their e-mail is private, and the employee does not understand what legitimate interest the employer could have in their e-mail, except for simply invading their privacy. Even if the employer is not particularly monitoring the e-mail of their employees, the employee should be aware that any activities that they do through e-mail or on the Internet could be watched, due to the ability that other computer users have of looking for a particular user on the Internet and/or hacking into the computer system (White, 1994).

Ethical Risks of Monitoring Employees

The ethical risks to employers of monitoring their employees are based on the perception of third parties, i.e. other companies, stakeholders, and potential customers. If any of these parties,

which are integral to the ability of the employer to run a successful business, decide that they do not agree with the actions of the employer, they will have the ability to take their business elsewhere. The employer has to worry about how society views their actions because without the support of the rest of society, the employer will be lacking in profits.

Perceptions

The idea of perception is very important when looking at issues from an ethical point of view. Decisions made ethically are based on one of a few different perceptions, which are our own perception, the perception of others, or your own perception of rules by which everyone abides (Hartman). The choice that is made is based on only one of these perceptions. In a workplace situation, it is more than likely that the business decision is based on either the perception of other people in the society or the understanding of common rules of business. The perception of other people in the society is important to the business because the profitability of the business is based upon the amount of people willing to work with that company. If the company is seen as unethical in any way, shape, or form, consumers and other people in society will be less likely to deal with that company (Robin, 1989). A rule of thumb for companies to abide by when dealing with ethical dilemmas is “how you would feel if you saw what you did today all over the Internet tomorrow” (Hartman). If the company would be okay in knowing that everyone would know how they treated their employees, consumers, etc., then they will be making a decision regarding an ethical dilemma. With regards to electronic monitoring, the company must be careful in keeping with guidelines that are legally set out in order to prove to themselves that they are being ethical about the issue of surveillance. One way that companies should look at ethical rules of society is that they should treat their employees as they would like to be treated if the tables were turned. Unfortunately, most employers, even though they surely started out in the business world by working under someone else, do not treat their employees as they would like to have been treated when they were in the same predicament. This way of treating their employees is brought on by the amount of power

that the employer holds over the employee in the working relationship.

Societal Effects

There are several ways in which society affects the company's method of deciding ethical dilemmas. Some of these factors brought on by society are: the law, and persuasion to do what is right (Hartman). The legal issues which are laid upon the business regarding the employer's ability to monitor their employees electronically inhibit the employer from making absolutely sure that the employees are not giving away any information which may be important to the company, and that the employees are not going against the company in some way. In *Watkins v. L.M. Berry & Co.*, although the plaintiff was discussing a job interview with a potential employer, her current employer was not legally allowed to eavesdrop on the conversation because they did not have any legal interest in that information (1983). The company would claim that they have a right to know information that could affect their business, but the law states that they must not monitor a personal telephone call after they have determined that the call was in fact a personal, and not a business call. Although the company may claim that the business reasons for monitoring that phone call would make them ethically correct in that surveillance, the law does not allow the company to listen in on personal telephone calls (1983). The impression that society makes on the company is very influential with regards to business decisions. The thoughts and opinions of society often guide the ethical decisions made by businesses (Hartman).

Ethical Decision Making

Typically, businesses respond to ethical dilemmas in the easiest way possible rather than thinking the situation through in order to respond in the way that works best for everyone involved (Hartman). They will tend to follow the same procedures, without looking at the specifics of the problem, as they would for problems which would fall into the same category. Businesses do not try to go out of their way to find the best solution for both parties; instead, they only try to comply with the minimum standards necessary in all circumstances. It is fairly simple for most businesses to alter the process in which they make

decisions in order to create a more ethical decision-making process (Hartman). In order to decide on an ethical solution to a business dilemma, the manager must collect as much information regarding the situation as possible, ensuring consideration of all possible alternative solutions. The manager must then consider the interests of parties who have important relationships with the company, including employees, and other interested parties. The manager must also consider possible reasons for the behaviors of the included parties, and the results that certain solutions may have on the behaviors as a result of the underlying reason for the behavior of the included parties. The manager must decide on the process that they are going to take to resolve the dilemma, then evaluate their resolution based on outcomes, and alter the process to better it for the next time (Hartman). In ethical decision-making, it is sometimes more important to be aware of the implications of the decision for other involved parties than to arrive at the right decision. This works better than conventional decision-making because although conventional decision-making is practiced more often in the business world and other business entities would understand decisions made through this process, a right decision that is not made ethically may strain some important business relationships, i.e., the employee/employer relationship. For example, if an employer must downsize a certain department, basing his decision on a practice of letting the last person hired be the first person to be laid off, and the most recent hire is a very strong worker and an asset to the company, his decision to lay off the last person hired would be an example of conventional decision-making, and not of ethical decision-making (Hartman). If the employer used the ethical process of decision-making in this situation, then he might realize that his decision to let this excellent worker go based on the idea of seniority is not the smart thing to do for the sake of the company or the worker in question. The other workers may have been perturbed at the actions of the employer if he did not abide by the general process of seniority, but the employer does have a right to run his business in the best possible way to gain the results that he is hoping to attain out of this business venture (Hartman).

Ethics & Privacy Issues

Some issues in the area of business ethics have come to the surface due to the increased technology in the workplace in the past few years. One of these issues is the question of whether or not the employer has the right to know certain information about the employee simply because the employer has the technical ability to find out that information. Since there have been great technological advances in the workplace, and in society in the past few years, the employer has much personal information about his employees at his fingertips. With regards to privacy concerns in the workplace, the knowledge of the employees that the employer has access to personal information about them can seem like an invasion of privacy even if the employer has no intention of leaking that information or using it against the employee (Hartman). One of the most important aspects of the right to privacy is that of being able to keep "private information private". If the employer has knowledge of private information about his or her employees, then they will be committing an invasion of privacy against the employee simply by having the knowledge of that private information. An important ethical conflict in the workplace is between the right of the employer to manage their business and the right to privacy of the employee.

The employer and employee have two separate issues that will not ever be compatible with each other. The employer has a need to manage his or her own business. In the course of managing their own business, the employer must be able to manage the productivity of their workers, and they also have a right to be informed of the goings-on of their workers while they are at work (Hartman). In order to monitor the productivity of their employees, the employer is able to install software on the computers that may monitor the number of keystrokes made by the employee. While the employee may argue that this electronic monitoring diminishes the amount of privacy that they might enjoy at the workplace, it is important for the employer to be aware of how productive their employees are (Hartman). Also, it is important for the employer to monitor the employees' usage of e-mail and the Internet for reasons of liability, such as the possibility of copyright infringement on the behalf of the

employee. If the employee commits the crime of copyright infringement while they are logged on to the company's computer system and the company is aware of the crime, they are liable to the government because the crime was committed on their computer system. Meanwhile, the employee has the need to have their right to privacy met by the employer not monitoring their behavior so as to maintain the ideal of privacy. Since the ability of the employee to conduct personal business with other companies during the daytime is hampered by the fact that they have to be at work while the other businesses are open, and cannot always make it there after leaving work at night, the employer has to understand the need of the employee to take care of some personal business while they are at work (Hartman). This is an example of the need for some sort of privacy at the workplace for the employee. The ethical dilemma is one of employer rights versus employee rights, and must be decided upon specific circumstances for every situation.

CONCLUSION

The issue of workplace monitoring and its impact on employee privacy continues to be an extremely controversial issue that could be decided for or against either side, depending on the perspective through which the person deciding between right and wrong is looking. From the legal perspective, it would appear as though the employer has a greater need to monitor the employees than the employee's need to avoid potential invasions of privacy. Many of the laws regarding employee privacy favor the employer's right to monitor the employees, and therefore, the majority of courts tend to side with the employer when such cases arise in court (Colucci, 2002). Even though some courts will extend the 4th Amendment right to privacy to private employees, it legally only covers employees of the public government (Hubbart, 1998). Looking at workplace privacy through a legal perspective would seem to show that employers have every right to monitor their employees, and it would be in their best interest to do so.

In examining the issue of workplace monitoring through a behavioral perspective, we discover that there are some reasons why it would not be a good idea for the employer to monitor

their employees. Even if the monitoring of the workplace is not found to be an invasion of privacy by the courts, the employee still might react in response to their perceived violation of privacy. In this case, the employee may resist the intentions of the employer by either actively creating a hindrance, or by subtly rebelling against the efforts of the employer (Vorvoreanu, 2000). In either instance of employee reaction, the situation is less clearly defined than the situation viewed through a legal perspective because the employer, while needing the ability to monitor their employees, must also concern themselves with the reactions of the employees, and therefore, temper their efforts of monitoring in order to balance the needs of themselves with the needs of the employees.

Examining this issue through an ethical perspective, we find that the lines of right and wrong are even murkier than with the analysis of the behavioral aspect of workplace surveillance. There is no clear right and wrong when dealing with ethics, only socially acceptable or unacceptable solutions to ethical dilemmas (Hartman). The basis on which employers must make their decisions with regards to ethical dilemmas is which type of perspective is most important at that time: their own perspective, the perspective of others, or the perspective based on natural laws. The most important aspect of the decision regarding electronic monitoring which is examined through the ethical perspective is the balance between the employer's potential liability and the rights of the employee to have some semblance of privacy. Therefore, when we examine this issue through an ethical perspective, while we should not disregard the laws that have been created to deal with this issue, it is also important that we take the rights and feelings of the employee into consideration.

REFERENCES

- 1965. Fowler v. Southern Bell Telephone & Telegraph Company, *Federal Reporter, 2d Series*, Vol. 343: 150: United States Court of Appeals, Fifth Circuit.
- 1978. Simmons v. Southwestern Bell Telephone Company, *Federal Supplement*, Vol. 452: 392: United States District Court, Oklahoma.

- 1980a. Awbrey v. Great Atlantic & Pacific Tea Co., Inc., *Federal Supplement*, Vol. 505: 604: United States District Court, Georgia.
- 1980b. Briggs v. American Air Filter Co., Inc., *Federal Reporter, 2d Series*, Vol. 630: 414: United States Court of Appeals, Fifth Circuit.
1983. Watkins v. L.M. Berry & Co., *Federal Reporter, 2d Series*, Vol. 704: 577: United States Court of Appeals, Eleventh Circuit.
1994. Steve Jackson Games, Inc. v. U.S. Secret Service, *Federal Reporter, 3d Series*, Vol. 36: 457: United States Court of Appeals, Fifth Circuit.
- 1996a. Ali V. Douglas Cable Communications, *Federal Supplement*, Vol. 929: 1362: United States District Court, Kansas.
- 1996b. Bohach v. City of Reno, *Federal Supplement*, Vol. 932: 1232: United States District Court, Nevada.
2002. Konop v. Hawaiian Airlines, Inc., *Federal Reporter, 3d Series*, Vol. 302: 868: United States Court of Appeals, Ninth Circuit.
- Adams, H. I., Scheuing, Suzanne M., & Feeley, Stacey A. 2000. E-mail Monitoring in the Workplace: The Good, the Bad and the Ugly. *Defense Counsel Journal*, 67(1): 32-46.
- Bible, J. D., & McWhirter, Darien A. 1990. *Privacy in the Workplace: A Guide for Human Resource Managers*. New York: Quorum Books.
- Colucci, M. 2002. *The Impact of the Internet and New Technologies on the Workplace: A Legal Analysis from a Comparative Point of View*. New York: Kluwer Law International.
- Hartman, L. P. Technology and Ethics: Privacy in the Workplace.
- Hubbartt, W. S. 1998. *The New Battle Over Workplace Privacy*. New York: American Management Association.
- King, N. J. 2003. Electronic Monitoring to Promote National Security. *Employee Responsibilities and Rights Journal*, 15(3): 127-147.
- Lefton, L. A. 1997. *Psychology* (6th ed.). Boston: Allyn and Bacon.
- Lyon, D. 1994. *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis, MN: University of Minnesota Press.
- McKelway, J. M. J., & Karcis, E.P. Michael. Workplace Privacy in the Electronic Age: Where Should the Lines be Drawn? Boston: Gadsby Hannah LLP.
- Orwell, G. 1949. *1984*. New York: Signet.
- Place, J. M. 2000. Communications Technology in the Workplace. Kansas City, Missouri: American Bar Association.
- Robin, D. P. R., R. Eric. 1989. *Business Ethics: Where Profits Meet Value Systems*. Englewood Cliffs, New Jersey: Prentice Hall.
- Schnaitman, P. 1999. Building a Community through Workplace E-mail: The New Privacy Frontier. *Michigan Telecommunications and Technology Law Review*, 5: 177-216.
- Smith, A. D., & Faley, Robert A. 2001. E-mail Workplace Privacy Issues in an Information- and Knowledge-based Environment, *Southern Business Review*, Vol. Fall 2001: 8-22.
- Vorvoreanu, M., & Botan, Carl H. 2000. *Examining Electronic Surveillance in the Workplace: A Review of Theoretical Perspectives and Research Findings*. Paper presented at the Conference of the International Communication Association, Alcapulco, Mexico.
- White, V. A. 1994. *Ethical Implications of Privacy in Electronic Mail*. Paper presented at the Technical Conference on Telecommunications R&D in Massachusetts, University of Massachusetts, Lowell.

Wood, G. 2001. ***Monitoring Employee Use.***
Paper presented at the International Bar
Association Conference, Cancun, Mexico.