

Employee Surveillance: An Ethical Consideration

Michael Bassick, Tyler McNamara, Deborah Sullivan

Introduction

The expansion and proliferation of technology has dawned a new era, blurring the pre conceived boundaries, and surfacing new issues in which managers have no experience. The moral, legal, and social principles that once helped guide ethical decision making are no longer sufficient, resulting in a variety of practices which accelerate the emergence of ethical dilemmas. One such issue is employee surveillance. New methods of monitoring employees e-mail, internet use, and location are used by many companies in order to maximize worker productivity, ensure the integrity and character of the organization, and to protect the interests of third parties such as customers and fellow workers.¹

Employee surveillance presents an ethical dilemma because advancements in technology have opened up avenues to fast-growing markets, with little agreement on which practices are ethical and which are not.² The underlying theme for the use of these advanced technologies is the invasion of privacy. Privacy is defined as:

The condition of not having undocumented personal knowledge about one possessed by others...personal knowledge...consists of facts about a person which most individuals in a given society at a given time do not want widely known about themselves.³

In essence, employees feel that their actions inside and outside of work, as well as in their personal time, are their business only. When employers start to delve into one's personal life, animosity and distrust are built between the company and its workers.¹ While some policies may seem pertinent and beneficial, there is a fine line between what information employers should have access to and what should stay private. Since privacy is a very non-specific term, individual types of privacy will be discussed in further sections.

Employee Surveillance: Ethical or Unethical?

In the following sections, ethical and philosophical theories which support the limitation of employee surveillance, particularly access to e-mail, use of the World Wide Web, and employee tracking initiatives will be discussed. The goal is to analyze this ethical challenge, leaving any pre conceived notions behind to offer an unbiased way of ethical thinking. Much of the current surveillance is unethical, and with the advent of growing technological capability, a framework must be put into place to ensure employee rights are protected. Privacy is being invaded and it is important to confront the issue.

Employer's Rationale

To begin, privacy is a right that many people take for granted. Technology is challenging this right, and as further advancements are made, the availability of privacy will continue to dissolve. In order to fully develop the sentiment that much of employee surveillance is unethical, examples from both sides of the story must be considered. A survey conducted by two research firms, Dataquest and IDC, concluded that “approximately 22.8 million U.S. employees (40 percent of the internet-enabled work force) waste one or more hours on the internet each day”.⁴ Business people know that time is money and this time employees “wasted” on the internet costs US businesses approximately \$63 billion a year.⁴ Many employers feel they have the right to monitor employees because they are being paid to perform certain duties, and the amount of dollars wasted hurts the bottom line.²

Another consideration is that companies are the owners of the office equipment and therefore have the right to specify how those resources are used.² Accordingly, as owners of these business tools “if the company has reason to believe that an employee is using its resources inappropriately, or to its detriment, the company has a right and a obligation to protect itself”.² Under this premise, companies have free range to know what they want about who they want. Companies pay employees a lot of money and misusing office equipment is activity that the employer should not have to pay for.

Supporters of employee surveillance will also argue that employers have a right to see what their workers are doing throughout the day. Performance levels are much more attainable which allows for companies to work more efficiently. Many companies track key stroke accuracy, e-mail use, destination of phone calls, web site hits, and employee movement throughout the building to measure the productivity of individual employees.¹ These productivity

measurements help managers predict outputs, ensure quotas will be reached, and make sure that hardworking employees are not stuck picking up the slack for their lazy or incompetent coworkers³.

One final motivation for intruding on employee privacy is in the interest of protecting a third party.¹ This entity could be customers, shareholders, suppliers, creditors, neighbors to the workplace and others. Since corporations are liable for their employee's behavior such consideration seems justifiable. These arguments are valid and it is agreed that some level of surveillance is necessary to regulate business operations.

Employee Defense

The news is often flooded with cases of identity theft and other crimes that have been made much easier due to technological expansion. Employee surveillance has also increased and many employees are unaware that they are being monitored.¹ Although there is no legislation making unannounced surveillance illegal, many employees consider corporate surveillance measures to be unethical and an invasion of privacy.⁵

Further support for decreasing the amount of surveillance is that employees are being distracted and overly cautious about what is allowed and what is not.¹ In addition, "there is evidence that computer monitored employees suffer health, stress, and morale problems to a higher degree than other employees".³ Meanwhile, surveillance carries many costs associated with its implementation. The equipment needed, installation, upkeep, and monitoring proves to be very costly for many companies.³ While some see these purchases as money well spent, employee resentment could very well make such equipment the cause for lower company moral and confidence. Aside from not wanting their personal space invaded, employees value the trust they are given by their employer.³ As in all cases, after one's trust is lost it is very hard to regain. This recognized, Seumas Miller writes:

"There are other important things in life besides efficiency and profitability. In particular, there is the right to privacy. The existence of the right to privacy, and related rights such as confidentiality and autonomy, is sufficient to undermine extreme views such as the view that employees ought to be under surveillance every minute of the day."³

Skeptics argue that “the right to privacy cannot be overruled by the proposed responsibility argument”.¹ Since the information obtained can lead to investigations not pertaining to the motivations above, it could be realized that the surveillance measures are just an excuse to unfairly monitor an individual. To further develop the argument that employee surveillance is unethical, specific invasions of privacy and philosophical models will be addressed.

Types of Privacy

Privacy is a very general term and it is necessary to identify specific types in order to describe how employee surveillance violates the privacy of workers. First, solitude, or physical privacy is the state of privacy in which persons are free from unwanted intrusion or observation.⁶ Next, informational privacy is concerned with the protection of ones anonymity, especially when dealing with personal information. Also, psychological privacy, the control over release or retention of personal information, and interactional privacy which protects communication between individuals and group members are at risk when companies practice employee surveillance.⁶ Finally the last two types of privacy with which we are concerned are personal and body/mental privacy. Personal privacy is simply the right to be left alone and to do what one wishes during their free time.⁷ Body/mental privacy is the idea that we have a freedom of speech and we should not be subject to self incrimination.⁷

While not all forms of privacy are inherent and prescribed social liberties, many are intrinsic. According to the U.S. constitution’s first and fourth amendments, we as US citizens have the freedom of speech, and the freedom from unwarranted search and seizure⁷. While these amendments support nearly all the above mentioned forms of privacy, those which are not can be further supported by the ninth amendment which states that “there are other possible rights that people retain which certified that rights not specifically enumerated in the amendments did not preclude their existence”.⁷

Aside from the constitution, privacy rights can be supported through philosophical means. John Locke’s foundations carry that we as humans have natural rights including life, liberty, and property.⁷ As associated with employee privacy, this ethical framework grants workers the right to privacy concerning their e-mail and information which constitute as personal property.

Lastly, U.S. common law includes the inviolability of the home and the person, the sanctity of confidential communications, and the sacredness of personal information.⁷ Therefore, many of the ways employers monitor their employees violate these definitions and are unethical.

Philosophical Models

The Rights Approach

Determining what is ethical is extremely difficult because everyone has different beliefs, values, and feelings. The rights approach is one method that can help people understand what is ethical. This approach suggests that, “ethical action is the one that best protects and respects the moral rights of those affected”.⁸ According to this framework, employees have the right to make their own choices, to be told the truth, and to not have our freedom interfered with.⁸

Employee surveillance is unethical because it takes away many of the rights addressed within this theory. One right stripped away from employees through surveillance is the right to make you own choices. Companies purposely adopt e-mail monitoring, website screening, and GPS tracking technology to eliminate employee’s rights to choose what they want to do.⁸ Companies do have a need to protect their organizational interests, but forcing employees to act a certain way through surveillance is not the ethical way to control behavior.⁷ Instead of cameras and monitoring software, an employer following the rights approach should encourage correct behavior by stating what is expected of the employees and then giving them choice to act in a way they feel is right⁸.

Employers often tell employees when they are being monitored. What employers often do not tell employees is the extent of the surveillance taking place.² For example, it is common for a business to state they use e-mail surveillance software but not describe what is appropriate to include in an e-mail, whether or not they are consistently reviewing e-mails, and if they are storing the e-mails for future use. By withholding information, companies are violating the employee’s right to be told the truth.⁸ Any employer that purposely omits pertinent information is acting unethically. According to the rights approach, companies must not hide any information from an employee. If employee surveillance must be used, it is only right to let the worker know exactly what the company’s policy is on using monitoring technology.⁸

Possibly the most well known right is stated within the first amendment, the right to free speech. In America, the right to free speech is an important and defining right of the country. The U.S. prides itself on being one of a few countries that provides the freedom of speech of its citizens.¹ Employee surveillance limits this right. Almost every company restrains speech in some way or another inside the business. This isn't illegal, because the First Amendment doesn't apply to private sectors, but it is unethical because it denies employees of one America's most basic rights.² Computer monitoring software is designed to keep employees from conducting personal business at work but it is also meant to monitor what employees are saying online. Employers legally have the right to discipline those individuals that say something offensive over the internet.⁸ This power restrains employees from exercising free speech therefore making it unethical under the rights approach to ethics. Companies should respect employee's rights to free speech by not discouraging speech through employee surveillance.

The rights approach is one of the most popular methods in determining whether something is ethical or not. Employee surveillance takes away many employee rights, because the rights approach focuses on the protection of rights, it is safe to conclude that employee surveillance is unethical. Most companies focus on the bottom line, not what is ethical, which is why employee surveillance continues to grow.³ A change in focus from profit to the employee morale is an essential ingredient in creating an ethical organization.

Virtue Ethics

Another ethical theory which emphasizes the process of moral character development is virtue ethics. Within this framework, morality is not guided by rules or rights but instead by the concept of character.⁹ Character, which consists of honesty, fairness, compassion and generosity, drives members of an organization to concern themselves with what to be, as opposed to what to do.⁹ "Virtue based ethics seeks to produce excellent persons who both act well and serve as examples to inspire others".⁹ Actors, those making the ethical decisions, focus on whether rights are deserved as opposed to what the rule book implicitly states.¹⁰

Under this theory, privacy can be considered a right that employees deserve. Companies implementing this ethical guidance believe that workers know how to act and display themselves with great character. Therefore, surveillance is unnecessary because employees' behavior and decisions will be consistent with the actions of a "good" person¹⁰.

Unethical Surveillance

When looking at the different surveillance capabilities most recently made possible through new technologies, there are some that seem more controversial than others. E-mail surveillance, internet monitoring, and employee tracking are among the most prevalent. Also, the lack of employee knowledge on how they are being monitored is unfair and must stop. Each of these will be discussed in detail and we will show how much of the behavior implemented by many companies is unethical.

E-mail Surveillance: Violations of Informational and Interactional Privacy

The use of electronic mail messages is one of the most common avenues of communication in today's business world.¹¹ Employers are motivated to screen employee e-mail in order to protect company assets and to ensure high levels of productivity.¹² Also, since employers are responsible for their employee's conduct, they feel the need to protect their own interests and the interests of all stakeholders.¹² In addition, there are few states that have laws regarding e-mail surveillance in the private sector. This gives employees the freedom to intercept e-mails at will. It is difficult to support employee rights to privacy since it is often found in court that even though workers have a "reasonable expectation of privacy", such expectations are invalid when "communications are sent over the company-controlled e-mail system".¹² It is important to realize that just because something is legal, it is not necessarily ethical. Regardless of reasonable expectation, employees still feel that they should have the right to communicate without interference. Informational privacy is continuously being breached and information which is considered to be private is no longer such. In addition, interactional privacy is invaded since one's employer can read private messages intended for individual persons. E-mail surveillance is an unnecessary practice which protects only the interest of the company and their bottom line without considering employee wants and needs.

Since privacy seems of little significance in the eye of employers, the virtue ethics approach can be used to provide a model for employee treatment and behavior. A company implementing this framework would rely on employees to conduct themselves in an ethical manner. Based on character development, virtue ethics gives employees the freedom to make their own decisions with the faith that their choices will represent those made by a "good"

person. Giving employees the ability to make their own decisions may seem risky from management's point of view, but evidence suggests that this increased responsibility has increased morale and improved employer-employee relationships. In fact, employees subject to surveillance have exhibited feelings of decreased employer trust, increased stress, and subsequently decreased productivity.¹²

Since it is clear that e-mail surveillance has serious downfalls, relying on the character of employees seems to improve productivity and instill confidence. To ensure that the virtue ethics approach is successful, companies can help employee ethical reasoning by holding workshops which encourage socially beneficial decision making. By coaching workers to make ethical decisions, rather than guiding behavior by rules, both the employees and employer will likely enjoy more favorable results. E-mail surveillance is an invasion of privacy and therefore unethical. If virtue ethics were used to encourage employee decision making, no surveillance would be necessary and privacy would be ensured.

An example of unethical e-mail surveillance can be seen by Dow Chemical. This company, a well known multinational chemicals producer took a snap shot of employee internet activity during a given day.¹³ Their findings were both alarming and discouraging. Over the course of this day 254 employees had sent or received inappropriate e-mail messages consisting of pornographic material, violent, and discriminatory content.¹³ While such findings would seem to support extensive surveillance, it is important to note that these employees did not know they were being observed. This introduces the argument that it is unethical to monitor employee behavior without their knowledge. Such employee activity should be condemned, however it is likely this activity wouldn't have taken place had employees known they were being monitored. As a result, Dow created a criterion for punishment which took into consideration the extent of an employee's participation, the offensiveness of the material, and what the employee did with the material. In the end Dow terminated 20 employees and disciplined others.¹³ Dow invaded the privacy of its employees by limiting their rights to physical, interactional, and body/mental privacy. Employees were observed unwillingly, private conversations were acquired, and emails were used as self incriminating evidence. In addition, Dow managers behaved unethically under the rights approach since they lied to their employees.⁸ While they didn't implicitly lie to their employees about monitoring activity, withholding the truth is still considered a lie. As a result, 20 employees were unjustifiably fired. Finally, their behavior may have permitted such action,

the employees were treated unethically since Dow's methods were deceitful and without regard for workers' privacy.

Monitoring Employee Internet Use: The Rights Approach

Website surveillance has increased exponentially over the past ten years. In a 2005 survey by the American Management Association, over three quarters of major U.S. firms monitored website connections, more than tripling the 1997 numbers.⁵ A main reason for this increase is a combination of advancements in website monitoring software and the drastic boost in the amount of employees that use computers at work. As of January 2002, nearly 55 million US adults accessed the internet at work, an increase of nearly 27% from the previous two years.³ This increase of internet accessibility naturally led to a large amount of time and money wasted on the internet by employees.

The misuse of the internet has posed a huge problem to most businesses. A seemingly easy way for a business to combat the problem is to just not allow employees to use the internet for anything other than work. The most common way for employers to do that is through the use of website monitoring software. 76% of major U.S. companies monitor website connections and over 65% of companies use software to block employees from connecting to inappropriate sites.⁵ The rise of computer monitoring popularity has led to a huge market for computer monitoring software.² Of these programs, one of the most popular named Investigator, has sold over 200,000 copies.¹⁴ Investigator is able to block websites, along with the capability to monitor every keystroke an employee makes, take a record of every dialogue box, and can even periodically take a snap shot of exactly what an employee is looking at on their computer screen.¹⁴ The number of ways these programs can monitor an employee is astonishing and now that the monitoring software product market is maturing, it is possible for any company to cheaply and easily use software to monitor their employees.

The ease of access and affordability of such programs overshadows the fact that the implementation of such surveillance is an unethical invasion of privacy. The rights approach grants employees certain unalienable rights including the right to freedom and privacy.⁸ Monitoring employee's internet use invades both physical and personal privacy. Regardless of location or ownership of equipment, employees still possess these rights and by being placed under such extreme scrutiny, they are being treated in an unethical manner. Part of the rights

approach identifies the employee's right to be told the truth.⁸ Most companies that implement internet surveillance do not notify employees what sites are permitted and which are not. While many of the unauthorized sites are self explanatory, unwarranted investigations can result from employees unknowingly visiting disallowed web pages. Further investigations can lead to additional infringements on employee privacy and unreasonable punishments could follow. Employees cannot be left ambiguous and companies who monitor internet use should provide workers with a white and black list, consisting of allowed and restricted web pages.¹¹ This will help limit the invasions of privacy but still will not make web site surveillance ethical. Once again virtue ethics can be implemented to encourage ethical employee behavior. Given this responsibility, it is likely employees will feel badly about defying the trust they have been given, and will act more accordingly.¹

A positive approach, like that used by Saratoga Systems in California, is to implement a more lenient surveillance which takes into consideration the needs of its employees. The company tries to accommodate its employees by permitting them reasonable use of company e-mail and internet use.⁹ Employees know they are being monitored, but they also know the company respects their occasional need to take care of personal business from the workplace. The company realizes that if employees needed to leave the office to take care of errands, more time would be lost in a day. If they can take care of some errands while at the office, it is more convenient for the employee, and they can quickly get back to work. A sense of trust is built between the employer and employee and motivates them both personally and professionally.²

This policy closely follows the virtue ethics guidelines. Saratoga Systems gives their employees a level of independence trusting that their actions will uphold the character of the company and that they will behave in an ethical manner.⁹ This example shows how virtue ethics can be successfully implemented. If more companies were to have faith in their employee's ethical reasoning, it is likely that they would be able to implement a system similar to that of Saratoga Systems.

Tracking Employees: Crossing the Line of Privacy

The collection of personal information through highly portable means is becoming increasingly popular throughout numerous governments and businesses.¹⁵ Examples of these tracking devices are radio frequency identification tags (RFID), smart cards, and identification

cards.⁷ Instances in which such instruments are used can be to track the movement of employees during work. This sort of monitoring can let the employer know how much of the time the employee spends at their desk, in the bathroom, or in the break room.¹⁵ While this information would seem to be very helpful to employers it is unethical because it invades physical and personal privacy of employees.⁷ The activity is unwarranted observation, and goes against the workers right to privacy during their free time. Even though they are at work, employees receive breaks throughout their day and it is only in their interest how they spend these breaks. Employers do not need to know when employees use the bathroom or grab a cup of coffee. If it is the productivity employers are concerned about, simply reviewing employee output would be enough. If an employee is reaching their quota and completing all assigned tasks, there is no need to see where they go throughout the day. On the other hand, if a select employee is not completing their portion of the work, performance measures will unveil disparities in the timeliness and quality of this individual's efforts compared with that of higher performers. With these standards in place, poorly performing employees can be confronted and the problem can be resolved or the employee can be let go. This can all be done without tracking employee location.

An additional instance where employee tracking presents an ethical dilemma is through the use of smart cards in employee cell phones. This technology allows the location of the employee to be known at all times. Such technologies are used primarily by delivery services and professions where driving is a major part of the job.¹⁵ In such cases, employee location is useful for organizing a workforce outside the office. Benefits include increasing the efficiency of operations by diverting employees to sites dependent on their current location, and assisting drivers with finding the shortest route between two points in order to avoid high traffic areas.¹⁵ While these uses create a greater efficiency, they are unethical because they violate employee rights to privacy. Physical privacy, interactional privacy, and personal privacy are all being intruded by such tracking surveillance.⁷ Since it is likely that employees will have their phones in their possession during off-the-clock hours, it can be identified where the employee spends his/her free time and who he/she spends it with. While such information seems futile, assumptions can be made about workers by their employers which can affect their reputation at work and possibly jeopardize their job.¹⁵ Whether the employee should be acting in this manner or not is none of the business of his/her employer. They are no longer representing the company therefore their actions affect themselves not their employer.

Secretly Monitoring Employees: Lies, Lies, Lies

It's only natural that employees use some of their work day to conduct personal business. What most individuals fail to think about is whether everything they do is private. Many would be surprised to know their employer is aware of every keystroke, every e-mail, every phone call, and more.¹ Equipment that belongs to a company can store e-mail that employees have deleted thinking they are protecting themselves.² The number of personal tasks that an individual can do over the internet is a great temptation to be distracted from a person's job. While the majority of companies inform their employees they are being monitored, the majority would prefer not to tell them.³ Every piece of information an employer is able to collect can be evidence that could cost an employee their job.

According to the American Management Association (AMA) and the ePolicy Institute, who regularly survey companies about their monitoring and surveillance activities, about 80% of companies surveyed notified their employees they were being watched.¹⁶ Of those who inform their employees about the monitoring, many aren't specific about the type of monitoring they are conducting. Employers often increase their surveillance programs without explanation, assuming the employee understands that the company policy manual reserves their right to monitor.¹⁶ Beth Givens, executive director of the Privacy Rights Clearinghouse, urges employees to pay attention to their employers' policies. "Employers should notify employees that they are being monitored, what type of monitoring is being done, and how data from monitoring will be used".¹⁷ Unfortunately this is not always the case.

Unless they are the subject of some workplace controversy, most individuals are unaware of how invasive employer monitoring is.¹ As this rapidly growing process is becoming a part of the way companies do business, individuals are quickly losing control of personal information they would prefer to keep private. Employers using software programs for monitoring argue that there reasons are justified. Whether it's a matter of protecting the company from security breaches, defending the risk of legal liabilities, or wanting to increase employee productivity, companies feel they have the authority to know everything they can possibly find out about each employee.³ Although various kinds of software provide the opportunity to acquire extensive amounts of information about an individual, the relevance of that information to the day to day operations of the business is inconsequential. Because there is little to no regulation or

legislation that prohibits employers from gathering information, they often feel empowered to collect as much information as they can gather.¹² Without the knowledge of what information is being acquired it is hard for an employee to realize how much their privacy is being invaded.

It is one thing for employee surveillance to occur when workers are aware of their company's practices, but for employees to be unknowingly watched is absurd and unjust. As mentioned before, the rights approach states that employees have the right to the truth. Companies that monitor employee behavior without notification are lying and therefore acting unethically. Also, body/mental privacy is being assaulted. The idea that we have a freedom of speech and we should not be subject to self incrimination is clearly not respected.⁸ Employees who do not know what behavior is allowed could very easily make a mistake and harmfully incriminate themselves or friends within the organization. Also, a company has a moral responsibility to notify employees of changes in their policy. Policy changes in all other facets of business are made clear so that employees will adhere by their instructions. When left ambiguous, employee's rights are being violated and they are treated unethically.⁹

Conclusion

Technology is an amazing phenomenon. Never before has the human race been so dependent on instruments and gadgets to get through their everyday life. There is no doubt that these advancements have increased the standard of living and made many of our everyday activities far more convenient. With this convenience has come a greater threat of privacy invasion. Simply because a new technology has increased our potential, does not make these new abilities ethical. As citizens of the United States, whether stated by law or a common ethical framework, deserve the right to keep certain things private. There is currently a vague line that distinguishes what is and is not considered private material, information, or knowledge. In order to give all citizens equal rights these definitions must be more clearly stated and understood by all. The ambiguity that currently exists between employer surveillance programs and employee knowledge of such monitoring must be eliminated. More than anything it is important that people know what activity is being watched and what is not. As our abilities increase, our moral and ethical thinking must accompany this growth. We must have a sense of responsibility to maintain two of the greatest natural rights that we possess; privacy and autonomy.

Works Cited

- [1] A. Persson, " Privacy at Work- Ethical Criteria," Journal of Business Ethics, vol. 42, pp. 59-70, 2003.
- [2] K. Loch, "Ownership, Privacy and Monitoring in the Workplace," Journal of Business Ethics, vol. 17, pp.653-663, 1998.
- [3] S. Miller, " Privacy, the Workplace and the Internet ," Journal of Business Ethics, vol. 28, pp. 255-265, 2000.
- [4] D. Elmuti, " Not Worth the Bad Will," Industrial Management, pp. 27-30, 2006.
- [5] American Management Association, " 2005 Electronic Monitoring and Surveillance Survey," New York: 2005.
- [6] H. Chao, "Privacy Issues in Internet Surveys," Social Science Computer Review, vol. 7, pp. 421, 1999.
- [7] A. Peslak, "An Ethical Exploration of Privacy and Radio Frequency Identification," Journal of Business Ethics, vol. 59, pp. 327-345, 2005.
- [8] M. Valesquez, " A Framework for Thinking Ethically," Issues in Ethics, vol. 1, no. 2, 1998.
- [9] D. Knights, " Leadership, Ethics and the Responsibility to the Other," Journal of Business Ethics, vol. 67, pp. 125-137, 2006.
- [10] J. Everett, "The Global Fight Against Corruption: a Foucaultian, Virtues-Ethics Framing," Journal of Business Ethics, vol. 65, pp.1-12, 2006.
- [11] G. Nord,, " E-Monitoring in the Workplace: Privacy, Legislation, and Surveillance Software," Communications of the ACM, vol. 49, no. 8, 2006.
- [12] B. Friedman, "Workplace Privacy: Employee Relations and Legal Implications of Monitoring Employee E-mail Use," Employee Response Right Journal, 2007.
- [13] C. Dupree Jr., " Who's Reading Your Office E-mail? Is That Legal?," Strategic Finance, April 2006.
- [14] F. Lane, The Naked Employee: How Technology is Comprimpising Workplace Privacy, New York: AMACON, 2003.
- [15] A. Joinson and Carina Paine, "Watching Me Watching You: Privacy Attitudes and Reaction to Identity Card Implementation Scenarios in the UK," Journal of Informational Science, vol. 32, pp. 334, 2006.
- [16] N. Flynn, " 2005 Electronic Monitoring & Surveillance Survey,"[Online Document] May 8 2005 [2006 Mar 11], Available at FTP: [www. AMANet.org](http://www.AMANet.org).
- [17] A. Crane, " Workplace Privacy? Forget It!," [Online Document] Jul. 18 2005 [2006 Mar 11], Available at FTP: www.Bankrate.com.