Employee Monitoring and Ethics:
Can They Co-Exist?

Angelina I. T. Kiser, University of the Incarnate Word, USA

Timothy Porter, University of the Incarnate Word, USA

David Vequist, University of the Incarnate Word, USA

ABSTRACT

More advanced technologies that make it possible to monitor employees in the workplace have led to controversies on both legal and ethical grounds. Employers can now easily monitor emails, Internet usage and sites visited, and keystrokes, as well as use GPS systems to track employees' movements throughout the day. At one end of the spectrum is the employer who claims that monitoring not only improves productivity but is a legal necessity that assists in keeping the company from becoming legally liable for employees' misuse of technology. Employees, on the other hand, want their privacy protected, and many believe that it is more a matter of them not being trusted. In this paper, an examination is presented that describes various forms of workplace surveillance and monitoring, viewpoints of both employers and employees, policies that companies have implemented, and the ethical and legal implications of such policies.

Keywords: *Electronic Monitoring, Information Ethics, Information Security and Privacy, Information Trust, IT Policy and Standardization*

INTRODUCTION

Employee monitoring has always occurred in business as supervisors oversaw the activities of their employees. Employees were, and are still, subjected to such measures as random bag checks to ensure that no company property was being stolen, punching time clocks to ensure the employee is at work at the specified times, and secured entrances that only allow certain employees to access restricted areas. Eventually, employee monitoring moved to employers recording phone conversations between customers and employees or using video surveillance to stay abreast of employee productivity and activities. Today, with the emergence of the Internet and other digital technologies, employers now have numerous options with which to monitor their employees – not just what they do, but when and where they do it. Computer software used by companies is being utilized to record computer key strokes, monitor websites visited, and even "spy" on employees in real-time (Turri, Maniam, & Hynes, 2008). According to the American Management Association (2007), 45% of employers track Internet content, keystrokes, and time spent on the keyboard, 43% store and review computer files, 12% monitor the blogosphere, and 10% monitor social networking sites.

DOI: 10.4018/jdldc.2010100104

Electronic monitoring has brought with it a barrage of controversies as employers insist that it is necessary and employees claim that it is an invasion of their privacy. According to Wakefield (2004), employers use monitoring and surveillance of their employees to: 1) protect the rights of employees, 2) create a safe work environment, 3) protect sensitive corporate information and assets, and 4) comply with federal laws. Corporations and other organizations gather and store sensitive information, and they are required to safeguard that information. Employee surveillance is simply one more safeguard to ensure that the information is secure. Employers also cite improved productivity as a reason for making use of employee monitoring and surveillance. Snapshotspy.com reported that 50% of employees use the Internet for personal use during a normal workday, which negatively affects productivity, customer service, network resources, and may even render a company vulnerable to legal liability (Young, 2010).

On the other end of the spectrum are the employees who feel that their privacy is being invaded and that their employers simply do not trust them or want to monitor every minute of their workday. Some employees have challenged the legal aspects of employee monitoring based on the concept of invasion of privacy (Hornung, 2005). Employers should be conscious of the employees' desire for some privacy and attempt to avoid unnecessary intrusions that lead to a proliferation of monitoring and surveillance (Nord, McCubbins, & Nord, 2006).

EMPLOYEE CONCERNS

People have an expectation of privacy, and they value that privacy in their personal lives. However, how much privacy should a person expect to have within the employment context? How invasive should an organization be in monitoring its employees? It appears that technology has outpaced the once traditional expectations of privacy. In the past, employees saw the manager watching them, or they were well aware of video and phone surveillance. Today, employees are "watched" through their use of their work computers via email and Internet usage. Companies can monitor what employees are doing during the entire workday with at least 40 million U.S. workers being subject to electronic monitoring (Alder & Ambrose, 2005).

In a study conducted by Hoffman, Hartman, and Rowe (2003), they cite several reasons for limiting employee monitoring:

- Monitoring may create a suspicious and hostile work environment.
- The lack of privacy may constrain work flow.
- It may be important for employees to conduct some personal business from the workplace.
- Workplace stress and press are increased.
- Freedom of expression and autonomy are hindered.
- Monitoring is intrusive upon one's right to privacy of thought.

Should workers feel excessively stressed in the workplace because of a negative work environment, productivity may actually decrease (Everett, Wong, & Paynter, 2004), which would counteract one of the purposes of employee monitoring. High levels of negative stress in employees can then lead to indirect costs to an organization, such as low morale, dissatisfaction, breakdowns in communication, and disruption of working relationships (Nelson & Quick, 2009). Therefore, it is important for employers to effectively communicate the reasons for electronic monitoring and find a balance between the need for the monitoring and the privacy of the employees.

EMPLOYER CONCERNS

Employers monitor their employees for a multitude of reasons, including: 1) minimize security risks, 2) ensure stable productivity, 3) protect stakeholder interests, 4) protect against potential liability, 5) ensure legislative compliance,