Chapter 8
Monitoring Employee Actions in the Workplace:
Good Business Practice or Unethical Behaviour?

Cliona McParland
Dublin City University, Ireland

Regina Connolly
Dublin City University, Ireland

ABSTRACT

While the use of Internet based technologies empower organisations immensely, the recent surge of pervasive technologies into the workplace environment has created situations whereby employees are becoming increasingly aware of the ways in which management can employ these technologies to monitor their email and computer interactions. Although it is apparent that in some cases management may have legitimate reasons to monitor employees' actions it is becoming increasingly evident that emerging issues and subsequent privacy concerns resulting from the use of these technologies have the potential to negatively impact organisational productivity and employee morale. This chapter outlines some of the major issues relating to workplace surveillance, identifying the emerging issues and subsequent privacy concerns from the employee's perspective, as well as the motivation behind managements' decision to employ monitoring technologies in the workplace.

INTRODUCTION

While the exponential growth of Internet-based technologies has empowered organisations immensely, the recent surge of pervasive technologies into the workplace environment has generated privacy concerns amongst employees. The pervasive computing environment is characterised by the seamless integration of technologies into society, and it is this transparent nature which has fuelled much of these privacy concerns. For example, employees are becoming increasingly aware of the ways in which management can employ such technologies to monitor their email and computer interactions in the workplace. Profit driven organisations however, aim to manage their

DOI: 10.4018/978-1-60960-573-5.ch008

business in an efficient and productive manner. As such, it is perhaps unrealistic to expect that such organisations would not avail themselves with the obvious empowering benefits that these communication monitoring technologies afford them. Furthermore, it can be argued that they may in fact have legitimate reasons to monitor employee actions in the first place.

Many questions surround the issue of workplace surveillance, in particular, relating to the ethical nature of managements ability to monitor employees computer interactions. The aim of this chapter therefore, is to outline some of the major issues relating to workplace surveillance, identifying the emerging issues and subsequent privacy concerns from the employee's perspective, as well as the motivation behind managements' decision to employ monitoring technologies in the workplace. As such, this chapter explores the ethical impact of monitoring in the computer-mediated work environment, addressing whether management's ability to monitor employee actions in the workplace represents good business practice or constitutes an invasion of privacy.

BACKGROUND

It is a common belief that one of the greatest threats to personal privacy lies in the monitoring and surveillance capabilities of modern technology. Privacy is a complex construct that remains beset by conceptual and operational confusion. It is an ambiguous concept that for many is difficult to either define or understand. For example, for every definition of privacy sourced from the literature, a counterexample can be easily produced (Introna, 1996). Understandably therefore, privacy is often defined and measured in terms of a specific study, event or situation and as a result, the conceptual confusion that surrounds the construct as well as the ways in which best to manage it remains a hot discussion topic. In order to gain a full understanding of the privacy construct, it is reasonable to suggest that one considers it from a multiplicity of viewpoints and as such, privacy is often examined as a psychological state, a form of power, an inherent right or an aspect of freedom (Parker, 1974; Acquisti, 2002; Rust *et al.,* 2002)

One aspect of privacy which for many is central to our understanding of the construct is the issue of control, specifically the individual's need to have control over their personal information. Control has been defined as "*the power of directing command, the power of restraining*" (Oxford, 1996: 291) and is consistently proposed in the literature as a key factor in relation to understanding individual privacy concerns. Personal control is important as it relates to the interest of individuals to control or significantly influence the handling of personal data (Clarke, 1988). Practitioner reports confirm the importance that individuals attribute to being able to control their personal information, particularly in relation to the use of Internet-based systems. For example, a 1999 Louis Harris poll indicated that 70% of online users felt uncomfortable disclosing personal information while a 2003 Harris poll of 1010 adults also found that 69% of those surveyed described their ability to control the collection of personal information as being 'exceptionally important'. Statistics like these indicate the increasing concern of individuals regarding the violation of their privacy and their desire to be able to control their personal information.

Interestingly, while individuals' sensitivity to control of private information is an issue of increasing concern, the truth regarding the extent of control over that personal information is often misunderstood, particularly amongst the Internet-using public. This is confirmed by a 2005 study by the Annenberg Public Policy Centre which discovered that 47% of the 1500 adults surveyed falsely believed they were able to control personal information distributed about them online simply because they had the right to view data collated by the on-line vendor, while a further 50% falsely believed they could control the depth of informa-