Chapter 4
Dataveillance in the Workplace:
Privacy Threat or Market Imperative?

Regina Connolly
Dublin City University, Ireland

ABSTRACT

The work environment is changing in response to market pressures, and the psychological contract that previously typified many employer and employee work relationships is coming under distinct threat as pervasive Internet-based technologies now enable management to monitor employees' email, computer interactions, and general work productivity. Although in some cases management may have legitimate reasons to monitor employees' actions, it is becoming increasingly evident that the use of these technologies has the potential to negatively impact employee productivity and morale, and in some cases employee health and wellbeing. This chapter outlines some of the emerging issues relating to workplace surveillance from the employees' perspective, as well as the motivation behind management's decision to employ technologies in order monitor their employees.

INTRODUCTION

The changing contours of global economics and shifting market pressures have resulted in a work environment that is now characterised by less job security, stagnant wages and where the nature of work has become more intense and ideosyncratic. Many employers feel that they must satisfy a market imperative that is constantly pushing for greater productivity, if their organisations are to remain competitive. Attempts to satisfy that imperative have resulted in a relentless drive for efficiency and a focus on rigorous performance quotas, which in turn have become key determinants of both employment and promotion.

Recent technological advancements have facilitated the achievement of those efficencies and in particular have enabled employers to gain more detailed insights into employee performance, including their own use of technology both during and after work hours. However, this has generated understandable privacy concerns for 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, measure

their performance and even monitor their social media activity. That workplace surveillance, or dataveillance, can negatively impact employee productivity and motivation as well as their trust in employers and consequent commitment to the organisation.

A SHIFTING CONTEXT

As profit driven organisations strive to manage their business in an efficient and productive manner, it is perhaps unrealistic to expect that such organisations would not avail of the obvious empowering benefits that 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. However, an inevitable outcome of these changes is that employees' relationship with their employers is changing in line with the changing balance of power in the workplace.

For an employee, knowing that their performance is being monitored and that that information may against them as part of performance assessment or promotion evaluation exercises, changes their perspective of the parameters of the employment relationship. Employee-employer relationships are typically perceived as being a two-way exchange, with the focus squarely upon the perceptions of reciprocal promises and obligations of both parties (Guest, 2004). These perceived obligations form a psychological contract that has been described as an individual employees' "belief in mutual obligations between that person and another party such as an employer" (Rousseau and Tijoriwala, 1998: 679). In short, employees have implicit and sometimes unvoiced expectations regarding employee contributions, in terms of effort, loyalty and ability for organizational inducements such as pay, promotion and job security (Morrison and Robinson, 1997; Conway and Briner, 2002).

However, the monitoring of performance presents a threat to that previously accepted contract and indeed can be perceived as a breach of expectations by the employer, which in turn can lead to feelings of injustice or betrayal of employees (Morrison and Robinson, 1997). Employees' reactions to contract violation have been shown to effect their organizational commitment (Lemire and Rouillard, 2005), work satisfaction (Sutton and Griffin, 2003), job security (Kramer *et al*. 2005) and motivation (Lester *et al*. 2001), as well as increasing their stress levels (Gakovic and Tetrick, 2003). Trust and fairness are core aspects of any psychological contract (Guest 2004) and workplace surveillance presents a considerable threat to the previously perceived trustworthiness and fairness of employers who now have the potential to leverage performance information against employees.

Many questions surround the issue of workplace surveillance in particular relating to the ethical nature of management's 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 workplace represents good business practice or constitutes an invasion of privacy.

PRIVACY AND SURVEILLANCE

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

Related Content

A Firegroup Mechanism to Provide Intrusion Detection and Prevention System Against DDos Attack in Collaborative Clustered Networks

M. Poongodiand S. Bose (2014). *International Journal of Information Security and Privacy (pp. 1-18).*

www.irma-international.org/article/a-firegroup-mechanism-to-provide-intrusion-detection-and-prevention-system-against-ddos-attack-in-collaborative-clustered-networks/130652

VCGERG: Vulnerability Classification With Graph Embedding Algorithm on Vulnerability Report Graphs

Yashu Liu, Xiaoyi Zhao, Xiaohua Qiuand Han-Bing Yan (2024). *International Journal of Information Security and Privacy (pp. 1-21).*

www.irma-international.org/article/vcgerg/342596

Three Models to Measure Information Security Compliance

Wasim A. Al-Hamdani (2009). *International Journal of Information Security and Privacy (pp. 43-67).*

www.irma-international.org/article/three-models-measure-information-security/40360

Better Securing an Infrastructure for Telework

Loreen Marie Butcher-Powell (2008). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications (pp. 2044-2058).*

www.irma-international.org/chapter/better-securing-infrastructure-telework/23207

Ransomware: A New Cyber Hijacking Threat to Enterprises

Xin Luoand Qinyu Liao (2009). *Handbook of Research on Information Security and Assurance (pp. 1-6).*

www.irma-international.org/chapter/ransomware-new-cyber-hijacking-threat/20635