Dataveillance: Employee Monitoring & Information Privacy Concerns in the Workplace

Regina Connolly, Dublin City University, Ireland
Cliona McParland, Dublin City University, Ireland

ABSTRACT
Information privacy concerns are a dominant concern of the information age. Such concerns emanate from the tension between the correct use of personal information and information privacy. That tension has extended to the computer-mediated work environment as employees are becoming increasingly aware of the ways in which management can employ technologies to monitor their email and Internet interactions. Such information privacy concerns have the potential to negatively impact organisational productivity and employee morale. The aim of this paper is to outline some of the major issues relating to workplace surveillance and provide a balanced perspective that identifies the emerging issues and subsequent privacy concerns from the employee’s perspective as well as the rationale underlying managers’ decision to employ monitoring technologies in the workplace. In doing so, it attempts to progress academic understanding of this issue and enhance practitioners’ understanding of the factors that influence employees’ technology-related privacy concerns.

Keywords: Computer-Mediated Surveillance, Dataveillance, Information Privacy, Monitoring, Pervasive Computing, Workplace Surveillance

INTRODUCTION
Information privacy is an issue of increasing concern to many stakeholders, including consumers, employers, privacy activists, researchers and policy makers. To a great extent, these concerns relate directly to the exponential growth of Internet-based technologies. Whilst the benefits bestowed by such technologies is undisputed, it is an undeniable fact that they have generated considerable concern regarding the way in which they can be used to collate and use information on individuals without their prior permission. For example, 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 that has fuelled many of these privacy concerns with employees becoming increasingly aware of the ways in which management can employ such technologies to monitor their email and computer interactions in the workplace. However, as profit-driven organisations aim 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 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.

A number of questions surround the issue of workplace surveillance in particular those relating to the ethical nature of management’s ability to monitor employees’ computer interactions. The aim of this paper therefore is to outline some of the major issues relating to workplace surveillance, to identify the emerging issues and subsequent privacy concerns from the employee’s perspective, as well as the motivation behind management’s decision to employ monitoring technologies in the workplace. As such, this paper 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.

INFORMATION PRIVACY

Privacy is a complex construct and one that remains beset by conceptual and operational confusion. It is an ambiguous concept in the sense that it is difficult to either define or understand. For example, for every definition of privacy sourced from the literature, a counter example can be easily produced (Introna, 1996). Thus, Solove (2006, p. 477) asserts that privacy as a concept is in disarray and nobody can articulate what it means. This conceptual confusion has been exacerbated by the multiplicity of perspectives that have been applied to examinations of the construct, resulting in a highly fragmented set of concepts, definitions and relationships. For example, 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, Kannan, & Peng, 2002). Many overlapping concepts such as confidentiality, anonymity, secrecy and ethics have added to the confusion that surrounds the construct (Margulis, 2003). In an attempt to reduce this confusion, Clarke (1999) identifies four dimensions of privacy: privacy of a person, personal behaviour privacy, personal communication privacy, and personal data privacy. However, as the majority of communications today are digitised and stored, Bélanger and Crossler (2011) contend that personal communication privacy and data privacy can be merged into the construct of information privacy.

The distinction between information privacy as opposed to physical privacy is easily identifiable. The latter concerns physical access to an individual and the individual’s surroundings and private space, whilst the former concerns access to individually identifiable personal information (Smith, Dinev, & Xu, 2011). In terms of historical development, attention was initially paid to the concept of physical privacy, but more recently with the increasing pervasiveness of communication technologies, the concept of information privacy has acquired greater significance. As far back as 1986, Mason predicted that four major concerns would result from the increased use of information and communication technologies — privacy, accuracy, property and accessibility. This prediction has proved to be correct and particularly so in relation to concerns regarding information privacy. Examinations of information privacy are based on the assumption that the ultimate target of review is information as opposed to physical privacy. Because information privacy is part of general privacy research, many of the early privacy concepts have been applied to information privacy, although it is also true that information-specific privacy concepts exist. For example, Smith, Milberg, and Burke (1996) propose four dimensions of information privacy: collection, unauthorized secondary use, improper access, and errors.

Central to our understanding of the privacy 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
Related Content

Exploring the Impact of Team based Reward on Project Performance in Outsourced System Development

An Investigation into the Risk of Construction Projects Delays in the UAE

Creating Software System Context Glossaries
[www.irma-international.org/chapter/creating-software-system-context-glossaries/13666/](www.irma-international.org/chapter/creating-software-system-context-glossaries/13666/)

The Collaborative Use of Information Technology: End-User Participation and System Success
[www.irma-international.org/chapter/collaborative-use-information-technology/4585/](www.irma-international.org/chapter/collaborative-use-information-technology/4585/)

Recruiting a Project Manager: A Hiring Manager's Perspective
[www.irma-international.org/article/recruiting-a-project-manager/123465/](www.irma-international.org/article/recruiting-a-project-manager/123465/)