Chapter V

Managing Workplace Privacy Responsibly

Richard A. Spinello
Boston College, USA

John Gallaugher
Boston College, USA

Sandra Waddock
Boston College, USA

ABSTRACT

This chapter presents an ethical case for strong workplace privacy rights, which have been jeopardized by the proliferation of monitoring systems and surveillance architectures. After explicating the functionality of those technologies and tracing the history of workplace privacy concerns, we analyze key statutory frameworks and provide some grounding for the ethical imperative to protect workplace privacy rights. But privacy rights must be balanced with the corporation's legitimate need for employee information. To achieve this balance, privacy-related issues must be diligently managed, and we recommend reliance on the Total Responsibility Management model. With the aid of that model, we identify and defend five operative principles for ensuring that monitoring technologies are deployed

in a fair and responsible manner.   In addition to underscoring the importance of privacy rights, our objective is to demonstrate that workplace privacy is an organizational issue that must be prudentially managed by corporations aspiring to be good corporate citizens.

INTRODUCTION

Thanks to the ubiquity of networked digital technologies, privacy rights in the workplace have been under severe pressure for the last decade. There are numerous privacy-invasive technologies that corporations rely upon to monitor their workers in order to help ensure employee productivity or prevent the theft of trade secrets. These technologies range from web site surveillance software to Instant Messaging (IM) monitoring systems that take periodic screen shots of a user's messages. Some monitoring systems, such as SilentWatch™ surreptitiously capture keystrokes, including those that are instantly deleted. If an employee types an angry e-mail message but deletes it before issuing the **SEND** command, every keystroke is still recorded and available for inspection.

Despite the fact that these technologies are reconfiguring the workplace and are often embedded in the worker's tools without knowledge or consent, inadequate attention has been paid to the ethical responsibilities associated with their use. Workers become accustomed only to the level of privacy which these tools and instruments allow. According to J. Cohen (2001), in this new world "rights (and thus expectations) are defined by instrumentality…and by (fictional) consent rather than by any sense of the inherent inviolability of private papers and thought processes" (p. 34).

For many companies whose reputations have been sullied by activist and media criticisms of their corporate practices, explicitly managing these responsibilities should be a major concern. Indeed, responsibility management, which is akin to quality management, is potentially a "new business imperative" of the 21st century (Waddock, Bodwell, & Graves, 2002). Many companies, particularly multinationals with extended supply chains, are developing "total responsibility management" (TRM) approaches resembling total quality management (TQM) (Waddock & Bodwell, 2002). Below we will attempt to illustrate how a similar approach might be put in place in domestic companies with respect to the implementation and use of privacy-invasive digital technologies.

There is good reason to be concerned about privacy. Abuse of employee privacy by companies has the potential to emerge as an embarrassing public issue for companies that have not thought through their rationale for using monitoring systems. Reliance on sweatshop suppliers along with child labor abuses exploded as corporate responsibility issues during the 1990s. Developing a responsibility management approach to those issues has helped some companies cope with the criticism directed at them. Arguably, similar approaches to

22 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/managing-workplace-privacy-responsibility/29307

Related Content

Standardization and Other Coordination Mechanisms in Open Source Software
Tineke M. Egyediand Ruben van Wendel de Joode (2004). *International Journal of IT Standards and Standardization Research (pp. 1-17).*
www.irma-international.org/article/standardization-other-coordination-mechanisms-open/2556

Understanding the Technology Development Process at the Early Standardization Stage: The Case of Cognitive Radio
Vladislav V. Fomin, Hanah Zooand Heejin Lee (2014). *International Journal of IT Standards and Standardization Research (pp. 1-20).*
www.irma-international.org/article/understanding-the-technology-development-process-at-the-early-standardization-stage/121702

Continuous Authentication in Computers
Harini Jagadeesanand Michael S. Hsiao (2013). *IT Policy and Ethics: Concepts, Methodologies, Tools, and Applications (pp. 268-293).*
www.irma-international.org/chapter/continuous-authentication-computers/75034

Investigating the Performance of the TSS Scheme in Noisy MANETs
Hussein Al-Bahadili, Shakir M. Hussain, Ghassan F. Issaand Khaled El-Zayyat (2013). *IT Policy and Ethics: Concepts, Methodologies, Tools, and Applications (pp. 1038-1058).*
www.irma-international.org/chapter/investigating-performance-tss-scheme-noisy/75068

Interaction Between Standardisation and Research: A Case Study
Tore Hoeland Weiqin Chen (2018). *International Journal of Standardization Research (pp. 22-38).*
www.irma-international.org/article/interaction-between-standardisation-and-research/218519