Chapter 63
Dataveillance and Information Privacy Concerns:
Ethical and Organizational Considerations

Regina Connolly
Dublin City University, Ireland

Grace Kenny
Dublin City University, Ireland

ABSTRACT

Information privacy research historically focuses on exploring individuals' concerns in the transaction environment. However, the recent growth of technology-enabled workplace surveillance is raising many concerns over employees' privacy. Employee surveillance practices are becoming increasingly prevalent, ranging from monitoring internet and email activities to capturing employees' interactions with customers and employees' personal health and fitness data using wearable health devices. Individuals may understand that employers can monitor their activities, but may not the potential uses or the repercussions of such monitoring. Moreover, employees may not feel they have the ability to opt-out of this monitoring. This chapter explores the privacy and ethical issues surrounding emerging means of workplace surveillance. The chapter considers both employee and employer perspectives and poses many questions to consider when deciding when does legitimate monitoring become an invasion of employee privacy?

INTRODUCTION

Privacy has been an issue of enduring concern across a wide variety of disciplines and throughout history with discussions spanning back to the writings of Aristotle. In recent decades privacy has grown exponentially in prominence, in terms of increased research activity in many disciplines, the introduction of more stringent legislation in many countries and attracting regular attention in media and societal discussions. Despite the continually growing interest in privacy, a widely agreed upon encompassing, unambiguous definition of privacy remains lacking. It can be argued that the absence of one universally, accepted definition can be attributed to the multidisciplinary nature of privacy, which has generated

DOI: 10.4018/978-1-5225-0983-7.ch063

debate in disciplines such as Law, Marketing, Management Information systems (MIS), Economics and Psychology (Pavlou, 2011). The contrasting conceptualisations of privacy across, and often within disciplines, has led to a fragmented body of privacy literature replete with inconsistent, underdeveloped, and partially validated concepts (Smith, Dinev & Xu, 2011). Thus the generalisability of the conclusions reached from privacy research is often constrained by the conceptual lens applied by the researcher to examine privacy and the context of the study.

The confusion surrounding the privacy construct is also apparent in efforts to determine what is and what is *not* considered privacy. Numerous similar concepts such as secrecy, anonymity and security have are often discussed interchangeably with privacy despite representing separate constructs. However, recently progress has been made to both, distinguish privacy from similar concepts and to organise and categorise the competing perspectives of privacy. For example, Smith, Dinev & Xu (2011) reviewed the varying conceptualisations of privacy across a number of academic disciplines and derived two broad views of privacy; cognate based views and the value based views. While the work of Smith, Dinev & Xu (2011) provides a means of classifying privacy, Dinev *et al.,* (2013) call for the integration of these differing perspectives to build a more rigorous, empirically testable framework of privacy and its closely associated correlates, which have often been confused with privacy.

The need to disentangle the labyrinthine privacy construct is driven by fact that information privacy is an issue of increasing concern to many stakeholders, including citizens, employers, privacy activists, researchers and policy makers. The growing prevalence of Internet-based technologies partly drives concerns across these parties. While these technologies can yield a bounty of benefits for organisations, employees, government bodies, and citizens, they also facilitate the collection, collation and analysis of vast quantities of personal information, often unbeknownst to the person the information pertains to. Such practices used by organisations to collect information on consumers, competitors, and even employees foster privacy concerns. In recent years, there has been a massive surge in the application of pervasive monitoring technologies in the workplace. Activities such as employee email and Internet monitoring unsurprisingly generates privacy concerns amongst employees. Employees' expectation of privacy in the work environment conflicts with the aim of all organisations to operate efficiently. The motivation behind organisations' use of technology-enabled monitoring is understandable and arguably a legitimate means to ensure productivity. However, it can also be argued that organisations' entitlement to engage in some monitoring must be balanced with maintaining some element of privacy for employees.

Technology-enabled monitoring of employees has grown exponentially in recent years, and this growth is forecast to prevail. According to Garner, 60% of organisations will implement a formal digital monitoring policy in 2015 (Garner, 2012). Such monitoring activities as noted tend to include email activity, internet and external social media use but, may also take the form of indisputably invasive key-stroke logging, and more recently, sociometric badges that record face to face employees' interactions with fellow employees and customers. Another emerging form of monitoring relates to wearable fitness devices, often used by individuals to track their personal activity and fitness. Employers have begun offering these devices through company wellness programs to monitor employees' physical activities. With technology enabled monitoring shifting towards invasive practices such as sociometric badges and crossing boundaries from work-related activities only to monitoring employees' health, more questions arise regarding how far organisations' right to monitor extends before it impeaches on individuals' right to privacy. The aim of this chapter therefore is to outline some of the major issues associated with technology-enabled workplace surveillance, to discuss the resultant employee information privacy concerns, as well as managements' motivation to employ monitoring technologies in the workplace. The