Chapter XV
Surveillance of Employees' Electronic Communications in the Workplace:
An Employers' Right to Spy or an Invasion to Privacy?

Ioannis Iglezakis
Aristotle University of Thessaloniki, Greece

ABSTRACT

The use of Information and Communication Technologies in the workplace is constantly increasing, but also the use of surveillance technology. Electronic monitoring of employees becomes an integral part of information systems in the workplace. The specific software which is used for monitoring electronic communications is, however, intrusive and infringes upon the employees' right to privacy. The issue of surveillance of employees' electronic communications is subject to different approaches in various jurisdictions. The most comprehensive protection to employees is afforded in the EU, however, there are still ambiguities concerning the balancing of interests between employers and employees.

INTRODUCTION

The penetration of Internet technology in the workplace is constantly increasing, as almost every office today is equipped with computer systems and Internet connections. The low cost and high efficacy of computers and electronic communications are important factors that make the use of Information and Communication Technologies (ICTs) in the workplace unavoidable (Kierkegaard, 2005, p. 226). However, this ever growing trend has also its drawbacks, due to the fact that it raises privacy risks for employees, since employers are taking advantage of surveillance technology in order to monitor employees' e-mail and internet usage. In addition, monitoring of electronic communications increases working stress and generates discomfort amongst employees.

Copyright © 2009, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

The monitoring of workers in the workplace is not a new phenomenon. Employers have used various methods to control the performance of employees and their behavior at work on the past and they continue to do so. Yet, there were limits to the amount of information that could be collected and used for monitoring purposes with traditional means (Fraser, 2005, p. 227).

Nowadays, new technologies provide more advanced possibilities for monitoring of employees and in more particular, of their surfing activities and the electronic communications that they use, such as e-mail, instant messaging, etc. Other aspects of workplace monitoring include drug testing, closed-circuit video monitoring, phone monitoring, location monitoring, personality and psychological testing and keystroke logging.

The particular subject which will be addressed in this chapter concerns workplace monitoring in relation to employees' electronic communications. This issue constitutes a specific aspect of the more general topic of electronic workplace surveillance, i.e. the use of information technology to monitor the activities and work performance of workers (Godfrey, 2001). Our attention will be drawn at the surveillance of electronic communications at work, that is, the use of monitoring devices in order to gain access to employees' e-mail communications and to data revealing their online activities.

The use of electronic communications by employees and of the Internet in big businesses is very high, while in medium and small-sized businesses it is also constantly rising. Besides the benefits of the wide use of e-mails, this brings about serious issues for companies, such as the dissemination of illegal or offensive material and the leak of trade secrets by disappointed employees to third parties (Mitrou & Karyda, 2006). Additionally, a great number of employees are wasting their working time surfing on the Net and sending private e-mails (so-called "cyberslacking"), whereas this may give rise to termination of employment contracts.

For those reasons employers consider as their right to control the online activities of their employees. Certainly, employers have a legitimate interest in monitoring the behavior of their employees in order to secure the acceptable performance of employees and maximize productive use of their computer systems, to prevent the leak of sensitive company information, to prevent or even detect unauthorized use of said systems for criminal activities and ensure security of computer systems, to avoid sexual harassment in the workplace and discrimination, and monitor employees' compliance with employment workplace policies related to use of ICT (EPIC; Lasprogata et al., 2004, pp. 2-3). However, such monitoring may have as a consequence the intrusion into the private life of employees and an infringement of their rights to respect of privacy and confidentiality of communications.

MONITORING METHODS OF ELECTRONIC COMMUNICATIONS AND MONITORING DEVICES

New technologies not only provide unlimited access to information, which becomes available to employees, but also effective means for their surveillance. Specific software applications exist, which facilitate the interception of communications and real time surveillance of surfing behavior. Such applications provide central control over software on individual PCs, meaning that programs can be remotely modified or suspended, while e-mail traffic and surfing activities can be read and analyzed (Davies). Companies are making extensively use of such software, which is affordable and widely available. In a survey carried out by the American Management Association and the ePolicy Institute in 2007, it was determined that employers were concerned over inappropriate use of the Internet in a great extent and as a result, they proceeded into monitoring of e-mail and Internet activities. Pursuant to the survey, 66% of employers monitor Internet connections and 65% block connections to unauthorized Internet sites (Survey, 2007).

12 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/surveillance-employees-electronic-communications-workplace/29368

Related Content

An Image Region Description Method Based on Step Sector Statistics and its Application in Image Copy-Rotate/Flip-Move Forgery Detection
Likai Chen, Wei Luand Jiangqun Ni (2012). *International Journal of Digital Crime and Forensics (pp. 49-62).*
www.irma-international.org/article/image-region-description-method-based/65736

Exploiting Geometrical Structure for Forensic Applications of Timing Inference Channels
Bilal Shebaro, Fernando Pérez-Gonzálezand Jedidiah R. Crandall (2013). *International Journal of Digital Crime and Forensics (pp. 54-69).*
www.irma-international.org/article/exploiting-geometrical-structure-for-forensic-applications-of-timing-inference-channels/79141

Children's Rights in the Digital Space: Legal and Ethical Considerations
Anjali Rawat, George Kurian, Romil Rawat, Janet Olivia Richmond, Anand Rajavatand Purvee Bhardwaj (2026). *Child Protection Laws and Crime in the Digital Era (pp. 79-106).*
www.irma-international.org/chapter/childrens-rights-in-the-digital-space/386097

Unexpected Artifacts in a Digital Photograph
Matthew J. Sorell (2009). *International Journal of Digital Crime and Forensics (pp. 45-58).*
www.irma-international.org/article/unexpected-artifacts-digital-photograph/1591

Information Disclosure on Social Networking Sites: An Exploratory Survey of Factors Impacting User Behaviour on Facebook
Clare Doherty, Michael Lang, James Deaneand Regina Connor (2015). *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance (pp. 515-532).*
www.irma-international.org/chapter/information-disclosure-on-social-networking-sites/115779