

Employees' privacy vs. employers' security: Can they be balanced?

Lilian Mitrou^{*}, Maria Karyda¹

*Department of Information and Communication Systems Engineering, University of the Aegean,
Samos GR-83200, Greece*

Received 27 July 2005; accepted 27 July 2005

Abstract

This paper addresses the controversy between employees' right to privacy and employers' need to safeguard organizational resources by employing monitoring tools. It shows how organizations can formulate use policies, by applying basic principles for fair and lawful monitoring. A list of key points is presented, which organizations should take into account, for developing such policies. Finally, the paper explores how, widely accepted information security standards, such as the ISO 17799, can aid the attempt to address this controversy.

© 2005 Elsevier Ltd. All rights reserved.

Keywords: Workplace surveillance; Monitoring; Employee's privacy; Insider threat; Information systems security; ISO 17799

1. Introduction

Information and communication technology have drastically transformed the workplace in the last two decades. Technology provides the means for improved productivity, and faster adaptation to changing market demands.

Traditionally, the terms of employment entail collecting a considerable amount of information about employees, as these data are necessary for basic management activities

^{*} Corresponding author. Tel.: +30 22730 82250; fax: +30 22730 82009.

E-mail addresses: L.mitrou@aegean.gr (L. Mitrou), mka@aegean.gr (M. Karyda).

¹ Tel.: +30 22730 82266; fax: +30 22730 82009.

such as hiring, payroll processing, performance evaluation and organization security. Additionally, the employment relationship has gradually become an indispensable source of information for state activities, including taxation or occupational health and safety. Within the context of the “information transformation” (Schwartz and Reidenberg, 1996), technology penetrated business and personnel decision-making and enabled increasingly sophisticated treatment of personal data and employees monitoring.

The terms *workplace monitoring* and *surveillance* refer to activities intended to collect and record information about employees, by keeping them under observation (UK Information Commissioner, 2003; CNIL, 2002). This can be done in a systematic or an ad hoc way, either by examining their work output, or by using electronic means.

Although employee surveillance is by no means a new phenomenon, the possibility to do so without any human intervention or interruption is. Currently, an immense new array of sophisticated technology is available to the employer (Altenburg et al., 2005; Desprochers and Roussos, 2001). The technology used to monitor employees is very powerful and extends to every aspect of employees’ life, making surveillance less overt and more diffused (Introna, 2000).

Although the uptake of monitoring tools is a fairly recent phenomenon, it seems to increasingly gain support among organizations. This uptake is augmenting, despite the fact that very often workplace monitoring results into adverse employee reaction, low employee moral and high turnover. Moreover, surveillance and monitoring have become components of modern information systems and the modern work environment. Surveillance is viewed as a “value added” element of information systems, as designers are often required to design technology, which will capture, analyze and disclose personal information. These technologies have not evolved in isolation. They are related to profound, far reaching changes in the structure of work and the ethos of management (ICC, 2003; Davies, 1999).

Information and communication systems are confronted by a great variety of threats. Attacks originating from outside, such as hacking attempts usually get public attention. Insider threats, on the other hand, pose a significantly greater level of risk (Schultz, 2002) and have a heavier cost for organizations. With the term “*insider threat*” we refer to threats originating from employees of an organization, who have been given access rights to information and communication systems, and misuse their privileges, performing actions that violate the security of these systems. Security controls used for protecting information systems from externally initiated attacks (e.g. firewalls and intrusion detection systems) are not effective in detaining insider threats, since the latter requires a different approach (Porter, 2003; Lee and Lee, 2002; Schultz, 2002). Surveillance technology is increasingly applied by organizations in their attempt to confront information systems security threats, and especially insider threats.

The focus of this paper is *on workplace surveillance with regard to electronic communications*; by that we mainly refer to the use of the Internet, as, due to the increase of new information technologies, communication activities have migrated from the periphery to the very centre of the work process and their monitoring has emerged as commonplace practice (Altenburg et al., 2005).

Internationally, the average proportion of employees in large businesses making daily use of external e-mail is rising (DTI, 2003). Data on large businesses in the UK indicate that in 91% of employees use the e-mail for carrying out business activities, and in 92% of the organizations employees visit web sites as part of their business activity (DTI, 2002). The benefits stemming from the wide use of e-mail for business is undeniable;

however, the widespread use of e-mail entails also a number of severe problems for organizations. The dissemination of illegal or offensive material via e-mail by employees, or the distribution of confidential information can cause bad reputation or even legal prosecution for organizations. Such reasons lead many organizations to explore ways for controlling information communicated by their employees, by means of e-mail, fax, phone calls or electronic file exchange.

Monitoring methods are implemented for many reasons such as controlling and allocating costs of different performances and communications, measuring and improving productivity. Many employers are confronted with the need for verifying breaches of confidentiality, preventing corporate image flaws or checking compliance with security rules.

This paper addresses the issue of workplace monitoring, for security reasons, i.e. to prevent or detect industrial espionage, theft of trade secrets and other proprietary information, copyright and patent infringement, unauthorized access to computer systems, to protect computer networks from becoming overloaded, to discourage unacceptable employee conduct and investigate complaints, and to respond to needs and requests in litigation related to electronic evidence.

Undoubtedly, an employer has a legitimate right and interest to run his/her business efficiently and the right to protect his/her property and himself from the liability or the harm that employees' actions may cause. On the other hand, monitoring raises serious concerns with regard to employees' rights and freedoms. The risks of intrusions on the employees' privacy, data protection and freedom of communication are enormous. Do employees abandon their right to privacy every morning at the doors of their workplace? How can employers provide for the security of their information systems, without offending employees' rights? Can organizations adopt a balanced approach between these competing rights and interests while, at the same time, preserving their security, especially from insider threats?

Although the protection of privacy is a concern for both organizations and employees, these have different perspectives: for employees, it is important to know that their private communications remain private. Employers, on the other hand, need to prevent illegal actions, or actions that could jeopardise the security of the information and communication systems.

This paper argues that organizations can address the standing controversy between an employee's right to privacy and an employer's need to safeguard organizational resources, by formulating *use policies*, which are based on *principles of lawful monitoring* and on existing, widely used *security management standards*.

The rest of the paper is structured as follows: the next section provides an overview of current approaches on the debate on workplace monitoring and the employees' right to privacy. Section 3 discusses the major legal, technical and organizational issues on workplace monitoring. Section 4 describes how ISO 17799 can accommodate the fundamental principles for lawful monitoring in the workplace and presents general directions on formulating use policies that are compliant with the principles for lawful monitoring. Finally, the last section presents the overall conclusions and indicates issues for further research.

2. Privacy in the workplace: Current approaches

Privacy is universally recognized as an individual, personal right of philosophical and moral origins. However its notion and content is often debatable. In our approach privacy

is far more than the Warren and Brandeis's passionate pleading for "*the right (of the individual) to be let alone*", a refuge for the individual, which serves as an incomplete constitutional paradigm in the computer age (Schwartz and Reidenberg, 1996). Privacy is, furthermore, a characteristic of relation with others (Podlech, 1979). It includes, among others facets of privacy (bodily, territorial etc.), the right to control of information and the control of access about oneself (Westin, 1967; Parent, 1983) or, as defined from part of the European theory, the "*right to informational self-determination*", which proves to be a prerequisite to the capacity to participate to social discourse (Simitis, 1987). Processing and sharing of personal information and the transparency of the individual achieved can have destructive effects on the capacity for free decision-making (deliberative autonomy). The opportunity of individuals to form and act on their own notions of good, presupposes that individuals both be able to retreat and participate to social life (Schwartz and Reidenberg, 1996).

2.1. Minimal expectation of privacy: The USA approach

Employees are routinely asked to sacrifice privacy rights to managerial interests like productivity, prevention and detection of threats and liability risks. In some jurisdictions, law and courts have recognized only a "*minimal right to privacy*", limited to those instances where the matter/area intruded upon is "intensely private".

Under the "*content approach*", courts "*decide the legitimacy of the employer's interest... by analysing the purposes behind the monitoring and whether the content of the communication is reasonably related to the proffered purposes.*" Under the "*context approach*", courts "*determine the reasonableness of the employee's expectations by analysing the employer's notification procedures*" (Kesan, 2002). However, in *Smyth v. Pillsbury* the judge noted that the plaintiff had "no reasonable expectation of privacy notwithstanding his employer's assurance about the confidentiality of the messages" (Desprochers and Roussos, 2001). Given the per definition public-nature of the workplace and its purpose, many argue that employees, who are hired to attend company business, cannot have a "*reasonable expectation of privacy*". Furthermore, they justify the lack of privacy, by referring to the fact that monitored communications are voluntarily transmitted on an employer's network, using equipment designated to serve business objectives (Fazekas, 2004).

The "*property argument*" has been proved a decisive one (Lasprogata et al., 2004): Courts have insisted on property rights, affirming the principle that employers may monitor communications taking place inside their premises with the use of their equipment. In *McLaren v. Microsoft*, the Texas Court of Appeals expressed the opinion that McLaren did not have a reasonable expectation of privacy since the e-mails were transmitted over the company's network and were "*at some point accessible to a third-party*". The judges noted that notwithstanding the personal password he used to access his messages and the fact he stored them in his "*personal folder*", the messages "*were not McLaren's personal property, but were merely an inherent part of the office environment*" (Desprochers and Roussos, 2001). This view was also shared by the Court of Milan in 2002, which rejected the complaint of a dismissed worker on the grounds that the e-mail addresses allocated to employees are "*normal work instruments and that the proprietorship of e-mail pertains solely to the employer*" (Delbar et al., 2003).

Another significant aspect concerns the issue of *liability*. Employee misuse of the Internet may, under the doctrine of respondent superior, result in substantial legal liability for

the employer to third persons. Illegitimate or unlawful acts like defamation, public disclosure of private and business facts, disclosure of trade secrets and patents, spamming or computer-fraud, committed during regular work hours, are causes for legal actions. Courts and regulators recognized that the substantial liability employers bear for their employees' acts, justifies or even requires the supervision of communications (Fazekas, 2004).

Employees' privacy expectation and—consequently—protection, are hardly-founded on constitutional texts, as such texts generally, as in the case of U.S. Constitution, have been found to restrict only government intrusions into privacy and therefore are inapplicable to workplace privacy intrusions by private employers and other non-governmental actors (Lasprogata et al., 2004). Even if individual autonomy is revered, as is apparent in the jurisprudence of “*decisional privacy*”, the right to privacy is treated as akin to personal property. During the course of bargaining, an employee can trade his privacy and “*exchange it for something of commensurate value, such as a job*” (Lasprogata et al., 2004). It is the alienability of privacy that allows an employer to receive (implied) consent of the employee or to virtually eliminate any reasonable expectation of privacy by notifying his/her employees of a monitoring policy.

2.2. *Right to respect of privacy: The EU approach*

American law in this area seems diametrically opposite to the situation in Europe: Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms states: “*Everyone has the right to respect for his private and family life, his home and his correspondence*”. The more recent Charter of Fundamental Rights of the European Union affirms that “[e]veryone has the right to respect for his or her private and family life, home and communications” (Art. 7) as well as the “*to the protection of personal data*” (Art. 8).

The European Court of Human Rights rejected the distinction between private life and professional life since the workplace is especially suited for social intercourse (Klare, 1982) and “*it is after all in the course of their working lives that the majority of people have a significant opportunity of developing relationships with the outside world*” (Niemitz v. Germany). The case Halford v. United Kingdom is insightful for the extension of the protection of privacy in correspondence to electronic communications: The Court decided that interception of workers phone calls at work constituted a violation of Art. 8 and rejected the argument of U.K. that the plaintiff had no reasonable expectation of privacy in those calls, as they were made using telephones provided by the employer.

A decisive criterion is the difficulty to “*distinguish clearly which of an individual's activities form part of its professional life and which not*” (European Court of Human Rights, Niemitz v. Germany). Information systems and tools facilitate the intrusion of professional life into the personal sphere. The boundary between home life and workplace, between work hours and private life, due partly to developments in both workplace and surveillance technologies partly to changes in demographics of employment, has become increasingly blurred. Furthermore, it is not always easy to draw the distinction between workplace and private information: monitoring raises additional concerns for example in the case of e-mail messages from a worker to an occupational health advisor or messages between employees and their trade union representatives (UK Information Commissioner, 2003).

Although Niemitz, Halford and other similar cases before the Court concern government action, it appears that in the EU the opinion that Art. 8 of the Convention is relevant also in private context has gained a strong support. Already in the 80's, governmental reports and high courts' decisions addressed the change, referring to the employee as "*the citizen of the enterprise*" (France-[Rapport Auroux, 1981](#)) and pointing out that the employer's opportunities to monitor his/her employees augments his/her chances to influence their behaviour and thus increases their dependence on the employer. Constitutional rights cease to be mere means of defence against state activities and become structural components of the employment relationship. Rights and freedoms penetrate the employer–employee relationship and question a system of "*indisputable prerogatives*" of the employer ([Simitis, 1999](#)).

A number of cases, judged by courts in European states, confirms this approach: The Austrian Oberster Gerichtshof established, in 2002, that employer monitoring of employee telephone use affected employees' "*dignity*", while the French Cour de Cassation (Onof v. Nikon) ruled that an employer cannot read personal messages sent or received by employees, without violating the right to privacy and infringing the fundamental liberty of confidentiality of correspondence, even if the employer has prohibited non-work related use of the computer ([Lasprogata et al., 2004](#); [Delbar et al., 2003](#)).

Respect for private life includes, to a certain degree, the right to establish and develop relationships with other human beings. The fact that such relationships, to a great extent, take place at the workplace puts limits to employer's legitimate need for surveillance measures. Employees have a legitimate expectation of privacy in the workplace and secrecy of communications and correspondence, which is not to be ruled out or overridden by the location and ownership of the electronic communications means used ([DPWP, 2002](#)).

The fundamental rights of privacy and secrecy of communications of employees are, however, subject to derogations and limitations, in particular where they are confronted with rights and freedoms of others similarly protected by the law, e.g. the legitimate interests of the employers. Employees' rights are balanced against the interests of employers when validating the processing of employees' communications and generally personal data. When can monitoring activity be considered lawful and justified? Which is the degree of tolerable intrusion in employees' communications?

An employer's ability to monitor must also be balanced with considerations of employee morale and job satisfaction. The panoptic effect of being constantly monitored, achieved through surveillance, has negative impacts interfering with the relationship of mutual trust and confidence that should exist between employees and employer ([UK Information Commissioner, 2003](#); [Desprochers and Roussos, 2001](#)). Studies have shown that workers whose communications were monitored, suffered from higher rates of depression, anxiety and fatigue than those not subject to monitoring at the same business ([Fazekas, 2004](#)).

Current practice in organizations requires that such issues be regulated by applying a *use policy*: in this way, employees can have a clear expectation as to what is considered responsible and ethical use of the technological infrastructure, whereas, at the same time, the same applies for the stance employers have against their employees. However, the controversy between the employers' legitimate interest to run their business effectively and the employees' legitimate concerns for the protection of their privacy, poses difficulties to the endeavor to formulate an effective, fair and applicable use policy. Moreover, the fact that the legal landscape regarding workplace surveillance remains confused and unclear, as we showed in the previous paragraphs, makes this effort even harder.

To address this issue, we provide in the following sections, a set of guidelines pertaining the legal basis of workplace monitoring, alongside with indications as to how existing, widely used security management standards, such as ISO17799, can facilitate the development of a use policy that complies with legal requirements.

3. Electronic monitoring: Legal, technical and organizational issues

3.1. *The legal basis of monitoring*

Employers have a legitimate interest in monitoring employees' communications for lawful and legitimate purposes that are necessary for the normal development of the employment relationship and the secure business operation. Legitimate monitoring and processing of the derived data includes data that are necessary (a) for compliance with a legal obligation of the employer, (b) for the performance of the work contract, (c) for the purposes of a legitimate interest pursued by the employer or (d) for the performance of a task carried out in the public interest (DPWP, 2001). The legitimate purpose, pursued through monitoring, should be set in advance of a measure's application and be readily demonstrable to employees (Charlesworth, 2003).

Doubts are expressed about the capability of the employer to legitimise monitoring through employees' consent. Consent must be explicit, freely given and fully informed. The European Commission has expressed the opinion that "*employers should avoid relying on the worker's consent as a means that legitimises by itself processing of personal data*" (European Commission, 2002) while the International Labour Office (ILO) accepts, under conditions, employee's consent as legitimate basis for the collection of data (ILO, 1997). In our opinion, due to the nature of the employment relationship, in which there is an inherent asymmetry of power and the employee is subordinate and dependent, reliance on consent should be confined only to the very few cases where the employee has a genuine free choice and is subsequently able to withdraw the consent without detriment.

3.1.1. *Principles for lawful and fair monitoring*

Before workplace monitoring can be considered lawful and justified, the employer must comply with the following fundamental privacy and data protection principles: *necessity*, *finality*, *proportionality*, *transparency* and *security* (Council of Europe, 1989).

3.1.2. *The principle of necessity*

Employers may carry out monitoring of electronic online communications data as long as it is pursuing the *prevention of illegal or defamatory acts*, acts that are contrary to good ethics or which can damage the dignity of another person, the protection of the economic, commercial and financial interests of the organization, the security and good operation of its information and communication systems and the observance of the principles and rules applicable in the company for the use of on-line technologies (Belgian National Labour Council, 2002). Employers must check if any form of monitoring is absolutely *necessary* for a specified purpose before proceeding to such activities.

Monitoring of communications or Internet use could be considered necessary only in exceptional circumstances: in order to obtain confirmation or proof of actions like criminal activity or detection of viruses. UK Information Commissioner proposes to carry out

a formal or informal “*impact assessment*” to decide if and how to carry out monitoring. This assessment involves the identification of purposes and benefits, the identification of “*adverse impacts*” on workers and possibly on third parties/customers and the consideration of possible alternatives (for example limitation of monitoring to high risk workers or areas) (UK Information Commissioner, 2003).

3.1.3. The principle of finality

Employers must distinguish between the various aspects of the employment relationship and specify the aims for which monitoring is required. Processing must be strictly confined to the data necessary with regard to the particular employment relationship. Both the amount and the kind of data vary according to the individual employee’s tasks or the context of the employer’s decisions (Simitis, 1999). Monitoring should be carried out for a specific, explicit, and legitimate purpose and monitoring data should not be further processed in any way that is incompatible with that purpose. For example, personal data collected in order to ensure the security or the proper operation of processing systems should not be processed to control the behavior of individual employees, except where the latter is linked to the operation of these systems (European Commission, 2002).

3.1.4. The principle of proportionality

The level of tolerated privacy intrusion depends on the nature of the employment as well as on the specific circumstances surrounding and interacting with the employment relationship (DPWP, 2001). The employer’s monitoring policy should be tailored to the type and degree of risk the employer faces. Monitoring must, in all cases, be *appropriate, relevant* and *proportionate* with regard to the aims that it is pursuing. Automatic and continuous e-mail and Internet monitoring should also be considered as prohibited (Lasprogata et al., 2004). The proportionality principle rules out routine monitoring of individual e-mails and Internet use of all employees, notwithstanding particular cases such as automated monitoring for purposes of security and proper operation of the system (e.g. protection against malicious software) (DPWP, 2002; European Commission, 2002).

The most important of the effects of the proportionality principle is that employers should always monitor employees “*in the least-intrusive way*” (ILO, 1997): The employer should consider for example if the investigation of specific incidents or problems can be based on accessing stored e-mails to follow up a malpractice, rather by continuous monitoring, or if monitoring can be limited to workers about whom there are grounds to suspect of wrong-doing (UK Information Commissioner, 2003).

Another critical effect relates to the *content* of the messages monitored. E-mail monitoring should be limited to traffic data *size* and *type* of any attachments, and not extend to the actual content of the messages sent or received. Private e-mails and files should be treated as private correspondence covered by the right to communications secrecy: The employer should in principle be prohibited from opening private e-mail and other files, notably those explicitly indicated as such, irrespective of whether private use of work devices and tools was allowed or not by the employer (European Commission, 2002). Opening of e-mails can only be justified in very limited circumstances, such as for detecting criminal activity on the part of the worker insofar as it is necessary for the employer to defend his/her own interests, if (s)he is liable for the employee’s actions or (s)he is the victim of the activity.

3.1.5. The principle of transparency

The transparency principle seems to be the commonly accepted *minimum component of a workplace privacy policy*. The transparency rule requires that employers' monitoring practices be fully and clearly *disclosed* to all employees subject to the policy, along with the *reasons* for the monitoring. Notably, cases in Denmark, the Netherlands and the UK, have established the necessity for employers to have issued a clear *use policy* or instructions on Internet/e-mail use before it is legitimate for them to dismiss or discipline employees on grounds of misuse (Delbar et al., 2003). Recently, German courts have ruled that employers may retrieve an employee's personal electronic communications only if in furtherance of a valid business interest, the employee has been given notice, and the rules governing Internet connection and email use applied by the employer have been agreed to by the employee's elected works council. The Regional Labour Court of Hessen recently upheld a lower labour court decision holding that an employer is not entitled to dismiss an employee for sending private emails, even where such behaviour was expressly prohibited, without a prior formal warning for the infringement (Lasprogata et al., 2004), while the Regional Labour Court of Rheinland Pfalz insisted on explicit prohibition of private Internet use as a condition of a valid dismissal.

The employer has to provide employees with a readily accessible, clear and accurate statement of the *use policy*, with regard to e-mail and Internet monitoring (DPWP, 2002). Ideally, an employer should give such notice upon hiring. The employer should also inform employees about the principal and secondary uses to which their personal data generated by such systems are being put (IWGDPT, 1996). Further elements of information should include details as to the nature and duration of the surveillance, features of technology used and type of information compiled, details of any enforcement procedures outlining the notification of breaches of internal policies and finally their rights to have access to the data processed about him and to correct errors (DPWP, 2002; IWGDPT, 1996).

Only exceptional circumstances may justify the so-called *secret or covert monitoring*. In Germany, the Federal Constitutional Court and Federal Labour Court have ruled that any secret monitoring is an intrusion into employees' private life (Delbar et al., 2003). This requires that there is suspicion on reasonable grounds that a grievous criminal activity has been or will be committed (ILO, 1997; IWGDPT, 1996). Additionally, according to ILO's Code of Practice, secret monitoring should be permitted only if "*it is in conformity with national legislation*".

The transparency principle is strictly connected with the need of employees' representatives' involvement. The representatives must be fully informed and consulted prior to any decision to introduce any electronic monitoring policy and, where necessary, obtain their agreement (DPWP, 2002; IWGDPT, 1996). In the EU, Directive 2002/14/EC provides additionally for information and consultation of employees' representatives on decisions likely to lead to substantial changes in work organization. Representatives must also be able at any time to check whether regulations and guidelines to protect the workers' privacy are followed.

3.2. Technical issues

Monitoring methods and tools include video surveillance of the workplace, software for scanning e-mails, eavesdropping on phone calls, monitoring and recording keystrokes, and

for recording web sites visited and remote files accessed. In the case of e-mail monitoring, differentiation needs to be made between e-mail *scanning*, which refers to checking attachments for potential viruses or for their size, and e-mail *monitoring* or *surveillance* that entails checking messages for actual content and specific attachments (Watson, 2002). E-mail monitoring tools can be used to examine messages anywhere: in the systems folder, while transmitted via telecommunication networks, in the recipients' mailbox, even in erased files. They can be configured to search messages for certain words or phrases and trigger a warning or block the delivery of the message.

However, the same technologies that threaten employees' privacy can also be used to help protect it. Technological solutions that can offer privacy protection, are known under the name Privacy-Enhancing Technologies (PET or PETs). Perhaps the most fundamental of these techniques depend upon *encryption*. PETs aim to protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, while preserving, at the same time, the functionality of the information and communication system. Use of PETs has achieved an important place among privacy protection instruments and is usually considered as substitute for other instruments of privacy protection, such as laws and regulatory bodies. However, PETs should be better considered complementary to other privacy protection endeavors, with which they must be *combined* in order to address the issue of privacy protection in an effective and holistic way.

3.3. Organizational issues

The advent of surveillance technology and the diffusion of monitoring tools in the workplace environment, make it impossible for employees to be aware of the many different ways technology can be used to monitor them.

An important issue with regard to the fair application of workplace monitoring, is the *asymmetry of power* that characterizes employment situations. Introna (2000) pinpoints that the current US climate is heavily biased in favour of the employer. He also underlines, however, that in spite of this unbalance of power, surveillance has not become a widespread practice. This remark is confirmed by Watson (2002), who discusses the results of different surveys on e-mail monitoring, showing that monitoring levels presented by UK-based surveys are "surprisingly high" compared to surveys based in the USA. Despite the differences among surveys, however, there is a clear trend among organizations, which suggests an increasing use of surveillance tools.

Monitoring within organizations can extend from *unlimited monitoring*, to *monitoring certain activities*, to *monitoring when suspicions* for illegal or inappropriate behaviour, to *no monitoring*, unless required by law (Whitman et al., 1999).

4. ISO 17799 and privacy protection

The International Organization for Standardisation (ISO) recently adopted the British Standard BS7799 ("Code of practice for information security management") and published it as the ISO 17799 International Standard (ISO/IEC, 2000). Since then, an increasing number of organizations world-wide formulate their security management system according to this standard. It provides a set of recommendations for information security management, focusing on the protection of information as an asset. It adopts a broad perspective that covers most aspects of information systems security, namely: *Security Policy*,

Organizational Security, Asset Classification and Control, Personnel Security, Physical and Environmental Security, Communications and Operations Management, Access Control, Systems Development and Maintenance, Business Continuity Management and Compliance.

4.1. ISO 17799 and privacy protection

Among its recommendations for organization security, ISO 17999 indicates that “*The use of personal information processing facilities for processing business information and any necessary controls should be authorized*”. By implementing such controls, organizations can, at the same time, achieve both organization *security* and personal *data protection*. It also suggests that an appropriate set of procedures should be defined for information labelling and handling, in accordance with the classification scheme adopted by the organization. These procedures should cover information assets in both physical and electronic formats, as well as different activities, such as copying, storage and transmission by post, fax, electronic mail, transmission by spoken word, including mobile phone and voicemail. To provide for the employees’ privacy, organizations complying with the ISO 17799, should adapt their classification scheme according to the monitoring and privacy protection guidelines.

To reduce the risks stemming from human errors, theft, fraud or misuse of facilities, ISO 17799 proposes a wide set of security controls, including that the employees’ legal responsibilities and rights, e.g. those stemming from the data protection legislation, should be clarified and *included within the terms and conditions of employment* (ISO/IEC, 2000).

The standard also states explicitly the importance of *user awareness*, and proposes a set of recommendations to “*ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work*” (ISO/IEC, 2000). According to the principles for lawful and fair monitoring, and especially the principle of transparency, as described in Section 3, employees must be aware of all monitoring practices, along with the reasons for the monitoring. Since, in most cases, workplace monitoring is used to address inside security breaches, it is evident that including the issues of workplace surveillance into a security training and awareness program, can help avoid negative employee attitude, and at the same time promote security awareness among employees. Moreover, the standard suggests that a formal disciplinary process should be in place, for employees who have violated organizational security policies and procedures.

For ensuring the correct and secure operation of information processing facilities, ISO 17799 suggests that organizations should “*draw up a clear policy regarding the use of electronic mail*”. Such a policy should include directions on issues such as (ISO/IEC, 2000):

- Attacks on electronic mail, e.g. viruses, interception.
- Protection of electronic mail attachments.
- Guidelines on when not to use electronic mail.
- Employee responsibility not to compromise the company, e.g. sending defamatory electronic mail, use for harassment, unauthorized purchasing.
- Use of cryptographic techniques to protect the confidentiality and integrity of electronic messages.

The standard also suggests that consideration should be given to the security and business implications of the use of information and communication systems. To address prob-

lems that can arise from their use, ISO 17799 suggests that appropriate policies and guidelines should be prepared and implemented to confront issues such as (ISO/IEC, 2000):

- Vulnerabilities of information in office systems, e.g. recording phone calls or conference calls, confidentiality of calls, storage of faxes, opening mail, distribution of mail.
- Policy and appropriate controls to manage information sharing.
- Restricting access to diary information relating to selected individuals.
- Categories of staff, contractors or business partners allowed using the system and the locations from which it may be accessed.

Additionally, the standard also suggests that, with regard to systems that are publicly available, security controls should be implemented so as that “*information is obtained in compliance with any data protection legislation*” and especially “*sensitive information is protected during the collection process and when stored*” (ISO/IEC, 2000).

Finally, ISO 17799 suggests that compliance with data protection legislation is best achieved by the appointment of a *data protection officer*, who should provide guidance to managers, users and service providers on their individual responsibilities and the specific procedures that should be followed.

4.2. Key points in formulating use policies

ISO 17799 acknowledges the importance of legislative requirements, such as legislation on data protection and privacy of personal information and on intellectual property rights, for providing a “*good starting point for implementing information security*” (ISO/IEC, 2000). According to the standard, an essential part of any information security management system is a *security policy*, aiming to “*provide management direction and support for information security*” (ISO/IEC, 2000). The standard also requires that the security policy includes a brief explanation of “*the security policies, principles, standards and compliance requirements of particular importance to the organization*” (ISO/IEC, 2000), especially those that concern compliance with legislative and contractual requirements. In this way, an organization applying a security policy can inform its employees on the data protection and privacy legislation the organization complies with.

It also suggests that, besides applying an organization-wide information security policy, effective security managements requires that, *more detailed security policies and procedures* for specific information systems or security rules should also be formulated. Under this perspective, organizations should formulate a standing operational use policy for day-to-day use of their information and communication systems, which is usually referred to as *use policy*.

A use policy can provide a common basis of understanding of what for and how employees can use information and communication systems. Well written and carefully worded use policies that inform employees on the *necessity* of the applied monitoring tools and methods, and the *purpose* for the monitoring (principle of *finality*) are more likely to avoid hostile employee reaction and gain employee tolerance or even support. ISO 17799 acknowledges that “*the co-operation of authorized users is essential for effective security*”.

We believe that the fundamental principles for lawful and fair monitoring, discussed in Section 3, along with the basic security guidelines derived from ISO 17799, as described in the previous section, should form the basis upon which an appropriate use policy is

formulated. Although the formulation of a use policy is highly dependent on the technological (i.e. type of information and communication technologies used) as well as the organizational context (e.g. business sector), several aspects of use policies are common in most organizations.

In the following we provide a list of *key points*, based on the analysis of legal, organizational and security issues, that can help organizations develop use policies that are both lawful and fair, while, at the same time promote the security of information and communication systems:

- The use policy should state its scope.
- The use policy should be compliant with data protection legislation.
- It should contain clear guidelines as to how employees may and may not use e-mail, telephones, fax and Internet access.
- The use policy should state the purposes for which monitoring is conducted.
- The use policy should describe the methods and tools applied for monitoring.
- The disciplinary process in the case the policy is violated should be defined.
- The use policy should describe the alternatives employees can use to preserve the confidentiality of their communications.
- Automated tools and systems should be used for e-mail scanning and protection against viruses and other types of malicious code.
- E-mail monitoring should be confined to address and header scanning.
- The policy should inform employees about the person responsible for overseeing its application.
- The policy should also refer to scheduled reviews and modification procedures.

5. Conclusions and open issues

In response to the bigger risks of privacy breaches, a number of solutions have been proposed. The (“minimal”, “reasonable” or law embedded) *expectation of privacy* seems to be generally accepted. The lack of a common legal paradigm is due to inconsistencies in the privacy laws and underlying legal and societal value systems of the different countries. These differences illustrate the value each legal system assigns to market (i.e. the employer’s) needs versus, at the core, fundamental human rights of the individual employee.

The issue of workplace monitoring has many different organizational, legal and technological aspects. In this paper we tried to show how employers can assess the privacy implications of electronic monitoring processes and choose to tailor these practices to balance employees’ privacy rights and interests with legitimate business concerns. We have presented and proposed a set of legal principles, based on existing European legal framework, but also reflecting fundamental privacy principles drawn from the OECD Guidelines Governing the Protection of Privacy (OECD, 1980) and Council of Europe’s Data Protection Convention (1981), as well as security guidelines derived from widely used security standards. These principles can serve as the basis for formulating effective, lawful and fair use policies. We have also presented a list of key points that should be taken into account when developing these policies.

Organizations can turn to basic principles for lawful monitoring, in order to formulate their policies. A further aid to this attempt can result from following the security guidelines

of a widely accepted information security standard such as the ISO 17799, adapted appropriately. Organizations will also benefit from applying specific use policies for their information and communication systems. These policies should be organized within a wider security management framework, so as to address both the issue of information systems security, especially the insider threat, and, at the same time, provide a fair and lawful monitoring scheme.

However, surveillance is—per definition—likely to violate employees' autonomy and their right to be free from unjustified intrusion into their workaday life. A moral right to privacy is grounded in ethics; particularly in the ethical principle that each person possesses dignity and respect and must be treated as a worthwhile end and not as a mere means. Even if the debates, dealt with in our paper are resolved, the issue whether employee monitoring is *ethical*, remains open.

References

- Altenburg, S., Reinersdorff, W.v., Leister, T., 2005. Telekommunikation am Arbeitsplatz. Multimedia und Recht 3/2005, 222 ff.
- Belgian National Labour Council, 2002. National collective agreement on the protection of workers' privacy with respect to controls on electronic on-line communications data.
- Charlesworth, A., 2003. Privacy, personal information and employment. Surveillance and Society 1 (2), 217ff.
- Commission Nationale de l' Informatique et des Libertés (CNIL), 2002. La cybersurveillance sur les lieux de travail. Paris.
- Council of Europe, 1981. Convention for the protection of individuals with regard to automatic processing of personal data, ETS No. 108, Strasbourg.
- Council of Europe (CoE), 1989. Protection of personal data used for employment purposes. Recommendation No. R (89) 2—Strasbourg.
- Data Protection Working Party (DPWP), 2001. Opinion 8/2001 on the processing of personal data in the employment context. 5062/01/Final.
- Data Protection Working Party (DPWP), 2002. Working document on the surveillance of electronic communications in the workplace. 5401/01/Final, Available from: <<http://www.europa.eu.int/comm/privacy>>.
- Davies, S., 1999. New Techniques and Technologies of Surveillance in the Workplace. MSF Information Professionals' Association, London School of Economics, London. Available from: <<http://www.amicustheunion.org/pdf/surveillencetechniques.pdf>>.
- Delbar, C., Mormont, M., Schots, M., 2003. New technology and respect for privacy at the workplace. European Industrial Relations Observatory. Available from: <<http://www.eiro.eurofound.eu.int/print/2003/07/study/TN0307101S.html>>.
- Department of Trade and Industry (DTI), 2002. Information Security Breaches Survey 2002. Available from: <<http://www.dti.gov.uk/>>.
- Department of Trade and Industry (DTI), 2003. Business in the information age—the international benchmarking study—2003. Available from: <<http://www.dti.gov.uk/>>.
- Desprochers, S., Roussos, A., 2001. The jurisprudence of surveillance: a critical look at the laws of intimacy. Working Paper, Lex Electronica 6(2), Available from: <<http://www.lex-electronica.org/articles/v6-2/>>.
- European Commission, 2002. Possible content of a European framework on protection of workers' personal data.
- Fazekas, P., 2004. 1984 is still fiction: electronic monitoring in the workplace and U.S. privacy. Duke Law & Technology Review 15. Available from: <<http://www.law.duke.edu/journals/dltr/articles/PDF/2004DLTR-0015.pdf>>.
- International Chamber of Commerce (ICC)—Commission on E-Business, 2003. IT and telecoms, employee privacy, data protection and human resources. Policy Statement.
- International Labour Office (ILO), 1997. Protection of workers' personal data. Geneva.
- Introna, L., 2000. Workplace surveillance, privacy and distributive justice. Computers and Society (Dec), 33–39.
- ISO/IEC, 2000. Information technology—code of practice for information security management. ISO/IEC 17799:2000(E), Geneva, Switzerland.

- International Working Group on Data Protection in Telecommunications (IWGDPT), 1996. Report and recommendations on telecommunications and privacy in labour relationships. Available from: <http://www.datenschutz-berlin.de/doc/int/iwgdpt/dsarb_en.htm>.
- Kesan, P., 2002. Cyber-working or cyber-shirking?: a first principles examination of electronic privacy in the workplace. *Florida Law Review* 54, 289ff.
- Klare, E., 1982. Critical theory and labour relations law. In: Kairys, D. (Ed.), *The Politics of Law*, New York, p. 62ff.
- Lasprogata, G., King, N., Pillay, S., 2004. Regulation of electronic employee monitoring: identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, United States and Canada. *Stanford Technology Law Review* 4. Available from: <http://stlr.stanford.edu/STLR/Article?04_STLR_4>.
- Lee, J., Lee, Y., 2002. A holistic model of computer abuse within organizations. *Information Management & Computer Security* 10 (2), 57–63.
- OECD, 1980. Guidelines governing the protection of privacy and transborder flows of personal data, Paris.
- Parent, W., 1983. Recent work on the concept of Privacy. *American Philosophical Quarterly* 20 (4), 341–355.
- Podlech, A., 1979. Das Recht auf Privatheit. In: Perels, J. (Ed.), *Grundrechte als Fundament der Demokratie*, p. 50ff.
- Porter, D., 2003. Insider fraud: spotting the wolf in sheep's clothing. *Computer Fraud & Security* 1 (4), 12–15.
- Rapport Auroux, 1981. Les droits des travailleurs, Rapport au président de la République et au Premier ministre, La documentation française, Paris.
- Schultz, E.E., 2002. A framework for understanding and predicting insider attacks. *Computers and Security* 21 (6), 526–531.
- Schwartz, P., Reidenberg, J., 1996. *Data Privacy Law*, Charlottesville.
- Simitis, S., 1987. Reviewing privacy in an information society, 135, *University of Pennsylvania, Law Review* 707 ff.
- Simitis, S., 1999. Reconsidering the premises of labour law: prolegomena to an EU Regulation on the protection of employees' personal data. *European Law Journal* 5, 45–62.
- UK Information Commissioner, 2003. *The Employment Practices Data Protection Code*.
- Watson, G., 2002. E-mail surveillance in the UK workplace—a management consulting case study. In: *Aslib Proceedings*, MCB UP Ltd. 54 (1), 23–40.
- Westin, A., 1967. *Privacy and Freedom*, New York.
- Whitman, M., Townsend, A., Aalberts, R., 1999. Considerations for an effective telecommunications—use policy. *Communications of the ACM* 42 (6), 101–108.