COMPUTER MONITORING IN THE 21ST CENTURY WORKPLACE

Prathiba Mahanamahewa

Course Director: Faculty of Law, University of Colombo

mahanamahewa@yahoo.com

94 1 2716210

Munidasa Kumaratunga Mawatha
Colombo 03
Sri Lanka

ABSTRACT

This paper attempts to lay the foundation for future research into an area that has been called the "hottest workplace privacy topic of the next decade." The existing empirical studies and the literature reviewed of this area suggest that the latest intrusive monitoring technologies which have been introduced to the current workplace has undoubtedly created an unwanted and unexpected imbalance and developed a wide gap in the 21st century employer/employee relationship. The paper argues for the introduction of Privacy enhancing technologies empowered with legal instruments in protection of workplace privacy. In addition, the paper is of the view that employees' awareness and training on workplace privacy policy developments are decisive factors to achieve this objective and this in turn creates trust and confidence and beneficial to both employees and employers in the current workplace. The paper proposes a contractarian framework to protect employers' interests and employees' on-line rights.

This paper suggests that employees' views and opinions are more important in computer monitoring to develop a privacy policy in the workplace. To attain these objectives an empirical survey was conducted in

five government sector organizations in Sri Lanka to gather factual information and to examine attitudes, beliefs and opinions on computer monitoring. The results of the study could be used as guide for policy-makers and for legislatures involved in drafting privacy legislation, and associated policies relevant to the workplace.

KEY WORDS

Electronic Privacy; Information Privacy; Data Protection; E-Policies; Workplace

COMPUTER MONITORING IN THE 21ST CENTURY WORKPLACE

1 INTRODUCTION

It is no secret that governments worldwide are going "online" (i.e., accessing the Internet and establishing Web sites) at a very rapid rate. The United States leads all countries with most of their agencies online. Canada and Australia online agencies follow the United States. In Sri Lanka, the government embarked on an ambitious program that established e-mail and Internet in all government sector organisations under the guise of World Bank in 2003. Under this project public sector employees are equipped with a computer and wide access to e-mail and Internet in the workplace. This transformation of workplace to on-line environment has raised numerous privacy related questions for both employers and the employees. In particular, the issue of e-mail and Internet usage and employee monitoring in the workplace is a significant matter. It was demonstrated here that many countries around the world are competing rapidly to maintain a policy to govern this issue in respect of employee privacy in the workplace. Finding the balance point for many public managers means developing, implementing, and enforcing an acceptable use policy for the e-mail and Internet. But what are the key components of such a policy? How and why do the components vary from organisation to organisation? This paper analyses the issue of electronic surveillance in the workplace and its impact on employee privacy rights. This paper will commence with a discussion of E-government and its various stations and in particular its implementation in Sri Lanka. It will then consider the information privacy as a human right in international and regional instruments. This will be followed by an evaluation of the regulatory framework for protection of privacy in United Kingdom and Sri Lanka. Finally it highlights the importance of an e-policy in an organisation to balance the competing interests of employer and employee.

2 E-GOVERNMENT

E-Government initiatives can be seen to operate at various levels (O'Flaherty, 2000). The first level comprises simple government to citizen communication through which government information such as reports, policy documents, legislation and case law is made available direct to the public through electronic means. In the second stage, citizen to government communication becomes possible allowing citizens to make electronic submissions concerning government proposals for example or to provide government agencies with new information about themselves, such as change of address, by electronic means. Third-level services facilitate more complex interactive transactions. These often involve legally binding procedures and/or online payments. Examples of such transactions include voter and motor vehicle registration or the submission of formal objections to applications for building permits. Fourth level services focus on the delivery of access to a wide range of government services across a whole government administration through a single contact point. At the fifth stage, yet to be fully realized in practice, government applications become intertwined with commercial applications and users are facilitated in building their own interfaces designed around their personal interactions with both government services and commercial entities.

3 INTERNET USAGE AND ELECTRONIC PRIVACY

There are four primary categories of Internet usage: sending and receiving electronic mail (Known as e-mail), accessing and posting documents on the World Wide Web, sending and retrieving computer files (known as file transfer protocol or FTP),and joining electronic discussion groups (such as news groups, listservs, and Internet relay chat groups). E-mail is the most widely used Internet service, although many users are active in all categories. In general the workplace presents a unique arena for privacy analysis. Two competing interests exist in the employment context: the employer's right to conduct business in a self-determined manner is matched by the employee's privacy interests or the right to be let alone.

For managers, monitoring is necessary. It is argued that workplace e-mail and Internet monitoring are the most effective means to ensure a safe and secure working environment and to protect employees. In addition, some contend that monitoring may boost efficiency, productivity and

customer service and allows more accuracy to evaluate performance (DeTienne, 1993; Sipior and Ward, 1995; Orthmann, 1998; Sipior et al., 1998). The impact of monitoring of these workplace relationships is the focus of this thesis. If used reasonably it may enhance efficiency without "trenching on" employees rights.

However, critics of monitoring point to research evidencing a link between monitoring and psychological and physical health problems, increased boredom, high tension, extreme anxiety, depression, anger, serve fatigue and musculoskeletal problems (Amick and Smith 1992; Kidwell and Bennett, 1994; Chalykoff and Kochan, 1989; OTA, 1987; Working Women Education Fund 9to5, 1990; Stanton, 2000). More seriously, critics point to violations of their fundamental right to privacy (Stone et al., 1983; Bylinsky, 1991; Culnan, 1993; Smith, 1993; Vest et al., 1995; Alge, 2001). Unless an acceptable remedy is soon found, workplace productivity may rapidly deteriorate and employee morale may disintegrate.

4 INFORMATION PRIVACY AS A HUMAN RIGHT

4.1 International Instruments

The most significant international human rights instrument is that of the Universal Declaration of Human Rights of 1948 (UDHR). Its provisions which deal expressly with privacy are set out in article 12, which states:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

In almost identical terms, article 17 of the International Covenant on Civil and Political Rights, 1966 (ICCPR) provides that:

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home correspondence, nor to unlawful attacks upon his honour and reputation.

Everyone has the right to the protection of the law against such interference or attacks.

4.2 Regional Instruments

Whereas the above provisions are framed essentially in terms of a prohibition on "interference with privacy", the equivalent provisions of

article 8 of the European Convention on Human Rights, 1950 (ECHR) are phrased in terms of a right to "respect for private life":

> Everyone has the right to respect for his private and family life, his home and correspondence.
>
> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The Charter of Fundamental Rights of the European, 2000 Union reaffirms the recognition of fundamental rights in the context of EU. Article 7 of the Charter states that

> Everyone has the right to respect for his or her private and family life, home and communication.

Article 8 of the Charter states that

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis for the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

The intention of the drafters of this article was to follow the traditional wording of article 8 (ECHR) while at the same time adapting the former to modern developments and technological change. This was done by replacing the term 'correspondence' (article 8, ECHR) with 'communications'. Article 7 guarantees protection against the intervention or interference of public authorities in the private sphere.

Article 8 of the Charter recognises Data Protection as an innovative fundamental right. The Draft Treaty establishing a Constitution for Europe ('European Constitution'), as proposed by the European Convention on the

Future of Europe reproduces article 7 of the Charter of Fundamental Rights under article 7 and article 8. Article 50 of the Draft Treaty is intended to establish a single legal basis for the protection of personal data, both for the protection of data which is processed by the European institutions. The protection of privacy may take on new meaning as a consequence of the Charter of Human Rights and the adoption of privacy provisions in a future European Constitution. Other than article 11 of the Inter-American Convention on Human Rights, the major regional human rights catalogue omits express protection for privacy or private life.

These international and regional instruments recognise privacy as a fundamental human and civil right. If article 12 of the Universal Declaration of Human Rights is taken in conjunction with article 8 of the Convention for the protection of Human Rights and Fundamental Freedoms, as well as with the concepts outlined by international organisations and individual countries, a fairly clear and broad definition of privacy can be identified, setting a standard of privacy that clearly protects the individual. That which is private should be respected, only to be breached in the case of very clearly set criteria, a notion reinforced with the European Convention of human rights. It is against these fundamental codes and declarations of human rights that this consideration of e-Work and monitoring is set. All actors considered are clearly covered by the definition and should, therefore, be respectful of and compliance with the protection provided by them. Although electronic surveillance is yet to be considered under the ICCPR, it has been taken up under the equivalent privacy right (article 8) contained in the ECHR, as well as in the draft European Constitution.

4.3 The Council of Europe and the Data Protection Directives

The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 seeks to protect individual rights and freedoms. The convention is particularly relevant because it provides for a right to privacy. In 1995, the European Union enacted the Data Protection Directive (95/46/EC) in order to harmonize member states' laws in providing consistent levels. The Directive provides for a basic or fundamental level of privacy that not only reinforces current data protection law, but also establishes a range of new rights. The twin objectives of the Directive expressed in Article 1 were: to protect the rights of individuals with respect to the processing of their personal data; and to

facilitate the free movement of personal data between member states. The first objective received much attention and it was the second that hold out the prospect of major economic benefit. The EU Directive (1995) is motivated by economic considerations, particularly the need to harmonise data privacy laws in the Union. However, the Directive also stresses the importance of fundamental human rights. The economic impact of the EU Directives has been far greater than any other instrument given its legal effect within the EU and its approach towards third countries. One of the fundamental economic objectives of the Directive was to enhance the free flow of data within the EU by removing barriers caused by internal borders.

In 1997, the European Union supplemented the 1995 directive by introducing the Telecommunications Privacy Directive (97/66/EC). On June 25, 2002 the European Union Council adopted the new privacy and Electronic Communication Directives (2002/58/EC). In the context of the spread of ICT at work and its associated risks, new concerns are arising in respect of the relationships between employers and employees to address these special issues related to workplace privacy. The European Commission is due to enact a Directive on workplace data protection in 2004 or 2005. The next section analyses information privacy defined in agreements of International organisation.

5 INTERNATIONAL ORGANISATIONS

5.1 Organisation for Economic Cooperation and Development (OECD)

In the late 1980s, the OECD issued a set of guidelines concerning the privacy of personal records. Although broad, the OECD guidelines set up important standards for future governmental privacy rules. Unsurprisingly, the organization had economic considerations in mind when it issued its guidelines. These guidelines underpin most current international agreements, national laws, and self-regulatory policies, and are voluntary and address the collection limitation principle, purpose specification principle, use limitation principle, openness principle and accountability principle. Clarke (1988) argues that the expression of privacy guidelines was shown to have been motivated by the protection of business activities, rather than of peoples privacy.

The primary reference for privacy protection is located in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980 and Implementing the OECD 'Privacy Guidelines' in the Electronic Environment: Focus on the Internet', Committee for Information, Computer and Communications Policy. This instrument is a set of guidelines. It is not a convention; and it merely "recommends" that member countries consider the principles into their domestic legislation. Greenleaf (1996) contends that existing legislations having incorporated privacy guidelines do not provide sufficient protection against new monitoring technologies coupled with highly bureaucratic administrative practices.

5.2 International Labour Organisation (ILO)

The ILO has no convention to protect privacy but has adopted a Code of Practice on Protection of Workers Personal Data 1997, which covers general principles about protection of personal data and specific provisions regarding the collection, security, storage, use and communication of such data. Unlike other ILO instruments, the code is not legally binding like other international treaties. It provides employers and workers with the basis for rules to be designed by them. The code was intended to provide guidance in the development of legislation, regulations, collective agreements, work rules, policies and practical measures in the workplace.

According to an ILO survey (ILO, 1993), workers in industrialized countries are gradually losing privacy in the workplace as technological advances allow employers to monitor nearly every facet of time on the job as a remedial measure and to protect employee privacy. The ILO introduced, therefore, guidelines on employee monitoring at the workplace. To further protect workplace privacy the ILO introduced a code of practice called the Protection of Worker's Personal Data (1997). Its purpose is to provide guidance on the protection of workers personal data and is not as a binding force. The code does not replace national laws, regulations or other accepted standards. It can be used in the developments of legislation, regulations, collective agreements, work rules, policies and practical measures at enterprise level. According to the ILO Code, secret monitoring is permitted only if there is suspicion on reasonable grounds of criminal activity or other serious wrongdoing. The ILO recognises that workers rights to privacy should be treated as a fundamental human rights issue, but the new technology can pose dangers to privacy, even as it is improving all

of our lives. The ILO calls the problem the "chemistry of intrusion", a combination of threats to informational privacy, increasing encroachments on physical privacy and increased physical surveillance.

There is a certain consistency among these principal instruments. Each seeks to establish consistent rules to protect the recognized right to privacy in order to pre-empt incompatible national rules that would damage the economic benefits of free flow of information.

It is now a quarter of a century since key data privacy instruments were adopted by the OECD (1980) and Council of Europe (1981). These were followed by the United Nations Guidelines (1990) and EU Directives (1995). Most of these instruments have had reviews of one or another sort. Nonetheless, there are people who wonder whether the various national laws, and these instruments, really achieve their objectives of protecting privacy and whether achieving the supposed benefits is worth the cost. The time to define the exact nature and extent of privacy protections is long overdue. Unless privacy is asserted as a human right, fundamental protections for individuals and institutions will decline leading to a breakdown of social and economic processes.

The EU Directives requires that "Each member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of provisions adopted by the Member states pursuant to the Directive" (EU 1995, Article 28.1). The OECD Guidelines fail to require the creation of privacy protection agency. However, the public expectation is that a specialist body will exist to supervise government agencies and corporations, and the OECD Guidelines fail to fulfil that expectation. The OECD Guidelines fail to specify the measures needed to ensure that privacy protection regime is achieved. The OECD Guidelines appear to be silent on this matter. They clearly need to be enhanced to require the privacy protection agency to make the maximum information available to the public, and to establish working relationships with privacy advocates and representatives of the public. Therefore, need to define a new the exact nature and extant of privacy protections.

6 LEGISLATION TO PROTECT PRIVACY IN UNITED KINGDOM

The UK does not have a written constitution. Nor, until recently, could it be said to recognize a generic concept of "constitutional rights". The Human

Rights Act 1998 (UK), which came into force on 2 October 2000, recognizes a right to privacy. Article 8 has broad application, and provides a concrete right for individual at work. In the absence of any widespread recognition of a common law tort of invasion of privacy, several British legislatures have attempted to create a statutory protection of privacy. Workplace privacy is regulated by two sets of legislations. Namely, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Data Protection Act 1998 (DPA). The main purpose of the Regulation of Investigatory Powers Act (RIPA) 2000 is to ensure that the relevant investigatory powers are used in accordance with human rights. The data Protection Act 1998, designed to implement EC Directive 95/46 on personal data, came into effect in March 2000, and establishes a separate statutory regime which governs the "processing" of "personal data". Therefore, even if employers obtain personal data as a result of an interception authorised under the Regulation of Investigatory Powers Act (or outside the scope of that Act), they must also ensure that they comply with requirements of the data Protection Act.

7 IS THERE ANY LEGAL PROTECTION FOR DATA PRIVACY IN SRI LANKA?

The concept of privacy is not clearly defined unlike the European Union, where most people seem to know what to expect, which makes the work of the judicial bodies easier as issues of interpretation are quickly settled. Conventionally, general privacy concerns have been addressed through the law of torts (breach of confidentiality, trespass and nuisance) and criminal law. Like many other Commonwealth countries the common law of Sri Lanka is based on principles of English law. In addition, some of the principles of law of contract are governed by Roman-Dutch law like in South Africa. The lack of a framework on data protection prevents e-business from the European Union and affects Sri Lanka's economy. Therefore, privacy norms and procedures are expected to arrive from the United Kingdom.

Therefore, legislative measures or other measures, such as the adoption of "Codes of Practice", embodying privacy principles would ensure workplace privacy protection on employees' personal information. This would mean that Sri Lanka is in a similar position with the West. The

question remains whether these arrangements can meet the extra demands brought about by electronic communications.

Information about an individual's tastes and leisure activity has economic value, and the exchange of such information helps to grease the economy. Sri Lanka has never banned the sale of such data, despite the potential impact on privacy. There are, however, many different levels of legal protection for privacy when websites and e-commerce firms, without consent, use private information for commercial purposes. No comprehensive protection exists. In many countries there is a general law that governs the collection, use and dissemination of personal information by the public and private sectors. An oversight body then ensures compliance. This is the preferred model for most countries adopting data protection laws and was adopted by the EU to ensure compliance with its data protection regime.

8 E-POLICIES

Organisations without such policies run the risk of being sued for actions of an employee. Policies "create clear standards to prevent employment disputes and ensure consistent supervisory administration of employment relations". The specific policy selected depends on the culture of the workplace, but most policies have common elements.

The common policy components are:

- Cautioning employee about the risks of using e-mail and the Internet.
- Informing employees:
  - that e-mail is irretrievable
  - that Internet activities can be traced by third parties
  - of downloading procedures and the risk of viruses
  - of all prohibitions of inappropriate and illegal uses
  - that the employer can be held liable for activities of the employee, and
  - that their electronic actions can be so identified with the employer.
- Include information designed to curtail employee conduct for which the company may be liable, namely: defamation, harassment, and discrimination; copyright and patent infringement.
- Establish limits on what may be downloaded from the Internet or exchanged via e-mail.

- Remind users that text, graphics, and software that appear to be freely available on the Internet are often subject to intellectual property laws that limit copying, distribution, and use.
- Confidential Information
- Use technological means to prevent trade secret and confidential files from being transmitted.
- Mandate the use of encryption software or ban the transmission of sensitive information altogether.
- Create an approval and clearing policy for information to be published on the web
- Establish monitoring procedures and inform employees about the details of such monitoring
- If applicable, clarify that incidental personal use is a privilege, which can be revoked for abuse or excessive use.

9 CONCLUSION

It is well established that neither constitution nor statutory law addresses the new privacy issues associated with technology and the old common law does not clearly cover the area of privacy in question in Sri Lanka. Therefore a gap exists between the time when a new communication technology is created and the time when a statute is designed by state legislature to cover the new technology. This paper contends that a modern computerised workplace reduces the arbitrary powers enjoyed by the employers and reduces their ability to act against the employee unilaterally and effectively. Hence, we can design a incentive-compatible, benefit maximising contact between managers and employees based on the following principles: employee participation in defining privacy policies; full disclosure of all implementation schemes pursuant to these policies; and employer monitoring to ensure compliance with such policies. Finally, this has been endorsed by the Article 29 – European Union Data protection Working Party (Article – 29 EU Data Protection Working Party, 2002, p.24) in their statement specifically: “A blanket ban on personal use of the Internet by employees may be considered to be impractical and slightly unrealistic as it fails to reflect the degree to which the Internet can assist employees in their daily life”.

10 REFERENCES

O'Flaherty (2000) 'Privacy Impact Assessments: an essential tool for data protection' A presentation to a plenary session on New Technologies, Security and Freedom' at the 22nd Annual Meeting of Privacy and Data Protection Officials held in Venice, September 27-30 2000.

DeTienne, (1993) "Big brother or friendly coach? Computer monitoring in the 21st century" The Futurist, Vol. 27, p. 33.

Sipior and Ward, (1995) "The ethical and legal quandary of email privacy" Communications of the Association for Computing Machinery, Vol. 38, p. 8.

Orthmann, (1998) "Workplace computer monitoring" Employment Testing - Law and Policy Reporter, Vol. 12, p. 182.

Amick and Smith (1992) "Stress, computer-based work monitoring and measurement systems" Applied Ergonomics, Vol. 23, p. 6.

Kidwell and Bennett, (1994) "Employee Reactions to Electronic Control Systems" Group and Organization Management, Vol. 19, p. 203.

Chalykoff and Kochan, (1989) "Computer-aided monitoring: Its influence on employee job satisfaction and turnover" Personnel Psychology, Vol. 42, p. 807.

OTA, (1987) Office of Technology Assessment. (1987) The electronic supervisor: New technology, new tensions (U.S Government Printing Office: Washington DC).

Working Women Education Fund 9to5, (1990) "Stories of mistrust and manipulation: The electronic monitoring of the American workforce" (Author: Cleveland, OH).

Stanton, (2000) "Reaction to Employee Performance Monitoring: Framework, Review, and Research Directions" Human Performance, Vol. 3, p. 85.

Stone et al., (1983) "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations" Journal of Applied Psychology, Vol. 68, p. 459.

Bylinsky, (1991) "How companies spy on employees" Fortune, Vol. 124, p. 131.

Culnan, (1993) "How did they get my name? An exploratory investigation of consumer attitudes toward secondary information use" MIS Quarterly, Vol. 17, p. 341.

Smith, (1993) "Privacy policies and practices: Inside the organizational maze" Communications of the ACM, Vol. 36, p. 105.

Vest et al., (1995) "Factors influencing managerial disclosure of AIDS health information to co-workers" Journal of Applied Social Psychology, Vol. 25, p. 1043.

Alge, (2001) "Effects of Computer Surveillance on Perceptions of Privacy and Procedural Justice" Journal of Applied Psychology, Vol. 86, p. 797.