On-line Rights for On-line Workers

Dr. Prathiba Mahanamahewa, Attorney-at-Law, Dean Law, Kotelawala Defence University, Senior Lecturer in Law, Colombo University, Commissioner, Sri Lanka Human Rights Commission

ABSTRACT

Privacy in the work place is an emerging legal issue. As technology becomes faster and cheaper, concerns about workplace privacy issues continue to mount. The impressive advancements in computer communications have created many new problems. Employers are increasingly adopting the practice of monitoring employee use of e-mail and the Internet in the workplace. This paper aims to address impact of employee privacy rights in such a monitoring and to propose a policy with regard to workplace monitoring in the information digital age and to analyze the legal rules regulating the operation of electronic monitoring in the workplace.

INTRODUCTION

The employee Internet and e-mail monitoring at private/public workplace is a burgeoning area because of rapid development of the use of electronic on-line communications in the digital information age and it is timely relevant to investigate its operation and legal rules that apply to electronic monitoring in the public/private workplace. Laws protecting the use of e-mail and Internet in the workplace are still developing; employees have no reliable defense against the monitoring of their e-mail messages, yet the employers should provide the workforce with their e-mail policies. Many important questions about respective employee privacy rights remain unanswered. More laws are being developed to protect both employers and employees. Until such laws are completely developed, few temporary available options remain. At the present time there is little information on how employee e-mail and Internet monitoring carry out in the public/private workplace.

Back Ground To The Problem & Previous Studies

The use of Internet and e-mail by the Sri Lankan government departments have been rapidly increased over the past few years, with recently launched e-government program to enhance on-line public service for the citizens without any delay. Most of the government institutions in Sri Lanka are connected to Internet with high computer use. Therefore it's the correct time for Sri Lanka to review and reform the law to face new challenges posed by electronic revolution.

Research into the legal regulation of the use of employee e-mail and Internet monitoring and surveillance is important because there has been a distinctly discernible rise in the use of e-mail and Internet by employees in the workplace. According to a worldwide survey on e-mail and Internet usage at workplace conducted by the Privacy Foundation in the year 2001 revealed that the usage of e-mail and Internet increased by 25 percent on one hand and on the other side monitoring of their staff too increased by 30 percent. Another survey conducted by Websense International in the year 2002 revealed that Internet misconduct n the workplace is being decisively dealt with in the

UK as quarter of UK companies have dismissed for the abuse, with nearly 70 percent associated with Internet pornography. Up till now there has been very little if any legal analysis of employee electronic monitoring to determine whether the present legal rules affecting electronic monitoring are adequate, and whether there are weaknesses in the present legal approaches.

Reasons For Employer Monitoring Of Employees

Employers argue that workplace e-mail and Internet monitoring is the most effective means to ensure a safe and secure working environment and to protect their employees. In addition some contend that monitoring may boost efficiency, productivity and customer service and allows to more accuracy evaluate performance. Also monitoring avoids misuse of the employer's equipment and prevents oversized e-mails clogging up network space

Employee Privacy Concerns

Critics of monitoring point out to research evidencing a link between monitoring and psychological and physical health problems, increased boredom, high tension, extreme anxiety, depression, anger severe fatigue and musculoskeletal problems one hand and more seriously violation of their fundamental right to privacy. Unless a legal remedy is soon found, employees feel a lack of respect from their employers, which may turn affect productivity or the culture of the workplace. Employer policies in this area are relatively scarce, also owing to the infancy of the issues. A survey conducted by American Management Association in the year 2000 revealed about 80 percent of firms provide e-mail systems to their employees, the survey suggests that only about one-third of firms with e-mail in place have a policy regarding review of that email. Also, absence of appropriate law is, in itself an impediment to the structuring of employee online monitoring through predictability.

Nature Of Monitoring

Over the past few years Internet and e-mail has increasingly become the primary form of communication in the business world, especially in the service sector. Therefore in today's technological society, it is too easy for employers to carry out pervasive surveillance of employee activity by electronic means, and such practices have potentially serious implications for employee privacy. The right to privacy is at core of this employee monitoring issue. There is a distinctive difference between 'over the shoulder' or 'walk around' monitoring and electronic monitoring. In the former, employees being monitored are aware of the supervisor's activity from the beginning to end. In the later, they are aware of the monitoring only if a deliberate signal is given. While the former is visible or audible, the latter is not. Employers regard the lack of awareness of the employees as an advantage of electronic monitoring.

Lack Of Legislative Protection For Employee Privacy

Countries have addressed this emerging legal issue of workplace privacy in different ways. In the United States with few privacy and data protection laws, relies mostly on self-regulation

and limited legislation. Many European countries have created stringent privacy laws. Germany, France, Netherlands and the United Kingdom are known for their particularly rigorous privacy laws. To standardize the protection of data privacy, the European Union in 1995 enacted the EU data protection directives (95/46/EU) that took effect in 1998. Most of the EU countries based their data protection at on these directives to provide adequate protection of data privacy.

These different approaches are legitimate as they reflect the needs of the respective countries. It is therefore necessary to examine what Sri Lanka's approach should be sit its economic, social and cultural environment.

International Agreements To Protect Privacy

There are three principal international agreements, which are of general relevance to information privacy: the Organization for Economic Cooperation and Development's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, The Council of Europe Convention on data protection and the International Covenant on Civil and Political Rights (ICCPR) (and its European equivalent) apart from theses agreements European Union Privacy Directives protect information privacy.

The Law, New Technology, and Workplace Privacy in Sri Lanka and United Kingdom

SRI LANKA

Constitutional Protections

The 1978 Constitution of the Democratic Socialist Republic of Sri Lanka does not explicitly recognize the right to privacy as a basic fundamental right. Though 1997 and year 2000 proposed constitutions contained right to privacy as a fundamental right. Therefore unlike U.S.A there is no reasonable expectation of privacy against intrusions by the state.

Legislations

Yet the government has not introduced any specific legislation, which protects the individual privacy or collection of personal information. The only legislation, which refers to this area, is the Telecommunication act on interception of communication.

Common Law

Under the common law the employer employee relationship is a contractual one. And may include a clause relevant to electronic monitoring. Another aspect is that the information, which is confidential, will be protected by the action for breach of confidence if it is disclosed in circumstances, which expressly or by implication create an obligation of confidence.

Labour Law

Collective agreement may include a clause relevant to e-mail and Internet monitoring in the workplace.

Case Law

There are very few cases related to individual privacy and not on workplace privacy or information privacy. The case of *Hewamanna v Attorney-General (1999)*; challenging the constitutionality of the proposed postal corporation bill the Supreme court decided that the postal corporation bill creating excessive powers for interception of communication and therefore ruled out as unconstitutional because it affects the individual privacy. In *Sunday times Defamation case (2000)* the Court of appeal pointed out that the press should not think they are free to invade the privacy of individuals in the exercise of their constitutional right to freedom of speech and expression, merely because the right to privacy is not declared a fundamental right of the individual, However to appreciate the value of privacy in the life of an individual, it is well to remember the importance which our constitution attaches to the man's autonomous nature, through the guarantees of basic human right. And these human rights are aimed at securing the integrity of the individual and his moral worth.

United Kingdom

The principles of European Convention for the Protection of Human Rights in to the UK law incorporate in the Human Rights act 1998, The Data Protection act 1998 which incorporates Directives 95/46/EU, Regulatory of Investigatory Powers Act 2000 and Telecommunications (Lawful Business Practice) regulation 2000 protect public employee privacy rights in the workplace. More recently UK information Commissioner issued code of practice of employee monitoring in the workplace to more strengthen to employee workplace privacy rights. Therefore every employer has to comply with these guidelines once they implement an electronic monitoring in the workplace.

Case Law in United Kingdom

It has already been established that the privacy rights enshrined in the European Convention on Human Rights are not limited to people's home lives: they can also extend to their place of work. In *Niemietz v Germany* and *Smith & Grady v UK* it was decided that the individual privacy rights extend to workplace.

A draft code of conduct for the protection of privacy at work

Any code of practice should comply with the data protection principles and privacy principles contained in the 1997 International Labour Office's "Code of Practice on the Protection of Workers' Personal Data," which protect employees' personal data and fundamental right to privacy in the technological era.

The General Principles Of The ILO Code Are

Personal data should be used lawfully and fairly: only for reasons directly relevant to the employment of the worker and only for the purposes for which they were originally collected;

Employers should not collect sensitive personal data (e.g., concerning a worker's sex life, political, religious or other beliefs, trade union membership or criminal convictions) unless that information is directly relevant to an employment decision and in conformity with national legislation;

Polygraphs, truth-verification equipment or any other similar testing procedure should not be used;

Medial data should only be collected in conformity with national legislation and principles of medical confidentiality;

Genetic screening should be prohibited or limited to cases explicitly authorized by national legislation; and drug testing should only be undertaken in conformity with national law and practice or international standards;

Workers should be informed in advance of any advance monitoring and any data collected by such monitoring should not be the only factors in evaluating performance;

Employers should ensure the security of personal data against loss, unauthorized access, use, alteration or disclose; and

Employees should be informed regularly of any data held about them and be given access to that data.

The code does not form international law and is not binding effect. It was intended to be used "in the development of legislation, regulations, collective agreements, work rules, policies and practical measures."

Draft Code of conduct

Any code of conduct on employee e-mail and Internet monitoring must adherence to the following principles: -

Personal data shall be processed in accordance with the law and in a proper and careful manner.

Personal data shall be collected for specific, explicitly defined and legitimate purposes.

Personal data may only be processed where: the data subject has unambiguously given his consent for the processing

Personal data shall not be further processed in a way incompatible with the purposes for which they

have been obtained.

Personal data shall not be kept in a form which allows the data subject to be identified for any longer than is necessary for achieving the purposes for which they were collected or subsequently processed.

Personal data shall only be processed where, given the purposes for which they are collected or subsequently processed, they are adequate, relevant and not excessive.

It is prohibited to process personal data concerning a person's religion or philosophy of life, race, political persuasion, health and sexual life, or personal data concerning trade union membership, except as otherwise provided.

This prohibition also applies to personal data concerning a person's criminal behavior, or unlawful or objectionable conduct connected with a ban imposed with regard to such conduct.

The policy should set out the employer's security procedures.

Workplace policies should be communicated to employees in plain English. They should be updated and re-circulated on a regular basis.

Employers should not engage in blanket monitoring of the contents of emails or Internet sites visited by employees. As an alternative, employers may monitor the traffic data, the time and number of communications.

Resolution?

I passionately believe that there is a balance possible between workers and employers-not simply in the privacy/monitoring debate, but in many of the ethical challenges presented by new technological advances. Ultimately, employees and employers share a common vision with regard to the purpose of work and of the market in general. When the personal interests of both sides are considered, viable alternatives emerge. From the employees' perspective, a resolution that would respect their personal autonomy by providing for personal space, by giving notice of where that space ends, by giving them access to and the right to change or correct the information gathered, and by providing for monitoring that is directed toward the personal development of the employee and not merely to catch wrongdoers. From the employer's perspective, this balance offers a way to effectively but ethically supervise the work done by their employees. It protects the misuse of resources, while also allowing them to better evaluate their workers and to encourage their workers to be more effective.

Conclusion

The issue of email and Internet monitoring in the workplace provides a prime example of a recent technological development, which potentially has a huge impact on individual privacy rights. Employees have a right to expect a certain degree of privacy in relation to email and Internet use. Any monitoring of electronic communications in the workplace should be proportionate to the severity of the risk faced by the employer. All employees are entitled to expect that their fundamental right to freedom and privacy will, to a certain extent, be respected in the workplace. After all, employees are spending more time at work than ever before and it is within the course of their working lives that employees have the most significant opportunity to develop social connections. The gist of my argument has been that we need more law. The 1978 Constitution or any legislation currently

existing in Sri Lanka has not developed its potential to protect privacy. We need changes to our laws and this is the ideal time to introduce a Data Protection Act to balance employer interest and employee privacy rights in Sri Lanka.

REFERENCES

Charlesworth, Andrew, 'Implementing the European Union Data Protection Directive 1995 in UK Law: The Data Protection Act 1998' (1999) 16(3) *Government Information Quarterly* 203

Jankanish, Michael, 'Monitoring and Surveillance in the workplace: Privacy issues in an international perspective' (International Labour Organization, 1993)

Kabay, M.E., 'What are employees' right to privacy in e-mail', Network World Security Newsletter 2002.

Leenknegt, G., 'The protection of Fundamental Rights in a Digital Age' (1999) 6(4) *European Journal of Comparative Law* 1.

Kovach, K, Jordan, Jennifer, 'The Balance Between Employee Privacy and Employer Interests' (2000) 105 (2) *Business & Society Review* 1.

The Information Commissioner, United Kingdom, 'The Employment Practices Data Protection Code' (Office of Information Commissioner, 2002)

Gorman, John, 'Monitoring Employee Internet Usage' (1998) 7(1) *European Review* 21

Shaffer, Gregory, 'The power of EU Collective Action: The Impact of EU Data Privacy Regulation on US Business Practice' (1999) 5(4) *European Law Journal* 419

R.C, Linowes, D.F Spencer, 'Privacy in the Workplace in Perspective' (1996) 6(3) *Human Resource Management Review* 165

S, Loch K.D; Conger, 'Ownership, Privacy and Monitoring in the workplace: A debate on Technology and Ethics' (1998) 17(6) *Journal of Business Ethics*

Smith, David, 'Monitoring in the Workplace Conference' (Paper presented at the Data Protection Act 1998: Related Paper, Bridgewater Hall, Manchester 2001)