Conclusion

Inline with Sharma's theoretical model, Holcim Lanka fosters opportunity-seeking, risk-embracing managerial interpretations towards environmental issues faced by the Sri Lankan cement manufacturing industry. These managerial interpretations are influenced through Holcim Lanka's organizational context which in turn facilitates the corporate choice of a voluntary-based environmental strategy. Therefore, it is clear, that there is a direct link between managerial interpretations and the nature of the environmental strategy adopted by Holcim Lanka Limited.

However, this move is highly influenced by Holcim Group rather than Holcim Lanka's voluntary initiative. Being a member of a MNC based in Europe enables Holcim Lanka to comply with stringent, globally applied standards and regulations in order to stay at the forefront of the local competition adopting a voluntary environmental strategy. Therefore, from Holcim Group's point of view, the managerial interpretations formed in Holcim Lanka enable the company to stay abreast with the group's companies worldwide adopting more of compliance-based environmental strategy. Hence, even though Sharma's theoretical model could be successfully applied in Sri Lankan context, it should consider situational factors in determining the organizational context that influence managerial interpretations towards corporate choice of environmental strategy.

Privacy protection and security of on-line data in a modern technological era *1

Seuwandhi B. Ranasinghe
Temporary Assistant Lecturer,
Department of Management & Organization Studies,
Faculty of Management and Finance

Introduction

Employees in all over the world are exposed to many types of privacy-invasive monitoring while earning a living. These include closed-circuit video monitoring, Internet monitoring and filtering, E-mail monitoring, instant message monitoring, phone monitoring, location monitoring, personality and psychological testing, and keystroke logging. Employers do have an interest in monitoring in order to address security risks, sexual harassment, and to ensure the acceptable performance of employees. However, these activities may diminish employee morale and dignity, and increase worker stress.

Today, the workplace privacy issues are mostly combined with on-line data protection as the whole world depends on knowledge and data. Nearly every daily routine can be carried out through or with the help of technology. Doing this, we also contribute to the flow of data, in particular over networks such as the internet. Everywhere we go, we leave traces thereby making it possible for anybody interested enough to collect, organize and analyze our personal data.

This article is intended to critically analyze the issues that have arisen from the law and practice governing privacy protection and security of on-line data. Indeed, it will be dealt with the practical issues relating to privacy implementation through self-regulation and dispute with the some human rights. The last parts of the article will draw attention to contemporary challenges and possible suggestion for the developing countries like Sri Lanka to develop a piece of law specially analyzing the above mentioned issues of online data protection.

Privacy and its importance in on-line

Privacy can be defined as right to be let alone though it has definitional variations. In today's context, it is very important with regard to the protection of on-line data. The spread of the internet and the seemingly borderless options for collecting, saving, sharing, and comparing information has triggered some of the neo-native problems in data protection. Furthermore, *wed hugs, cookies, spyware, botnets* and *phishing* are some ways that invasion of on-line privacy can be happened.

Methods of protection

There are four major models for privacy protection. Depending on their application, these models can be complementary or contradictory. In most countries reviewed in the survey, several models are used simultaneously. In the countries that protect privacy most effectively, all of the models are used together to ensure privacy protection. EU countries mostly rely on **comprehensive laws** such as Data Protection Acts on other hand in many countries, **sectoral laws** are used to complement comprehensive legislation by providing more detailed protections for certain categories of information, such as telecommunications, police files or consumer credit records. Data protection can also be achieved, at least in theory, through various forms of **self-regulation**, in which companies and industry bodies establish codes of practice and engage in self-policing. With the recent development of commercially available **technology-based systems**, privacy protection has also moved into the hands of individual users.

Existing legal framework

When discussing the existing legal framework of protection mainly it can be indentified in three different layers namely, international protection, regional framework and local framework of protection. International protection is based on human rights point of view though the regional protection in particularly EU is based on both comprehensive and sectoral protection.

The Sri Lankan government has not yet introduced any specific legislation that protects individual privacy or collection of personal information. Mainly, the common law remedy called *'Actio injuriarum'* addresses the issue indirectly. The only legislation that refers to this area is the Telecommunication Act No. 27 of 1996, which regulates the interception of communications.

The rapid developments in information and communications technologies in Sri Lanka have significantly affected the current legal system. The absence of a data protection authority in Sri Lanka is a real threat to the protection of on-line data which can be easily accessed and stored. The government is currently in the preliminary stages of introducing a new data protection law to ensure the privacy of individuals and information, and the confidentiality, availability and integrity of information and the integrity of transactions.

The Parliament passed the Information and Communication Technology Act No. 27 of 2003 to provide for the establishment of a national policy on information and communication technology and for the preparation of an action plan. The Computer Crimes Act, No.24 of 2007, also provides a basis for protection. The Act addressed computer misuse; unlawful obtaining of data[9]; cyber-stalking; unauthorized disclosure of confidential information[10] and illegal interception of data.[11] These are important provisions which are to ensure privacy and integrity of subscriber information, traffic data and communication that is being held in computers or transmitted via computers and information and communication technology.[12]

A scrutiny of the issue

Though Sri Lanka has not a sound and unique way of protection on-line data, there is a compelling need to introduce such law in modern technological era. However, when creating a new law, it should be emphasized the polycentric nature of the issue. Furthermore, after 9/11 the data protection issues became much more crucial as the security concerns overtook the individual rights. In the context of fast-moving technology there is a need of refining the laws though we enact a law in future. Therefore it is suggested to have, self-regulation system of on-line data protection where the private sector can implement their own policies to address the issue. Even then, that also subject to criticized as the employer always have bargaining power than the employee. This will empower them to add unfair terms relating to privacy issues to the employment contract.

Conclusion

It is undeniable that, privacy issues and online data have enormous economic values and a lot of implications in our day. Therefore, right to privacy in online should be protected but it should not be an absolute protection as the issue has more than one human right dimension. Under the circumstance, the promotion of a self-regulation would be better but at the same time the establishment of a government regulatory body is essential to scrutinize the situation as a watchdog while adopting a mechanism for public awareness.

---

1 W. A.D.J. Sumanadasa (*Attorney-at- Law*), Assistant Lecturer, Department of Management and Organization Studies, Faculty of Management and Finance, University of Colombo.

2 Section 7

3 Section 10

4 Section 8

5 Selvakkumaran N, *The legal regime governing computer crimes; an appraisal of the Sri Lankan Law*, Academic Conference on "Law in Context: An agenda for Reform", Faculty of Law, University of Colombo, 24th October 2008