Abstract

This paper examines the extent to which the basic principles of data protection laws may be read into provisions in human rights treaties proclaiming a right to privacy. The problems caused by the difference between the USA and EU approaches to data protection are highlighted. The paper documents some of the legislative developments mean for E-Business and the link between data captured, stored and processed into information and the resulting effect on privacy is important. This article further argues in Sri Lanka the Information Privacy should be constitutionally protected and the law should be based on a EU model considering EU derivatives (1995/EC/46).

1. Introduction

According to the United Nations Conference on Trade and Development (UNCTAD), E-commerce and Development report of 2002, revealed that the global number of Internet users is expected to reach 655 million by the end of 2002. (Compared to 500 million at the end of year 2001.) An emerging feature of this report is that during last year a growing share of new Internet users was found in developing countries, accounting for nearly a third of new Internet users worldwide. In Sri Lanka during 2002 there was nearly a 25 percent increase of the Internet usage, compared to the year 2001. Internet usage is having an annual rise of about 30 percent, which is equivalent to about 2.5 percent of the global population. The report further states that the world’s largest e-commerce market has experienced a mild recession in 2002 [1]. When analyzing reasons for this decline, several surveys conducted in New Zealand, Australia and U.S.A, revealed that there is a great fear among the consumers about feeding their personal information to computers for e-business. Is their personal data adequately protected and well secured? If this fear continues in future it may badly affect the e-business development. This paper discusses the law relevant to data protection giving special attention to Sri Lanka.

2. Why do Countries Enact Data Protection Legislation?

The most commonly stated motive for data protection legislation is to protect individual privacy from being compromised by computerization and to provide a framework for finding a balance between the interests of the individual, the data user, and the community at large. The 1981 Council of Europe Convention on Data Protection forms the basis of all national legislation within Europe. The U.K. Data Protection Act 1998 was with a view of protecting private individuals from the threat of the use of erroneous information regarding them, or the misuse of correct information about them held in computers. This satisfied the Council of Europe Convention on Data Protection, and enabled the U.K. data processing industry to participate freely in the European market. India is ready with their draft of the data protection act and is planning to enact legislation in the coming winter session of the parliament.

It has been revealed that the countries without a data protection law may lose business especially from Europe because the EU Directive on the Protection of Personal Data prohibits the transfer of personal data to non-EU countries that do not meet the European “adequacy” standard for data protection. As a result, this Directive also places important burdens on Sri Lanka and other countries that collect personal data online. The absence of data privacy legislation in India has proved to be a handicap to Europe and U.S.A to carry on business processes with India and Indian companies.

3. What is Data Protection?

Providing a definition for data protection is as difficult as finding the reason for its existence. It is the legal protection of individuals with regard to automatic processing of personal information relating to them. Therefore not only should there be a clear balance between data users and data subjects, but also a scale of values attached to any individual [2].
4. Why Data Protection Law Needs at this Hour?

The use of Internet and e-mail by the Sri Lankan government sector and the private sector has been rapidly increased over the past few years. They have launched an e-government project to deliver accurate and prompt services to the public. Most of the government institutions in Sri Lanka are connected to e-mail and Internet associated with a high computer use. Sri Lanka has to face these new challenges posed by the electronic revolution to protect individual privacy of processing their personal information. In many countries including Sri Lanka, laws have not kept up with the technology, leaving significant gaps in protection. In other countries, law enforcement and intelligence agencies have been given significant exemptions. Therefore the mere presence of law may not in fact provide adequate protection.

5. What is E-Government?

E-government is all about government agencies working together to use technology so that they can provide individuals and the business sector with better government services and information. It is not a massive Information Technology (IT) project. Much of it is about establishing more effectively common standards across government, delivering services, and providing better ways for agencies to work together, using technology. E-government can enhance the citizen’s access to government information and services, and can provide new ways to increase citizen participation in the democratic process and in building a knowledge-based economy with sustained prosperity.

E-government makes it easier to do business with government. It also makes it cheaper. In Australia it has been estimated that it can cost as little as $1-7 each time you use a service online. This compares with $2-200 to deliver the same service over the counter, by mail or telephone, or even by sending out a brochure.

Businesses will find it much easier to work with government organizations than they do today. They will specially notice the reduced cost of dealing with government. Business people will also be able to find the right information and regulations. They will also be able to conduct the related transactions quickly and in an integrated way. By encouraging use of the Internet, e-government will indirectly foster opportunities for business to develop their online services and would be a real boost for a business with a small workforce.

6. What will E-Government Mean for Small and Large Business Ventures?

A significant benefit for business will arise from the participation of government in the information economy. While the focus of this program is on taking government online, the effect will be to stimulate and to move a critical mass of Sri Lanka business services online. This would make a positive impact on for our ability to operate in the global economy.

7. What is E-Business?

The convenience, availability and worldwide reach of E-business enhances existing business or creating a new virtual business. IBM defines e-business as “a secure, flexible and integrated approach to delivering differentiated business value by combining the systems and processes that run core business operations with the simplicity and reach made possible by Internet technology”. E-commerce is just one aspect of e-business like e-franchising, e-mailing, e-marketing, e-business, the Internet, and globalization all depending on each other. The more global players exist the more e-business would want to play its part. The more e-business is on-line, more people will be attracted to get direct Internet access. The more people are online more global players will arise.

8. The Relationship Between E-Government, E-Business and Data Privacy

Online business or online delivering public services, means feeding personal data to the computer. These data are transmitted from one place to another place. When this is being done the data collectors, service providers or data registers are involved in this activity. The personal data of customers and citizens should thus be protected by law without keeping any room for manipulation, possible misuse or unauthorized disclosure to a third party.

9. Threats to Personal Privacy

Consumer awareness about privacy is increasing, particularly among Internet users. Sooner or later, consumers will demand that their privacy be respected. This may require some modification to business practices and customer service and may even involve costs not previously incurred. Even American big business has accepted that privacy is a concern, which must be addressed. All the public surveys conducted by, and for big business in America, showed a lack of confidence in that consumer’s personal information may not be protected if they entered into transactions on the Internet.
Privacy concerns have thus been clearly identified as a barrier to the development of e-business [3].

Firstly, personal information that an individual would prefer not to disclose to others, can be obtained from imprints left by identifiers on the hard drive of a computer. For instance, in registering Microsoft Word, an identifier was placed on the hard drive that could have permitted Microsoft to track all movements on the Web. Although Microsoft changed the registration system, an identifier is now made through registration of Microsoft Media Player, as well as through other software systems.

Secondly, web bugs can similarly disclose personal information that many of us would prefer to keep confidential. Web bugs are images embedded in a web page that can transmit information to a remote computer when the page is viewed. The remote computer can track which computer accesses which page. The Web bug is quite a recent innovation. They are also known as clear GIFs, or 1 x 1 GIFs. A web bug is a tiny graphic, included in a web page or e-mail message, used to identify who or how many people are viewing the material. They can be placed in the image tags of the underlying HTML code of the page and they can also placed in HTML enabled e-mail messages. For instance, Toys-R-Us.com used a tracking device to compile information about online shoppers. After August 2000 when this practice was discovered, the site discontinued the practice. This apparently violated Tory-R-Us’ privacy policy.

Thirdly, an Internet Service Provider (ISP) is a gateway to the Internet. ISPs hook up a personal computer or system of computers to the Internet. ISPs can divulge a host of information about an individual, including name, address, and credit card. They can recapture personal information that was sent through their services. ISPs can also recapture session information, such as the URLs visited by a user, through its service. At times they have disclosed private information about individuals, leading to embarrassment and adverse employment consequences.

Fourthly, cookies are small text files placed on an Internet user’s computer when a website is accessed. They contain information sent by the server to the user’s browser. If desired, a web user can sometimes view cookies in the source code of the header of a web page. Generally however, the information collected is not displayed to the user, but is recorded, tracked, and stored by the user’s computer and browser. The website can read the cookie later to identify the personal preferences. Such information will enable the user to navigate the website more easily on return visits. Websites, for instance, can recall registration information, so that users need not re-register each visit. Similarly, cookies enable each user to move forward and backward within a site each session. Most cookies last during a user’s “session.” Some can be programmed to last forever -- persistent cookies -- with the corresponding power to keep track of the user’s movements on the Web.

Marketers can then use information about an individual’s use of a site to tailor and fine tune sales and promotional offers to consumers, whether on the Web, via e-mail, or at home. Marketers bring information to those who may not know of particular goods and services. Information links sellers to willing buyers, helping achieve a more efficient economy. To some extent, individuals who choose to participate in commercial transactions must give up some personal information to have access to credit and other financial services.

Such information, however, can also be used to reveal all of our personal habits. If marketers share information with each other, an entire mosaic is created revealing our buying patterns, our browsing interests, and the time we spend on the Internet. Many fear the adverse consequences if that information gets into the wrong hands. Estimates suggest that the average American is listed on many computerized databases.

Individuals can disable cookies by setting their browsers not to accept them. Some websites will not do business with such users, and in any event, disabling cookies makes navigation through websites quite cumbersome.

Fifthly, the Internet permits data marketers to pull together a vast amount of information easily. Public records are aggregated on many Internet sites.

Sixthly, companies have programmed “bots” or spiders to canvas the web and retrieve personal information on other sites, usually email addresses. Thus, a third-party can with ease harvest email addresses and other identifying information supplied to a website. Although websites protect financial information through secure socket layer (and other) technology, less sensitive information can be obtained.

10. Is there any Legal Protection for Data Privacy in Sri Lanka?

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. The following covers the constitutional & other legal protection for individual privacy in Sri Lanka.

In many countries around the world, there is a general law that governs the collection, use and dissemination of personal information by both 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.

11. International Agreements to Protect Privacy

There are three principal international agreements, which are of general relevance to data privacy [4]:

2. The Council of Europe Convention No 108 for the Protection of Individuals with regard to the Automatic Processing of personal data adopted 28 January 1981
3. The International Covenant on Civil and Political Rights in 1966 (ICCPR) (and its European equivalent)

Apart from these agreements is the European Union Council Directive 95/46/EC entitled “Directive on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of Such Data” [5] which was adopted on October 24, 1995 and the United Nations General Assembly guidelines for the Regulation of Computerized Personal Data files on December 14, 1990. In July 2000, the European Commission, which issued a proposal for a new directive on “the processing of personal data on the protection of privacy in the electronic communications sector”. This replaces the 1997 EU Telecommunications Directive and the General Agreement on Trade in Services (GATS) (Stating in art XIV that member states are not prevented by this worldwide agreement to adopt or enforce regulations relating to the protection of privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentially of individual records and accounts)

12. Constitutional Protections

The 1978 Constitution of the Democratic Socialist Republic of Sri Lanka does not explicitly recognize the right to personal privacy as a basic fundamental right. In October 1997 and the year 2000 the proposed Constitutions envisaged right to privacy as a fundamental right. The proposed October 1997 Constitution’s Article 14 (1) specifically states, “Every person has the right to respect for such person’s private and family life, home, correspondence and communications and shall not be subjected to unlawful attacks on such person’s honour and reputation. Therefore unlike the U.S.A there is no reasonable expectation of privacy against intrusions by the state.

13. Legislation

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 No 27 of 1996 and that too refers to interception of communication.

14. The Indirect Protection of Privacy

The Common law in Sri Lanka does not recognize any right to protect personal information. It only permits peripheral protection or remedial action for, invasions of privacy stemming from the inappropriate use of personal data.

15. Contractual Liability

It is possible to include the terms of a contract express protection for personal information. Typically, such provisions are broader than just personal information. They extend to the protection of all information flowing between the parties to the contract. These types of clauses supplement any existing rights the parties which may already have under the tort of breach of confidentiality. The law also implies a number of protections into a variety of contractual relationships. But the contractual relationship is not the essential ingredient, which has given rise to these protections. It is rather the confidential nature of the relationship. Special relationships exist between banks and customers, doctors and patients and lawyers and clients. They may also exist in a non-contractual context; for example, the confidentiality that exists between priests and their parishioners. The ability of the law of contract to provide a solution is severely limited because the data subject is not in a contractual relationship with the data collectors or users. Thus there are no express or implied contractual rights bestowed upon the data subject.

16. Tortuous Liability

16.1 Negligence

There are various possibilities in tort. The most obvious possibility would be an action brought by the data subject against the data controller for negligent use of storage of the data. For instance, a third party has gained unauthorized access to personal data about the data subject due to the direct or vicarious negligence of the data controller. Such an action will be possible only
where a duty of care owed by the data controller to the data subject is established, and this will involve inter alia a consideration of the nature of the information.

16.2 Trespass

Trespass consists of the wrongful entry by the defendant onto land belonging to the plaintiff without consent, the plaintiff being the rightful possessor of the land. Where access to personal data is achieved through the unauthorized access to a computer, which is accomplished in turn by the wrongful physical entry of the defendant upon the plaintiff’s premises, an action will obviously lie for the trespass to land, though this has been incidental to the main objective of gaining access to personal data.

16.3 Defamation

Defamation is a cause of action intended to protect the reputation of a person whose standing has been lowered in the estimation of “right thinking members of society” by the publication of a derogatory and untrue statements. The electronic dissemination of derogatory statements about a data subject through discussion groups or other Internet facilities will provide the subject matter with a cause of action in defamation provided that they are untrue.

16.4 Intentional Inflicting of Distress

Where a person intentionally or recklessly conducts himself so as to cause emotional distress to others, he is liable for that distress. Conceivably, the same course of action would lie where a person revealed personal information designed to cause the data subject acute embarrassment. It is essential that the injury suffered be of an enduring or physical nature.

16.5 Misfeasance in Public Affairs

This tort requires misconduct by the holder of a public office. Such persons must owe the public duties in the manner in which the administrative duties of the officer are performed. The breach of the statutory duties of confidence imposed upon public servants in relation to personal data accessed or used in the course of their administrative duties, for example, would give an aggrieved data subject a cause of action.

17. A Mechanism for Addressing Data Privacy Issues

Global consistency is fundamental to achieving effective privacy protection. If different standards and approaches are taken, the confusion that would result could well undermine rather than enhance consumer protection and it could hinder the development of E-business. If one stand is to be adopted globally, I suggest that the Informational Privacy Principles based on OECD guidelines and European Directives would be a practicable solution. Therefore the Sri Lanka draft Data Protection law should be based on these principles. All these principles are based on protection of the individual privacy protection [6].

18. What are Informational Privacy Principles?

Principle One - Manner and purpose of collection of personal information

Personal information must not be collected where it is gathered by unlawful means; for example theft. This principle extends on prohibition to collection by unfair means. It further elaborates that such collection must be necessary for or directly related to that purpose.

Principle Two - Solicitation of personal information from the individual concerned

This principle is designed to ensure that agencies that collect personal information take steps to make the data subject aware of the purpose for which the information is being collected and, where the information is passed on by the collector, the details of the person or persons who receive the information. This principle only applies where the collector solicits the information from the data subject or individual concerned.

Principle Three - Solicitation of personal information generally

Where information is collected through a process of solicitation, the collector must ensure that reasonable steps are taken to determine the relevance, completeness and currency of the data. In addition, this principle requires that the information collected does not unreasonably intrude upon the ‘personal affairs’ of the data subject.

Principle Four - Storage and security of personal information

This is an important principle, which lies at the heart of the integrity and security of the personal information that is collected and stored. The term ‘record keeper’ is introduced here. The record-keeper must ensure that security safeguards that are appropriate in the circumstances are taken to prevent loss, unauthorized access, use, modification or disclosure other misuse of information.

Principle Five - Information relating to records kept by a record-keeper
This is the openness principle. It requires a record-keeper to have in place a system to enable data subjects, or any other person, to determine whether a record-keeper has possession or control of any records containing personal information.

**Principle Six** - Access to records containing personal information
The availability of access by data subjects to material in the possession or control of record-keepers is central to any privacy regime. This principle sets out that the data subject is entitled to have access to these records without excessive delay or expense, except where the record-keeper is required or authorized to refuse access pursuant to any law that provides access by persons to document.

**Principle Seven** - Alteration of records containing personal information
This principle sets out the rights of the data subject in relation to ensuring the quality of the information held about him or herself. Appropriate corrections, deletions and additions are required to ensure that the record of personal information conforms to the principle.

**Principle Eight** - The record-keeper to check the accuracy etc. of personal information before use
A record-keeper who has possession or control of a record that contains personal information shall not use that information without taking such steps (if any) as are, in the circumstances, reasonable to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant accurate, up to date complete and not misleading.

**Principle Nine** - Personal information only to be used for relevant purposes
The intention of this provision is clearly to prevent misuse of information where it is not relevant to the purpose for which it will be used.

**Principle Ten** - Limits of disclosure of personal information
A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless, the individual concerned has been informed that the information of that kind is usually passed to that person, body or agency or the individual concerned has consented to the disclosure and the disclosure is required or authorized by law.

**Principle Eleven** - Sensitive information
Any information relating to ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual life shall not be used or disclosed by a record-keeper without the express written consent, freely given, of the individual concerned. Information relating to an individual’s criminal history may only be processed as required or authorized by law.

19. The Role of Data Protection Commissioner
An essential aspect of any privacy protection regime is oversight. In most countries with a data protection act, there is also an official or agency that oversees enforcement of the act. This must be absolutely an independent supervisory authority. Independence is also a problem in many countries where the agency is under the control of political arm of the government or part of the ministry and is given considerable power; Government must consult this agency when the government draws up legislation relating to the processing of personal information. The body also has the power to conduct investigations and have a right to access information relevant to their investigations, impose remedies such as ordering the destruction of information or ban processing, and start legal proceedings, hear complaints and issue reports [7]. The agency is also generally responsible for public education and international liaison in data protection and data transfer. It should also maintain the register of data controllers and databases. Another significant feature of this body is that the agency issue guidelines and drafts regarding industry code of conduct and practice for public consultations before it implements.

A major problem with many agencies around the world is a lack of resources to adequately conduct oversight and enforcement. Independence is also a problem. In many countries, the agency is under the control of political arm of the government or part of a particular Ministry and may lack the power or will to advance privacy or criticizes privacy invasive proposals.

20 Conclusion
Unlike the European Union, the United States traditionally has adopted a different approach to data protection. The European Union embraces privacy as a fundamental right and thus considers comprehensive legislation as the most appropriate means to protect personal information. Such an approach requires the creation of government data protection agency and approval before the processing of persona data. By contrast, many Americans believe in the free market and are constantly suspicious of government intrusions. The U.S approach relies on a mix of legislation, administrative regulation and industry self-regulation through code of conducts developed by industries as an alternative to government regulation. In my opinion, I firmly believe if Sri Lanka is really willing to accept the benefits of the
globalization and getting absorbed into International trade we still are not too late for any proposed data protection law that should be based on European model of the EU directive and the data privacy principles because U.S Industry self-regulations are more flexible and there is no independent authority to protect and implement data users rights. Finally we should recognize data privacy as one of our fundamental rights. We need more laws in the emerging new area to attract more e-business through out the world.

Bibliography

1. UNCTAD, E-Commerce and Development Report


