Sunday Times 20th July 2003

Internet, e-business and privacy concerns

By Prathiba Mahanamahewa

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.

Countries without a data protection law may lose business 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 places burdens on Sri Lanka and others countries that collect personal data online. The absence of data privacy legislation in India has proved to be a handicap to Europe and the U.S.A. in business process outscoring to Indian companies.

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 laws may not provide adequate protection.

Online business or online delivery of public services means feeding personal data to the computer, and having it transmitted from one place to another. Data collectors or service providers or data registers are involved in this activity. Therefore the personal data of customers and citizens should be protected by law without keeping any room for manipulation, possible misuse or unauthorized disclosure to a third party.

Threats to privacy

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

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.

Web bugs can 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. They are also known as clear GIFs, or l x l 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 be placed in HTML enabled e-mail messages. For instance, Toys-R-Us.com used a tracking device to compile information about online shoppers but stopped after it was discovered.

Internet Service Providers (ISPs) can divulge a host of information about an individual, including name, address, and credit card. They can recapture e-mail that was sent through their services. In addition, ISPs can recapture session information, such as the URLs visited by a user through its service. ISPs at times have disclosed private information about individuals, leading to embarrassment and adverse employment consequences

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. However, generally, 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. Most cookies last during a user's "session," but some can be programmed to last forever -- persistent cookies -- with the corresponding power to keep track of the user's movements on the Web.

Moreover, 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 email, 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.

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.

Information about an individual's tastes and leisure activity has economic value, and the exchange of such information helps 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 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.

Sri Lanka's 1978 Constitution does not explicitly recognize the right to personal privacy as a basic fundamental right though subsequent proposals envisaged the right to privacy as a fundamental right. 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 1991 Telecommunication Act that too refers to interception of communication.

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.

It is possible to include in 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 may already have under the tort of breach of confidentiality. The contractual relationship is not the essential ingredient, which has given rise to these protections; rather, it is 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, confidentiality between priests and their parishioners. The ability of the law of contract to provide a solution is severely limited because most data subjects are 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.

A library picture of a student in a computer institute. In Sri Lanka data protection laws have not kept pace with the advancement of computer technology. In consequence, there are frequent invasions of privacy by the business sector on the Internet.

Online business or online delivery of public services means feeding personal data to the computer, and having it transmitted from one place to another. Data collectors or service providers or data registers are involved in this activity. Therefore the personal data of customers and citizens should be protected by law without keeping any room for manipulation, possible misuse or unauthorized disclosure to a third party.

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. This may be because 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.

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.

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 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 course of action in defamation provided that they are untrue.

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.

Another tort requires misconduct by the holder of a public office. 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 course of action here.

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, the Informational Privacy Principles based on OECD guidelines and European Directives would be a practicable solution. Therefore Sri Lanka's draft Data Protection law should be based on these principles.

Personal information must not be collected where it is gathered by unlawful means; for example theft. Moreover, this principle extends to collection by unfair means.

The principle of solicitation of personal information from individuals 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.

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.

Storage and security of personal information 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 or misuse of information.

The principle of alteration of records containing personal information 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.

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, complete and not misleading.

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.

Limits of disclosure

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.

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.

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; the agency is under the control of the political arm of the government or a part of the ministry. This agency is given considerable power; government must consult this agency when it 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. The agency is also generally responsible for public education and international liaison in data protection and data transfer.

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 contro of the political arm of the government or part of a particular ministry and lacks the power or will to advance privacy or criticizes privacy invasive proposals

Unlike the European Union, the United States traditionally has adopted a different approach to data protection. The EU 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 suspicious of government intrusions. Therefore U.S. approach relies on a mix of legislation, administrative regulation and industry self-regulation through codes of conduct developed by industries as an alternative to government regulation. It is not too late for Sri Lanka to accept the benefits of globalization and be absorbed into the international trade system. Any proposed data protection law should be based on the European model of the EU directive and the data privacy principles because the U.S. data protection model is an ad hoc one and without an independent authority to protect and implement data users rights.

(The author is a Ph.D Researcher in IT Law. University of Queensland. Australia and Lecturer ir Law, Faculty of Law, University of Colombo)