Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 7 (5): 732-742, 2007
ISSN 1812-5654

E-Data Privacy and the Personal Data Protection Bill of Malaysia

Sarabdeen Jawahitha, Mohamed Ishak and Mohamed Mazahir
Centre for Cyberlaw, Faculty of Management, Multimedia University,
63100 Cyberjaya, Selangor DE, Malaysia

Abstract: Hi-tech development in information and communication technology or ICT enables the public to carry out various business activities. In the course of such businesses, all relevant individual information are saved in the computer system. However, keeping such information in computer is not at all secured due to the availability of technology that may circumvent or get access to the said information. This could be a threat to the privacy specially data privacy. Regulatory compliance and liability issues arising from the use of information technologies and possibility of privacy violation should be given important consideration as the evolution and progression of e-related activities is dependent upon and influenced by the rapidly changing advances in law. The Data Protection Bill 1998 was drafted setting provisions on data principles and rights to data subjects so that data privacy can considerably be protected. However, the introduction of Data Protection Bill 2001 is seen to have focused more on regulation of private sector than public sector whereby the level of protection for data held in public sector is very much reduced.

Key words: Data privacy, violation, protection, law

INTRODUCTION

It is difficult, if not impossible, to define the parameters of the right to privacy including data privacy. Despite the difficulties in defining, privacy is recognized as a fundamental right in Article 12 of the United Nation's Universal Declaration of Human Rights 1948. Article 12 stipulates that no one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attach upon his honour and reputation. Everyone has the right to the protection. Following this declaration many countries have adopted a claim for breach of privacy through various means, either through legislation or court decision. Malaysia through the draft of Personal Data Protection attempts to achieve special recognition for protection of data privacy under the law so that it benefits the government, consumers, companies and various other sectors.

Personal data under the Malaysian 1998 Bill is defined to mean any information recorded in a document in which it can practically be processed wholly or partly by any automatic means or otherwise which relates directly or indirectly to a living individual who is identified or identifiable from that information or from that and other information in the possession of the data user including any expression of opinion about the individual and any indication of the intentions of the data user in respect of that individual (Section 2 of the Malaysian Personal Data protection Bill 1998). This definition includes any information or opinion of a living person that is identified or identifiable as personal data (Ida, 2002). The flaw of this definition is that it does not include other data, which may be used to identify a living individual. However, the court in R v Department of Health Ex Parte Source Informatics (1999) EWHC 315 held that anonymisation does not remove a duty of confidence towards the data subject to an action in tort. With the advancement of ICT, the issue of privacy protection most importantly data privacy protection was given considerable attention (Bonavia and Morton, 1998). Protection of the patient medical records is also recognized as magnified by the advances in telemedicine because of the amount and size of information generated, long-distance transmitted, storage and access. It is said that e-trail of transactional data left behind as individuals use the Internet in a rich source of information about their habits of association, speech and commerce when aggregated, these digital fingerprints could reveal a great deal about an individual (Goldman and Hodson, 2000). Thus this paper addresses the issue of e- data privacy, violation of data privacy, the concern of e-user, consumer and patient and the draft laws of Malaysia that address the issue of personal data privacy including e-medical data.

INFORMATION AND COMMUNICATION TECHNOLOGIES AND BREACH OF DATA PRIVACY

The use of the ICT, the Internet communication in particular captures the personal profile of e-patients

Corresponding Author: Sarabdeen Jawahitha, Centre for Cyberlaw, Faculty of Management, Multimedia University, 63100 Cyberjaya, Selangor DE, Malaysia

without their knowledge whenever they are using the e-dossier for consultancy or other medical purposes. The use of new technology is on the increase and that potential breach may occur when personal information is acquired without consent or knowledge of data subject. Malaysian consumers are also concerned about their privacy. A survey done by Taylor Nelson Sofres Interactive showed that the percentage of Internet users has dropped from 25% of the population in 2000 to 21% in 2002. Among the existing Internet users, only 3 to 5% users are online shoppers. Out of which 38% felt that doing shopping offline provided adequate security including privacy protection. A recent survey revealed that the assurance of privacy protection was the most important factor encouraging e-commerce. 99.66% of the respondents felt that assurance against abuse of personal data was pertinent. Majority of the respondents felt that the web sites must ensure the security during transfer of sensitive data (El-Islamy, 2003). In a more recent survey, the Malaysian e-consumer felt that protection of privacy coupled with security was inevitable for the success of e-commerce. The survey revealed very clearly that Malaysian consumers were mainly concerned about security and privacy issues. More than 77% responded that privacy and security was more important than convenience.

Consumer concern over security and privacy is intertwined. The anxiety about their personal data or confidential information getting into the wrong hands or even the hands of the Government is a major obstacle to more people going online. Although misuse of personal data has not been prevalent or highlighted in the local press, many users are constantly reminded of the possibilities by the vast number of spam received. The most popular reason given by the respondents for their reluctance to fill online registration forms at web sites is that information is not provided on how the data is going to be used (62%) and that they do not trust the entity or company collecting the data (60%). There is an innate knowledge that personal data is being used and "sold" by Internet companies and that consumers are more careful about releasing their financial information such as credit card number. Their fear of their data being misused is compounded by the fear that unscrupulous parties can gain access to their data by hacking the Internet companies they have transacted with (Raihan *et al*., 2003). The technology in relation to e-health is growing rapidly. For example the science of genomics, that is to say, the study of genes and their functions, which lead to the complete mapping of the human genome and proteomic (the study of proteins produced by cell type and organisms) allow doctors to see what is coming through one's genes and protein codes. Thus it will allow to have personalized medical treatments (Yat Seng, 2003). Research like this and further research on biomedical requires data in various sizes, location and sources. Thus integration of data is important. The integration of data from various size, depth and location is being done by using Federated Data Technology. This technology allows to access data in its current location. This allows the information to be distributed while data remain undisturbed in its original form. So it means:

- As information updated, researchers will be updated and have access to live information;
- Researchers will be able to access heterogeneous data from diverse sources and
- Information being accessed in its original form will retain its specialized search capabilities which can be lost when moved into a data warehouse.

In Malaysia the TM Net Sdn. Bhd. in collaboration with Medijaring Sdn. Bhd. introduced Netmyne e-Health system. Under this system data is kept at TM net's state-of-the-art and secure data centre. The system has four main components:

- Medi claim- this enables online billing submission, verification and transmission of information between health care providers and companies.
- Medi Track- This is the processing tool that manages the claim process, monitors medical benefit utilization, generates reports and prepares payment summaries.
- Medi Assure- it offers administrative support for organizations that do not want to get involved with medical billing management.
- Medi Fund- it is a payment agent, a value-added service to manage the payment process to hospitals and clinics on behalf of employers (NSTP, 2002).

Under the system, once an identification number is keyed in, a screen will pop up with the patient information. The member companies can access the databases to enquire on details like medical chits or sickness statistics. Similarly the insurance companies too are able to access the necessary information.

The purpose for introducing this system is said to improve the health care system by using Internet-based solution to connect providers, patients and governments; to educate and inform health care professional, managers and consumers and to stimulate innovation in care delivery and health system management (NSTP, 2002).

The innovations are great but what is worrying the patients are the abuse and misuse of their medical information and violation of privacy. Similarly, Pantai Group started ePantai in the year 2000. It is an electronic infrastructure network company that will connect business-to-business and business-to-consumer. In Phase one "medilines" was introduced to update the patients' medical records and inventory level. In Phase two, it focuses on building e-Health facilities like Electronic Reporting System for its diagnostic laboratory services and the inclusion of an Integrated Electronic Medical Record to enhance services. Focus three focuses on payment and e-procurement issues (Bernama, 2000). It is said that the public concern over privacy protection should be given serious consideration so that, the Malaysian vision of being a global ICT and Multimedia hub and promotion of e-commerce as stated in the Eighth Malaysian Plan can be materialised.

NEW INITIATIVES FOR PROTECTION OF PERSONAL DATA PRIVACY

The ability of the technology to build up personal profile in a matter of minutes, at minimal cost deters the netizens and the e-patients in particular from full utilization of the technology. As a response to this, many countries passed law establishing comprehensive standards for the prevention of the unauthorized dissemination of personal information among various companies and organizations both inside and outside. Malaysia elected to enact new legislation to provide adequate protection for the Internet (Ryder and Rodney, 2003).

Malaysia in 1998 came up with the Data Protection Bill following Hong Kong, New Zealand and UK legislation and was later opened for the public to give comments. The Bill was drafted to create trust among the Internet users by providing adequate protection for personal data. Currently, there are Malaysian companies came up with privacy policy to quell user's fear that their sensitive data will be disclosed. However, the privacy policy adopted by the companies was not adequate to provide sufficient protection, as it was static description of business practices that could be modifiable at any time without prior notice to the users. In certain cases the companies use opt-out system, the users are unlikely to read the privacy policy and therefore, will not be able to exercise opt-out option. Therefore, the Malaysian government has taken legislative initiatives to safeguard the privacy right of its citizens.

Personal data protection Bill 1998: The Malaysian government through the Ministry of Energy, Communication and Multimedia had introduced the Bill in November 1998 called the Personal Data Protection Bill. The 1998 Bill aimed at regulating the collection, possession, processing and use of personal data by the data user (individual or and company or and organization or and government) to provide protection to the individuals. By providing safeguard the government intended to promote confidence among the consumers, patients and the users of both networked and non-networked industries and to accelerate uptake of e-related activities plus promotion of a secure e-environment in line with the objective of Multimedia Super Corridor.

The personal data that comes under the protection of section 2 of the Bill is that of personal data of a living individual. Therefore the companies' data is excluded from the preview of the Bill. However, it is interesting to note that regardless of the recognition under the Interpretation Act and the Companies Act 1965 that the company is a legal person, the Bill excluded the companies from its protection (Saad, 2002). The protection is extended to data processed by automatic means or manual, wholly or in part. In order to have protection under the Bill, there must be the element of process. Process means carrying out of any operation or set of operation on any personal data. Recording, amendment, deletion, organization, adoption, alteration, retrieval, consultation, alignment, combination, blocking, erasure, destruction or dissemination of the personal data are included in the definition of process. The meaning of process is too wide that can cover everything that might be done with or to personal data (Loyd, 2000).

In order to have the data protected, it must contain information, which had been recorded in a document. However, the Bill has defined neither information nor record. Information can be taken to mean, however, all types of knowledge about a data subject that can be communicated. Record could be defined as "the preservation of the thing, for an applicable period of time with the object of subsequent retrieval or recovery (Gold, 1998). The definition of personal data includes protection of the data of a person who is identified or identifiable. Basically, this provision covers an identified person who is known in person and also covers identifiable person. Identifiable is the one whose separate identity is ascertainable but who is not known in person. However, he can be traceable by various available factors.

Personal data also includes any expression of opinion about the individual and any indication of the intentions of the data user in respect of that individual. In the Hong Kong case of Eastweek Publisher Limited and Eastweek Limited Applicant and Privacy Commissioner for Personal Data Respondent [2000] 1 HKC, 692 the court held that a photograph which was taken in a street and later published in fashion magazine is not personal data as the data user or controller has no interest in identity of the

individual. It was not practicable for the identity of the individual to be ascertained by the data user on the information he held. The case may be only relevant if it is shown that it does not restrict to cases where the data subject is identifiable by the data user or controller. As the medical or biological information of patients are considered as personal data, the Bill can be extended to protect e-medical data of patients.

Data principles: Section 4 of the Bill illustrated the principles that need to be adhered to when collecting holding, processing or using personal data. The first principle requires that personal data shall be processed fairly and lawfully. In addition, the data user must be informed of when and what personal data is collected and for what purpose they will be used. The use of technology to collect the personal data including the transactional data is prohibited as most of the companies are using them without the consent of the consumers or the users. According to this principle the use of personal data for direct marketing purposes is also prohibited. In addition, there is an explicit prohibition of personal data for direct marketing purposes in section 52 (2) of the Bill. According to this provision, offering of goods, facilities or services or advertising of the availability of goods, facilities or services or solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes by way of mail, fax, e-mail or other similar means of communication or telephone call is prohibited. The collection and the profiling of user data and use of those data for mass mailing purposes or spam are banned by this provision.

Unsolicited commercial e-mail, commonly known as spam, is a major nuisance for e-consumers. The Gartner Group estimates that 90% of all Internet users receives one item of spam at least weekly and a half receives six or more each week. It is estimated that the average consumer will receive 1,600 spam messages each year by 2005. Companies sending the spam purchase the addresses from electronic commerce companies and also harvest secretly from web pages, discussions groups and web chats. The consent of the Net users is not asked before the addresses are collected. Once the addresses are collected, it is difficult to remove. Many spam messages do not have any return address. Even if there is a real address, many spammers take return messages to create new lists of verified e-mail addresses that they can sell for a greater amount.

However, the bill made a presumption that the collection of data has been fairly done if a person who is authorised by or under any law to supply such information supplies the data or if the person is required to supply it by or under any convention or other instrument imposing an international obligation on Malaysia. Even the Bill did not mention, any law means Malaysian law. It may be presumed that the use of any law could be Malaysian law. Only, spammers from Malaysia are regulated by this Bill, as the Bill does not extend to limit the activities of foreign Spammers. Therefore, this section will not provide much benefit as most Spam originated beyond Malaysian territory. The second data principle stated that the personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes. The principle further requires that the data collected must also be adequate, relevant and not excessive in relation to the purpose. The purpose for which data is to be processed may be specified either by giving notice to the data subject or in a notification given to the commissioner (Loyd, 2000). The compliance of this principle requires the data user or controller not to use or process the excessive data simply because that data can be useful for future purposes. It is also related to the third data principle. According to third principle, the personal data collected must only be used for the purpose it is collected or any other purposes directly related to that. Once it is used for the purpose for which it is used, then the data needs to be deleted or erased, unless such erasure is prohibited under any law or against public interest (Section 44 of the Bill). The use of this data to other purposes is only justifiable given consent to such use. The forth principle further illustrates the issue of consent for disclosure of personal data. According to this principle personal data shall not, without the consent of the data subject be disclosed except where the disclosure is for the purpose in connection with which it was collected or is directly related to that purpose. But if a user of the data is the registered data user, the disclosure of data is allowed for the registered person only. Section 42 of the Bill further provides few exceptions to the general principle regarding consent. Under this provision if the disclosure is necessary for the purpose of preventing or detecting crime, the disclosure is required under the law or disclosure is justified as being in the public interest, the requirement of consent can be waived.

The consent, for the purpose of the Bill, must be obtained specifically at the time the collection of data was obtained. Consent involves a positive demonstrative act and it is not to be implied (Bell v. Alfred Franks and Bartlett Co Ltd. (1980) 1 All ER, 356). The consent obtained can be through opt-in or opt-out method. By using opt-in method, the consumers, users, patients etc. are required to provide positive indication to the

subsequent use of their personal information. The opt-out method, on the other hand, requires the data subject to inform the companies that he is not consenting to the use of his data for the subsequent purposes. Even if the marketers or the companies prefer to use the opt-out method for the purpose of cost cutting, the opt-in will provide more protection for the consumers. As a normal practice of merchants, the customers will be informed of the fact that data supplied may be used for specific purposes and given the opportunity to object to this practice. However, if the data is to be used later for a non-obvious purpose, then explicit consent is inevitable.

In case of sensitive data, explicit consent is necessary. Explicit consent requires the consent to be absolutely clear. Sensitive data was not defined under the Bill. It is stated that sensitive information may include racial or ethnic origins, political opinion, membership of political association, religious beliefs or affiliation, philosophical belief, membership of professional or trade organization, membership of trade union, sexual preference or practices, criminal record and individual health information (Eugere *et al*., 2000). It should be noted that most sensitive information is readily available or known only if it is disclosed by the data subject and despite of this fact, explicit consent is necessary when that data will be collected or processed or used (Forth Schedule of the 1998 Bill).

The fifth data principle requires that the data collected must be accurate, complete, relevant, not misleading and where necessary, kept up to date. Subsection (b) of the Act allows the data user to record the data accurately, which he received from a data subject or third party inaccurately. However, while recording accurately, the purpose for which the data was collected need to be considered. In the circumstances where the data was corrected to reflect accuracy, the data subject's view needs to be obtained and recorded. The fifth principle imposes an absolute obligation to keep the data up-to-date at all time. It requires updating continuously for each and every data collected regardless of the facts that they may or may not be used for continuing decision or action. The sixth principle imposes duty on the data user to destroy the data once the purpose of its collection is fulfilled or achieved. The principle states that personal data shall not be kept for longer than it is necessary for the purpose for which they were collected. In order to ensure that the data is destroyed upon utilization, it is required on the data user to implement a system of data holding and removing unnecessary data. The issue of maintaining accuracy under the principle is given consideration too. Maintaining accuracy of data is important when and after they are collected because the possibility of error or inaccuracy is potentially high. For example, the data held in the UK Police National Computer was subject to an 86% of error. Similarly in US, the US credit bureau holds more than five billion records and trades information regarding credit cards, loans, bankruptcy, etc. It is reported that there are errors in 43% of such files held by the bureau.

The seventh principle allows the data subject to access and to correct the personal data. In addition, the data subject is to be informed of the collection of data and the purpose of such collection at reasonable intervals without undue delay or undue expense. Facts like nature of personal data, the purpose of collection, frequency of alteration of the personal data need to be analysed in deciding what can be considered as reasonable intervals and undue delay. The principle is further explained in sections 32 and 36 of the Bill. According to these two provisions, the data subject is given the right to access and correct the personal data. These rights are only operative when the data subject requests in writing. Within 45 days of written request, the data user is duty bound to comply with the request. However, it should be noted that not in every circumstance such claim will be entertained. The data user may refuse to grant these rights if the data subject did not comply with the requirement of written request or the information supplied was insufficient or the disclosure may lead to the revelation of another individual personal data. If a decision is made as to refusal of access, the data subject must be notified within 45 days. However, if the required data is kept in the employees' data, access to the data may be denied for 7 years from the date of appointment (S.114 of the Bill).

The eighth principle is concerned about the security of personal data. It requires that practical steps to protect personal data against unauthorized or accidental access, processing or erasure, alteration, disclosure or destruction should be taken. In order to ensure security the nature of personal data held, the harm that results in such process or activities, the place where the data is held, the security measures incorporated into any equipment, etc. need to be analysed before the data is put in use. The data users are duty bound to have secured and highly reliable systems to prevent others from unauthorized access, like hacking or cracking, etc. Placing higher level of encryption and firewalls is very important. If anybody had accessed the information or personal data without authorization, they are not only committing an offence under the Computer Crimes Act of 1997 but also going against the eighth data protection principle. In UK, an employee of a credit reference agency used online search facilities made available for him in the course of

employment to conduct a credit search for non-work related purpose. The employee was found liable for procuring the disclosure of data. Having such a provision is really necessary because Malaysian users, consumers of the Internet are concerned about the safety of the personal information given over while browsing or transacting for goods or services.

In a recent survey by TNS Global, it was found that security over the Internet was a major concern. Only 32% of the Malaysians interviewed considered that it was safe to use the Internet to provide the personal information to the government while using the government site. Those who considered it as unsafe have risen to 47% as compared to 42% in 2002. Another survey revealed that 72% of the Internet users was very concern about security on the Internet. There was a noticeable increase of concern when it involves online purchasing as 80% responded that they were very concerned about security in relation to online purchasing. More than 95% responded that security and privacy features were important factors for them in deciding to do business with an Internet-based company, while only 29% of the respondents thought that security features such as encryption and passwords were sufficient to provide security and safety for users (Raihan *et al*., 2003).

The ninth principle that is last is concerned about information that is generally available to data subjects. Accordingly, necessary steps must have been taken to inform the data subject regarding the data users' policy and practices relating to personal data and must have been known to the data subject as to the kind of data held by a data user. All these nine data principles are formulated to protect the data subject's interest and to prevent abuse. Section 4 obliges the data user to comply with the data protection principles. Accordingly, any personal data collected, held, processed or used by a data user shall comply with all the data principles stated under the First Schedule of Personal Data Protection Bill. However, data users may get themselves excused from being compliant with these principles if they are exempted specifically under the Bill.

Exemption of application of data protection: The Bill exempted application of the data principles for various reasons. Total exemptions are allowed for matters covered under sections 79 and 85 of the Bill. Section 79 states that data held by an individual and concerned only with the management of his personal, family or household affairs or for recreational purposes is exempted from the Bill. The exemption is only given to the individuals who are using the data for the purpose of personal, family household and recreational management. Therefore, this exemption is not applicable to companies, recreational clubs or organizations. Section 85 exempts the application of the Bill for sensitive data, which are used or processed after the death of the data subjects. In order for this section to be operative the following conditions need to be met:

- The data must have been collected, held, processed or used during the life of the data subject;
- The data is continued to be held, processed or used for the same purpose and
- The use of data must be within ten years from the death of the person or a reasonable period that may be determined by any code or ethics.

Partial exemptions are afforded to data collected for national security, defense or international relation, crime, taxation, health and social work, regulatory function, news activities, judicial appointment, legal professional privilege, staff planning, personal reference, statistic and research purposes. Section 72 of the Bill states that personal data held by or on behalf of the government is exempted from all the principles but eighth if the personal data is held for the purpose of safeguarding national security, defense or international relations. However, the exemptions mentioned in principles 1, 2, 3, 4, 7 and 9 are only granted by the Minister responsible for personal data protection after consulting with the Minister responsible for national security, defense or international relation (Subsection 2). Generally the data protection Minister will sign a certificate stating that the exemption applies or at time, is required. This certificate is conclusive evidence that the data is exempted from protection under the Bill. This seems to imply that the data subject will have no right to appeal to data Commissioner against the issuance of this certificate even if the Minister does not have reasonable ground for issuing the certificate. The Bill expressly allows the Minister to direct the Commissioner not to carry out any inspection or investigation on the personal data. If such directive is issued, it is compulsory on the Commissioner to comply with.

Other exceptions are available in sections 76, 78, 80, 82, 83 and 86. Section 76 exempts application of principles: 3, 4 and 7 to select suitable judicial officers while principle 7 has been excluded in section 78 if the data supplied is for legal professionals. Section 80 allows certain exemptions to assist in staff planning while section 82 exempts the requirement of data principle 7 for data given as a form of reference. Section 83 provides exemptions from data protection principles 3 and 4 for data kept or held for the purpose of statistics and research. The Bill 1998 certainly provides some protection for the personal

data but there are a number of exemptions attached with those data protection principles cast a doubt as to the real benefit to the protection of privacy in general and personal data protection for e-medical data privacy in particular.

Rights given to data subject: Besides the data protection principles, the Bill also provides certain statutory rights so that there could be a balance between the business urgency in using the personal data and the data subjects' interest to prevent misuse of personal data. Section 32 (1) of the proposed Bill 1998 states that the individuals are given the right:

- To be informed by any data user whether any personal data of which that individual is the data subject being held by the data user;
- To be supplied by any data user with a copy of the personal data held by the data user; and
- Where the processing of personal data of which that individual is the data subject held by automatic means, to be informed by the data user of the logic involved in decision-making.

The first part of this provision provides the right to be informed of the collection and holding of personal data about the data subject to him. Upon the supply of such information the data subject has the right to access and obtain a copy of data held by the data user or controller. However, the data subject is required to write to the data user for such copy with a payment of appropriate fee (Section 32 (4) and section 47 (2). If the data subject requires copies from different databases or more copies from the same database, request and payment are to be made separately. When data is held for various purposes in various files or databases requesting access to that data will be burdensome on the e-consumers.

The right to access is coined with the right to correct personal data. Section 36 of the Bill reads that subject to subsection 2:

- A copy of personal data has been supplied by a data user in compliance with a data access request;
- The data subject or relevant person considers that personal data is inaccurate.

The data subject or a relevant person may make request to the data user that the data user makes the necessary correction to the personal data. When the data subject or relevant person considers that the data supplied by the data user is inaccurate the data subject or relevant party can request for the correction. Before the data user complies with such request, it must be satisfied that there is such inaccuracy in the data. If he is so satisfied, within 45 days after receiving the request, necessary correction of such personal data while supplying the applicant with the copy of corrected data is mandatory. In addition, the data user is obliged to disclose to third party who is holding the data for one year immediately preceding the day on which the correction is made. Such disclosure of correction of personal data must be accompanied by a notice writing the rational for the correction.

The other right that has been given to a data subject under the Bill is the right to prevent collection likely to cause damage or distress. Section 40 of the Bill allows the data subject to require the data user not to collect his personal data or to cease holding, processing or use of any personal data. The right is only available when it is shown that such collection, holding process or use is causing or likely to cause damage or distress to the data user or other individuals. The notice to the data user must be in writing. The data user may not be able to stop collection, holding or use of data which may cause or likely to cause if it is shown that:

- The data subject has given consent earlier;
- The collection, holding, processing or use is necessary for the performance of contract, entering into a contract, compliance with any other legal obligation where the data user is a subject. The denial is also possible when it is necessary to protect the interest of the data subject or other circumstances where the commissioner prescribed by way of gazette.

Section 41 (1) permits a data subject to request in writing the data user to ensure that no decision which significantly affects him or her is based solely on the processing of personal data by automatic means. As a general practice, the companies do rely on computer aided or automated decision making to evaluate matters relating to data subjects or consumers credit worthiness, reliability, efficiency, etc. When such decision is made that significantly affects a data subject, the data user must notify the data subject that the decision was taken on that basis as soon as reasonably possible (Section 41 (2). However, if it is shown that the process also invokes human intervention or discretion and then the provision of automated decision making process is not applicable as this right is only applicable when a decision is solely made by automated processing. The question as to how much human intervention is needed is not addressed in the Bill. It perhaps requires more than trivial contribution

to the decision. Placing signature or stamp on an automated decision may not be adequate to exempt the application of the protection granted under section 41 (1).

In addition, section 41 (2)(b) provides that the data subject is entitled within 21 days of receiving the notice of automated data processing, to appeal to the data user to reconsider the decision or to take a new decision other than on that basis. However, the application of the right is exempted for the purposes stated in subsection 4. This provision states that:

- The decision is taken in the course of steps taken:
  - For the purpose of considering whether to enter into a contract with the data subject;
  - With the view of entering into such a contract; or
  - In the course of performing such a contract.
- It is authorised or required by or under any law;
- The effect of the decision is to grant a request of the data subject;
- Steps have been taken to safeguard the legitimate interest of the data subject; or
- It is made in such other circumstances as may be prescribed by the Commissioner by order published in the Gazette.

These exemptions legalize the automated decisions making practices of companies as well as the banks since these companies use expert systems and the databases to reject an offer of sale or service or application for credit cards. These exemptions certainly will increase the reliance on automated decision making as it is considered to be a key business strategy. As a good business strategy the Forrester report suggests that to succeed with automated e-business, the firms must build an infrastructure that applies automated decision-making to various time frames, using different rules based on different data (Advisor Zone, 2000). After analysing the important provisions of the Bill 1998, it seems that it creates doubt as to its adequacy to protect the data subject, e-consumers. Generally the wider the scope of application of a particular legislation, the higher the adequacy level would be. But the Malaysian Bill is said to be narrow in its scope with too many exceptions. Therefore, it will cripple the effectiveness of the law. In the event of conflict between the data protection law and other laws other laws shall supersede over the Bill (Saad, 2003). Section 105 provides an explicit exclusion for data held outside Malaysia, unless the personal data is used or intended to use in Malaysia, or if the control of personal data, holding, processing or use of personal data is done through an agent in Malaysia. This provision is major setback in protecting the personal data from foreign enterprises. Perhaps this provision may derogate the protection given under the Bill.

Data protection bill 2001: The Bill 1998 on Personal Data Protection was the first effort made by the Malaysian government in recognition of the need for the law on personal data protection. This Bill was opened for public opinion and consultation on its applicability and suitability for Malaysia. Seven workshops were conducted and various parties had given their feedback concerning the Bill. Participants in this consultation agreed that the data protection should cover not only the companies but also the government agencies and that the commissioner should be an independent body under the Parliament unlike the Bill 1998 in which the commissioner is appointed by the Minister and he is answerable to the Minister only. Opinion on the necessity of having independent data commissioner was collected by the researcher. 71.9% of the respondents said that the commissioner either had to be independent or answerable to Parliament to ensure fairness and to avoid bias. However, 6.3% (this represents are from the education and the other industry) viewed that it was not necessary for the commissioner to be independent or answerable to Parliament as in Malaysia most commissioners including the human right's commissioner is somehow answerable to the Minister or government. However, others viewed that independent commissioner would be able to be fair to everyone even if the government was involved in case of any dispute. Some others viewed that the independence of the commissioner is important to avoid manipulation. Therefore, it certainly created a doubt as to the neutrality of the commissioner when it comes to conflict between the interest of data subject and the government interest. A number of companies and government agencies requested that they should be exempted from the application of data protection legislation as they were already regulated by other legislation like Banking and Financial Institutions Act, Official Secrets Act. Having considered various parties' opinions and applications for exemption and the 9/11 catastrophe in USA, the ministry concerned had redrafted the Bill 1998 to reflect the rights of individuals and the companies and the government's interest over the personal data. The redrafting was considered as unavoidable since it was felt that the Bill 1998 which followed UK legislation on personal data protection was not acceptable as it was not adequate, complex and onerous. Therefore, it was decided by the draftsmen of this Bill that the Safe Harbor Model with modifications will suit better for the Malaysian

circumstances. As it is flexible and not onerous on the data user to get pre-consent on all types of data before collection or holding or use (Nor, 2003).

The regulators believe that the new draft will satisfy the data subject, the user as well as the requirement of UK directive on the adequacy of law concerning the protection of personal data. This Bill proposes to cover any personal data directly relating to living individuals and it regulates person, body of persons, corporation and government who collect, use or disclose personal data. In this respect there is no difference between the Bills 1998 and 2001. The new Bill by providing different sets of data principles to private and public entities and also differs from the 1998 Bill.

The private sector is required to follow seven principles as in Safe Harbour unlike the nine principles provided in the old Bill. The new principles are:

Notice principle: This principle requires the data user to inform the data subject the purpose of data collections, contact details of data user, the types of third party, the data to be disclosed and the information about the limitation of its use. The required notice is to be clear and in conspicuous language when the data is collected or within a reasonable time upon its collection or before the data be used for the purpose other than for which it was collected.

Choice principle: This principle allows the individual to opt out to other purpose for which the data was not originally collected or subsequently authorised by the data subject.

Disclosure principle: Under this principle disclosure of personal data to third party must follow notice and choice principles if the transfer is for the similar purpose for which it was initially collected. However, before the data user discloses he has to ensure that the third party provides same level of protection as it is provided by him.

Security principle: Ensuring security from loss, misuse, unauthorized access, unauthorized disclosure, amendment or destruction while collecting, using or disclosing personal data is a very important duty imposed on the data user under this principle.

Data integrity principle: When the data user collects, uses or discloses personal data, the data shall be relevant to the purpose. The relevancy of data to be decided by the commissioner by considering the activities of organizations or companies. This principle further requires that any subsequent disclosure or use must be compatible with the original purpose.

Access principle: The purpose of this principle is to allow access to data subject to correct, amend or delete where the personal data is inaccurate. However, this right is not available where it is proven that the burden or expense of providing access is greater than the risk to the individual privacy or allowing access will lead to disclosure of other individual's data where the individual concerned did not consent to such access. Access will also be denied where such access is regulated by law.

Enforcement principle: This principle requires that the data user should provide clear transparent mechanism to ensure compliance of data principle and in the event of non-compliance recourse for affected individual must be expressed unequivocally (Nor, 2003).

When it comes to public sectors the new Bill only requires them to comply with the principles of collection, use and disclosure as required by law; right to access by written law; and responsibility to protect personal data. It also requires the public sector to have a personal data protection policy. The reason for giving relaxation to public sector under the Bill, according to Mohamed Nor from the Ministry responsible for the data protection, is that the public sector adequately regulate privacy issue through Official Secrets Act 1972, section 4 of Statistics Act 1965, section 19 of National Land Code and section 139 of Consumer Protection Act 1999. Additionally, the data subjects are indirectly protected in public sector through administrative measures and disciplinary legislation. It seems that the new Bill instead of providing better protection of privacy compromises this right for the benefit of companies and the government so that the economic enrichment and national security could be protected. Basically, the available laws like the Official Secrets Act, the Statistics Act or the Consumer Protection Act do not guarantee adequate protection. They cover only small portion of issue on the whole segment of right to privacy. These provisions in no way will be able to protect the e-consumer privacy over the global dossier.

It is argued that even if the new Bill adopted the Safe Harbor Model, the weaknesses as regards the voluntary self-regulation and enforcement under the Safe Harbor were adequately addressed by providing a single regulatory body for the personal data protection under the Bill. However, how the regulatory body is going to be constituted, what are the functions, power and restrictions of this body are yet to be disclosed. Nevertheless, it is expected that the regulatory body that will be established to enforce the legislation would be autonomous in term of finance and human resources. One of the obvious weaknesses of this Bill is that other written laws will prevail over this Bill to the extent of its

inconsistency. The reason being is that the legislation is drafted to fill in the gaps concerning personal data protection, which is not covered by available written law in the country.

The Safe Harbor model besides the weakness on enforcement has various other problems that left many people to wonder whether the principle under safe harbor will be able to provide basic protection of data. It does not provide protection for public record information. Protection is also exempted for any processing of personal data pursuant to conflicting obligation or explicit authorization of US law. Legal redress in case of breach is not adequate, unlike it has been assured by the US Department of Commerce. The only available law protecting the individuals against breach of privacy is through tort liability. However, the US courts thus far had not addressed tortious liability on the issue of breach of data privacy (Reidenberg, 2001). Although it is alleged that the Malaysian new Bill embodied the weaknesses of Safe Harbor by minimising restriction to the application of data protection principles and also by providing adequate redress mechanism to the victimized individuals against the data controller. How far the new legislation is going to provide protection for privacy is yet to be known to the public as the Bill is still kept under Official Secrets Act of Malaysia. It is important to note that having adequate and satisfactory level of protection for privacy is inevitable as it can bring benefit not only to the individuals but also for government and companies. It is undeniable that privacy legislation may incur cost to the government, companies as well as the institutions. A related study found that privacy legislation will cost between 9 million and 36 million US dollars in US (Hahn and Robert, 2001). However, Reidinberg commented that this study did not reflect the actual picture of the cost as the cost was evaluated by asking a group of consultants how much they would charge to write privacy software.

In addition, the consultants were asked to assume that the database contained web site registration information on 100,000 to 10 million users and they estimated that the costs ranging from USD 44,000 to 670,000 per site. The study exaggerated the real cost and in fact had ignored any financial losses resulting from breach of privacy (Reidenberg, 2001). The financial loss due to lack of privacy protection could be more. According to Forrester reports, the US consumers spent USD 12 billion less online in 2000 as a direct result of inadequate privacy protection. Therefore having adequate protection for Malaysian consumers, patients and users is certainly going to be a boost in contributing to national economic prosperity along with the success of MSC flagships.

CONCLUSIONS

The technology can be used to facilitate the breach of personal privacy of e-users. Assurance of protection against such violation is necessary to convince people to fully utilise the Internet dossier to their benefit and the benefit of the nation at large. The most concerned right to privacy in the ICT era is the information or data privacy, in particular the medical data privacy. To address, though, there is yet none but the government came up with the draft legislation. The 1998 draft Bill setting nine data principles provides various rights to data subjects. However, the exemptions provided by this Bill give chance to collectors or users of personal data to by pass the protection provided under this Bill. While the 1998 draft remains as a draft the government tries to modify it as draft 2001. The new draft, which is kept confidential, is said to be following the Safe Harbour Model. The new draft provides two sets of rules, one to the government and the other to private companies. The government is said to be less regulated than the companies. It is said to be alarming as government is holding and processing lots of data for various purposes. Thus how far the Personal Protection Bill is going to provide protection to e-medical data privacy is to be seen in near future.

REFERENCES

Advisor Zone, 2000. Automated Decision-making Key to Business Strategy, available: http: //suppluchainadvisior.com/doc/06705. pp: 1.

Bell v. Alfred Franks and Bartlett Co Ltd., 1980. 1 All ER 356.

Bernama, 2000. Asia Pulse Pte. Ltd. at: http://global. factiva.com

Bonavia, I.M. and W.L. Morton, 1998. Personal Information Privacy Issues Relating to Consumption in the US Market place, Consumer Interest Annual, 44: 25.

Eastweek Publisher Limited and Eastweek Limited Applicant and Privacy Commissioner for Personal Data Respondent, 2000. 1 HKC 692

El-Islamy, H., 2003. Protection of Online Privacy and Its Impact on E-commerce. Available: http://www. cljlaw.com.

Eugere *et al*., 2000. Privacy in an e-business world: A question of balance. Journal of Law and Information Science, l: 7.

Gold, R.V., 1998. 1 AC 1063.

Goldman and Z. Hudson, 2000. Virtual Exposed: Privacy concerns are keeping consumers from reaping the full benefit of online health information. People-People- Health Foundation, pp: 1-12.

Hahn, W.R., 2000. An Assessment of Costs of Proposed Online Privacy Legislation. Available at: http://www.actonline.org/pubs/HahnStudy.pdf. pp: 23-24.

Ida, M.A, 2002. E-commerce and Privacy Issues: An Analysis of the Personal Data Protection Bill. Paper Presented in 17th BILETA Annual Conference. Amsterdam: Free University, pp: 2.

Loyd, J.I., 2000. Information Technology Law. 3rd Edn. UK: Butterworths.

New Strait Times Press, 2002. TM Net's Netmyne e-Health for an Efficient Health care Industry. Financial Times Information Ltd. At:http://global.factiva.com.

Nor, M.A.A., 2003. E-Privacy in the New Economy. Presented in National Conference Management Science and Operations Research 2003, Melaka. Century Mahkota Hotel, 2: 241.

Raihan, N. *et al.*, 2003. Security and Privacy Issues as Barriers to E-Commerce Growth: A Consumer Perspective. IBIMA, Cairo, pp: 118.

Reidenberg, R.J., 2001. E- Commerce and trans-atlantic privacy. Houston Law R v Department of Health Ex Parte Source Informatics [1999] EWHC 315.

Ryder, D. and Rodney, 2003. E-privacy and online data protection: Legal issues and perspectives on the indian experience. Presented in International Conference on Privacy, Data Protection and Corporate Governance in the Internet Economy. KL, JW Marriot Hotel, pp: 3.

Saad, A.R., 2002. Privacy and Personal Data Protection Act in Malaysia. Available :http://www.arsa.com

Saad, A.R., 2003. Privacy and Data Protection in Malaysia: Strategies, Direction and Legal Protection. Presented in International Conference on Privacy, Data Protection and Corporate Governance in the Internet Economy, KL. JW Marriott's, pp: 35.

Taylor Nelson Sofres Interactive -Global E-Commerce Report, 2002.

Yat Seng, C., 2003. Net Value- Get Ready for E-health. The Edge Communication Sdn. Bhd. At:http://wwwglobal.factiva.com.