2008

E-health Data Privacy: How far is it protected?

Jawahitha Sarabdeen
University of Wollongong, jawahith@uow.edu.au

Mohamed Mazahir Mohamed Ishak
International Islamic University - Malaysia

Publication Details

Sarabdeen, J. & Ishak, M, E-health Data Privacy: How far is it protected?, Communications of the IBIMA, 1, 2008, 110-117.

E-health Data Privacy: How Far It Is Protected?

Dr. Jawahitha Sarabdeen
Department of Business,University of Wollongong in Dubai,P.O.Box: 20183, Dubai,UAE
jawahithasarabdeen@uowdubai.ac.ae http://www.uowdubai.ac.ae
Mohamed Mazahir Mohamed Ishak
Research Graduate,Ahmad Ibrahim Kulliyyah of Laws,International Islamic University Malaysia,
Kuala Lumpur,Malaysia
mimmazahir@gmail.com

Abstract

The ICT advancement in the e-health industry paved the way for diagnosis, analysis and treatment conveniently good for the consumers and the relevant industry players. Consequently, consumer concern over the health information, its collection, use and storage has been on the increase seeking ways to protect them all. Legislative measures adopted in the US, the UK and Australia are seen to be ensuring adequate protection for the health information as Malaysia steps forward in the right direction. Research analysis of this study results in pros and cons of the available legal measures and mechanism with recommendations for a better legislative future for the privacy regime in Malaysia.

Keyword: ICT, e-health, privacy, Malaysia.

1. Introduction

The advancements in Information and Communication Technology have enabled the health industry to carry out diagnosis, analysis and treatment by online doctors or medical practitioners beyond geographical boundaries. In the process, all relevant information about the patient are stored in the computer system of the medical practitioner and other related parties for record and reference purposes. The collection, use and storage of the medical information in the computerized system facilitate easy access for further use and reference. But the greatest challenge is providing protection of privacy and confidentiality of the medical information (data) that being stored. The developed nations see the inevitable transition of ICT based industries is a common phenomenon. Having realised this phenomenon, countries like the US, the UK and Australia have taken bold steps towards improving and enhancing the health sector by ensuring adequate protection for the patients' records. For example, Australia through the National Health Information Management Advisory Council's Health Online: A Health Information Action Plan for Australia[1] provides strategy for information management and the use of online technology within the health sector. It also addresses the issue of protection of patient's records against abuses. One of the fast developing countries like Malaysia is also striving towards providing some sort of protection for health data privacy.

The research utilizing the content comparative legal research methodologies seeks to analyse the legal framework of Australia and Malaysia on e-health data privacy to see how far the legal protection is available and its level of adequacy.

2. Literature Review

Joan Dzenowagis[2] states that technological development in health sector brought new relationships between consumers and providers and consumers and suppliers. This development creates a dual challenge for legal and regulatory framework. The challenge can be put as "growth" vs. "protection". He stresses that there is a need for common regulatory and standards relate to information gathering, storage and exchange, reliable, secure, effective networks and evaluation of impact on consumer. For him the issue of privacy and confidentiality will be one of the major issues in e-health sector.

A survey by Louis Harris[3] reveals that privacy concern in e-health initiatives is real. It confirms the perception of lack of control and sufficient safeguard for medical records. 25% respondent reported that they believed their medical record had been improperly disclosed, and 34% of the health care professionals believed that the records were given to unauthorized persons "somewhat often". In Malaysia too the privacy concern is said to be a cause

[1] Health Online, "A Health Information Action Plane for Australia," <www.health.gov.au/healthonline/her_rep.htm> (accessed 13 December, 2005).

[2] Joan Dzenowagis, *Protecting eHealth Consumers Regulatory & Normative Issues*, (USA: World Health Organization, 2000), 3.

[3] Harris Interactive, Survey on Medical Privacy (pdf), (New York: Louis Harris & Associates, 2004),<http://www.harrisinteractive.com/news/newsletters/healthnews/HI_HealthCareNews2004Vol4_Iss13.pdf>

hindering the adoption of ICT based health program. A recent survey revealed that the assurance of privacy protection was the most important factor encouraging e- activities. 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.[4] Malaysian users 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.[5]

Noor Raihan et al., finds that 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.[6] According to Privacy International, Malaysia lacks comprehensive legislative framework to provide protection for e-health data.[7] Jawahitha and Mazahir state that although there is an absence of specific provision on the issue of right to privacy in the Malaysian Federal Constitution, articles 5(1) and 8(1)[8] may recognise such a right if these provisions are to be interpreted broadly and liberally in accordance with the particular needs of the developing society. They also point out that the expression of 'life' appearing in article 5(1) does not refer to mere human existence. It incorporates all those facts that are an integral part of life itself and more matters, which go to form the quality of life. As such the right to privacy which is considered as important to have a decent and quality life may be easily included in the expression of "life". In the event if right to privacy is recognised under article 5(1) as one of the fundamental liberties, then the netizens will have better protection of their right to privacy in case where there is a decision that adversely affected the guaranteed fundamental liberty. When such a decision is taken, article 8(1) will ensure that right to access to justice is ensured. This provision will ensure that procedural and substantive fairness have been adopted. [9]

The Privacy International states that the legislation which has implication to privacy includes Computer Crimes Act 1997, Digital Signature Act 1997, Communication and Multimedia Act 1998, Penal Code, Official Secrets Act 1972, National Land Code 1965, the Consumer Protection Act 1999, and the Banking and the Financial Institutions Act 1989.[10] The Computer Crimes Act imposes criminal punishment to those who access, modify, communicate or use computer programs or files or documents without authority. The "General Consumer Code 2003" issued by the Malaysian Communications and Multimedia Commission, the statutory body established in accordance with the provisions of Communications and Multimedia Act 1998 also addresses the issue of privacy and provides certain remedies against violation of privacy.

As put by Abu Baker Munir et al., this General Consumer Code 2003 sets out rights of consumers for services offered by the communications and the

[4] Hurriyah-el-Islamy, "Protection of Online Privacy & Its Impact on E-commerce," <http://www.cljlaw.com> (accessed 13 January, 2005), 4.

[5] Taylor Nelson Sofres Interactive, *Global E-Commerce Report*, (USA: Taylor Nelson Sofres Interactive, 2002), 2.

[6] Noor Raihan, Elena, & Jawahitha, "Security and Privacy Issues as Barriers to E-Commerce Growth: A Consumer Perspective," *Proceedings the 2003 International Business Information Management Conference*_(Cairo: IBIMA, 16-18, December 2003), 114.

[7] Privacy International, *Survey: Malaysia*, <http://www.privacyinternational.org/survey/phr2003/countries/malaysia.htm> (accessed 17 December, 2005).

[8] Article 5(1) reads that "no person shall be deprived of his life or personal liberty save in accordance with law" and article 8(1) states that "all persons are equal before law and entitled to the equal protection of the law."

[9] Jawahitha & Mazahir. "Protection of e-consumer Privacy in Malaysia," *International Conference on Intelligent Agents, Web Technologies, and Internet Commerce*, (Gold Coast: IEEE, 2004): 12-14.

[10] Privacy International, *Survey: Malaysia*, <http://www.privacyinternational.org/survey/phr2003/countries/malaysia.htm> (accessed 17 December, 2005), 2.

multimedia industry.[11] The main objective of this code is bench marking the service delivery as well as providing model procedures for the handling of consumer complaints, speedy consumer dispute resolution and the protection of consumer information.

Recent Caslon survey suggests consumer concerns about privacy equal worries about the security of online purchasing as major roadblock for Australian e-commerce. Over 80% of the top 200 Australian sites seek personal information but fewer than 10% have a privacy policy that meets the national Privacy Commissioner's principles. Scott McNealey of Sun claims that privacy is no longer an issue for concern. Solveig Singleton argues: "there is little to fear from private collection and transfer of consumer information". That assertion is in inconsistence with the government responses to bad practices. It is also in inconsistence with the users and business perceptions that there are substantive concerns.[12]

3. E-Health Data Privacy in Australia

In Australia, it is generally believed that medical professionals own the patients' medical records and they have the right to decide whom the record is to be revealed to.[13] With the introduction of e-health, concerns of right to data privacy became a primary concern for the patients. Data collection, use, access and storage of e-health data or medical information of the patient have been considered as the issues that require necessary attentions from the regulators in term of protection and confidentiality. The concern over health data privacy has been a very important issue in Australia because right to privacy is not enshrined in the constitution of Australia. However, later the government has taken initiatives to provide Commonwealth and State legislation. The statutory privacy regime was initially restricted to the public sector, and progressively extended to cover the private sector. The Privacy Act 1988 was passed to regulate the public sector. It creates a single, nationally consistent framework for protecting privacy. Beginning December 2001, the private sector came under the regulation of the Privacy Amendment (Private Sector) Act 2000, which amended the Privacy Act 1988. The introduction of the Privacy Amendment (Private Sector) Act 2000 paved the way for better privacy protection of the patients in the private clinics and hospitals. [14]

The law now offers privacy protection and choice to patients while balancing this with the need for health service providers to share information for the provision of quality health care.[15]

3.1 The Privacy Act 1988

The Privacy Act 1988 and related regulations address the privacy issues in the public sectors and that includes the public hospitals clinics etc. The Privacy Act 1988 applies the 11 Information Privacy Principles (IPPs) to all Commonwealth Government departments and the Government of Australian Capital Territory (ACT). It protects personal information held by the Federal Public Sector. Section 14 of the Privacy Act 1988 sets out very detailed information on privacy principles that are briefly discussed as follows:

Principle 1 requires that personal information must not be collected by unlawful or unfair means. The information must be collected for the purpose that is lawful and directly related to a function or activity of the collector. Principle 2 ensures that the collector of personal information takes necessary steps to make the data subjects aware of the purpose for which the information is being collected. However, this principle is not applicable if the information is obtained indirectly from a third party or provided on a voluntary basis. The duty of the collector to make the data subject aware of the purpose for which the information is collected must be performed before the information is collected. According to data principle 3, a collector who collects information through a process of solicitation shall take reasonable steps to ensure that the information collected is relevant, up to date and complete. The data principle 4 imposes an obligation on a record-keeper to ensure the protection of the record against loss, unauthorised access, use, modification or disclosure, and against other misuse. If the information is required to pass on to a third party, all reasonable steps must be taken to prevent unauthorised use or disclosure of information contained in the record. According to Principle 5, a record keeper is to take steps to enable the data subject or any other person, to ascertain whether the record-keeper has possession or control of any records containing personal information. The record-keeper shall make the information collected available for inspection by members of the public.

---

[11] Abu Bakar Munir & Ganasegran, "The General Consumer Code: Towards Compliance by Internet Service Providers," *CTLR* Issue 3, (2004): 64.

[12] Caslon.com, "Caslon Analytics: Privacy Guide," <http://caslon.com.au/austprivacyprofile3.htm> (accessed 3 June, 2006)

[13] Malcolm Crompton, "What is Privacy," *Privacy and Security in the Information Age Conference,* 16-17 August, 2001, < http://www.privacy.govau/news/speeches/sp51note.html> (accessed 3 June, 2006).

[14] Caslon.com, "Caslon Analytics: Privacy Guide," <http://caslon.com.au/austprivacyprofile3.htm> (accessed 3 June, 2006)

[15] Ibid. 3.

Principle 6 states that a record-keeper can have possession or control of a record that contains personal information; the individual concerned shall be entitled to have access to that record. Principle 7 imposes an obligation on the record keeper to ensure the accuracy, completeness, relevance and currency of the information. The record-keeper is required to make appropriate corrections, deletions and additions to ensure that the record of personal information confirms with this obligatory principle. According to the 8th principle, a record-keeper who has possession or control of personal data 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 accurate, up to date and complete. Principle 9 states that a record-keeper who has possession or control of a record that contains personal information shall not use the information except for the purpose to which the information is relevant.

The 10th privacy principle prohibits a record-keeper from using the personal information obtained for a particular purpose or any other purpose. This principle is not applicable, if the individual concerned has consented to the use of the information for the other purpose or it is required or authorised by or under the law. Principle 11 prohibits a record-keeper from disclosing the information to a third party unless the conditions as below are satisfied that the individual concerned is reasonably aware that information of that kind is usually passed to a third party or the data subject was consented to the disclosure or the record keeper believes that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of some other individual. The exceptions are also extended to the disclosure that is required under the law or the disclosure is reasonably necessary for the enforcement of the criminal law.

3.2 The Privacy Amendment Act 2000

The privacy Amendment Act 2000 is an extension of the Privacy Act 1988 and it regulates the private health sector. This introduced The National Privacy Principles (NPPs). These principles were designed with the aim to deliver, *inter alia*, promotion of greater openness between health service providers and patients regarding the handling of health information. They cover the whole information lifecycle from collection to storage, maintenance, use and disclosure. Under the law, health service providers can only collect information if the patients have given consent. The patients' consent can be reasonably considered as implied as long as it is clear to the patients the reason for the collection. It may be necessary that the service provider advises the patients about how the information will be handled. The patients will have access to the information collected. He may look at the information, obtain a copy of the information like x-ray, take note of the information, listen to the information, and get an electronic copy of information stored on a computer system or a database.

This Privacy Amendment Act 2000 gives individual a right to know what information an organisation holds about and a right to correct that information if it is wrong. By this Act, consumers have the right to know the reasons for collection of their personal information by private sector. They will also know the kind of information it holds about, the usage and the parties who will get the information. Patients can also make a complaint if they think that their information is not being handled properly. Some of the privacy principles like data security and data quality will be applied to organisations that already hold data when the Privacy Amendment Act 2000 is implemented.

The collection principle states that an organisation must not collect personal information unless the information is necessary for one or more of its functions or activities. The information collected must be of lawful and by fair means. At or before the time, it must take reasonable steps to ensure that the individual is aware of the organization that is collecting and the amount of collection. The data subject is given the right to gain access to the information collected. This Act like the Privacy Act 1988 requires to disclose the purposes for which the information is collected and the organisations to which the organisation usually discloses information of that kind.

The principle is also explaining the issues pertaining to sensitive information. It prohibits organisations collecting sensitive information about an individual except with the consent or that individual or if it is required by law. However, it allows an organisation to collect personal information for the following purposes of research relevant to public health or safety and the compilation or analysis of statistics relevant to public health or public safety; and the management, funding or monitoring of a health service. However, it is an obligation on the organisation to take reasonable steps to permanently identify the information before the organisation discloses it. The Privacy Amendment Act 2000 regulated the way private organisations can collect, use, keep secure and disclose personal information. This gives a right to know why a private sector organisation is collecting one's personal information, what information it holds about him, how it will use

the information and who else will have access to that data. The Act covers private sector "organisations which includes businesses with annual turnover of more than $ 3 million, all health service providers, regardless of turnover, health service providers that hold health information etc.[16] The Privacy Amendment Act 2000, however, exempts political parties, the media and small businesses as well as use and disclosure of employee records. The exemption as to small business is a bit problematic because it is estimated that the small business exemption will leave up to 95% of the Australian business untouched by law. A small business is the one with an annual turnover of $3 million or less, which do not provide a health service or hold health information and does not provide contractual services to Commonwealth and does not transfer personal information about an individual as well.[17]

4. E-Health Data Privacy in Malaysia

Due to various concerns over data privacy, Malaysian government had drafted the Personal Data Protection Bill in 1998. The Bill was intended to regulate the collection, possession, processing and use of personal data by the data user (individual or and company or and organisation or and government). Providing statutory protection for the individuals' data is set to be its primary concern. With this initiative the Malaysian government sought to promote confidence among the users of Internet for various purposes including the medical purpose. This in turn accelerates the uptake of e-health and other related e-environment.[18] The Bill was introduced to satisfy the increasing demand of the local and international community. The principles that need to be adhered to when collecting, holding, processing or using personal data are illustrated in section 4 of the Bill. It consists of 9 data principles. They are:

First Principle	The personal data shall be collected fairly and lawfully
Second Principle	Purposes of collection of personal data
Third Principle	Use of personal data
Forth Principle	Disclosure of personal data
Fifth Principle	Accuracy of personal data
Sixth Principle	Duration of retention of personal data
Seventh Principle	Access to and correction of personal data
Eighth Principle	Security of personal data
Ninth Principle	Information to be generally available

The Bill remained as a draft till 2001. After the 9/11 catastrophe in USA, the government had redrafted the 1998 Bill to reflect the rights of individuals and the companies, and the government's interest over the personal data.[19] The redrafting was considered as necessary 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. The government decided to adopt the Safe Harbor Model with modifications as it was thought that it will suit better for the Malaysian circumstances. The Safe Harbor Model is said to be flexible and not onerous on the data user to get pre-consent on all types of data before collection or holding or use.[20] Further, it is believed that the new draft will satisfy the data subject, the user as well as the requirement of EU 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. However, the new Bill by providing different sets of data principles to private and public entities differs from the 1998 Bill.

The obvious difference under the new Bill is that 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:	It 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.
Choice Principle:	This principle allows the individual to opt out to other

[16] Caslon.com, "Caslon Analytics Profile: Australian Privacy Regimes 2006", <http://caslon.com.au/austprivacyprofile3.htm> (accessed 3 June, 2006).

[17] Federal Privacy Commission, "Inquiring into the Provisions of Privacy Amendment (Private Sector) Bill 2000", <http://caslon.com.au/austprivacyprofile3.htm.> (accessed 3 June, 2006).

[18] Multimedia Super Corridor, <http://www.msc.gov.my> (accessed 31 December, 2006).

[19] As the draft is kept under Official Secret Act, only secondary data will be analysed here.

[20] Mohamed Nor, "e-Privacy in the New Economy," *Presented in National Conference Management Science and Operations Research 2003*, vol.2, (Melaka: Century Mahkota Hotel, 24-25 June, 2003), 241.

	purpose for which the data was not originally collected or subsequently authorised by the data subject.
Disclosure 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.
Security Principle:	Security from loss, misuse, unauthorised access, unauthorised 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. This principle further requires that any subsequent disclosure or use must be compatible with the original purpose.
Access Principle:	This allows access to data subject to correct, amend or delete where the personal data is inaccurate. This data principle is not applicable: 1.Where it is proven that the burden or expense of providing access is greater than the risk to the individual privacy or 2. It is shown that allowing access will lead to disclosure of other individual's data where the individual concerned did not consent to such access. 3. 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.[21]

Public sectors, under the new Bill, are only required to comply with three major principles:

1. The principles of collection, use and disclosure as required by law;
2. Right to access by written law; and
3. Responsibility to protect personal data.

The reason for relaxation given to public sector under the Bill is that privacy in the public sector is adequately regulated 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. The existing legislation does not guarantee adequate protection. They cover only small portion of the issue on the whole segment of the right to privacy. These provisions in no way will be able to protect the privacy over the global dossier and as regards the protection of e-heath personal data too the situation remains the same. Some of the obvious weaknesses of the new Bill are:

1. How the voluntary self-regulation and enforcement under the Safe Harbor are to be addressed by providing a single regulatory body for the personal data protection under the Bill is not clear;
2. How the regulatory body is going to be constituted, what are the functions, power and restrictions.
3. 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.
4. It does not provide protection for public record information.
5. Protection is also exempted for any processing of personal data pursuant to "conflicting obligation" or "explicit authorisation" of law.[22]

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 victimised individuals

[21] Ibid., 242-244.

[22] Joel R Reidenberg, "E- Commerce and Trans-Atlantic Privacy," *Houston Law Review*, no.38, (2001), 745.

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. There are 7 data principles that are applicable to private sectors. These principles may control the abuse of personal data for business profitability. However, since the new draft is proposing "opt-out" system, level of protection guaranteed as compared to the Bill 1998 could be seen less. The other problem with the new draft is that the government agencies are exempted from the application of many data principles. As the government is the holder of huge amount of data including e-health data, how far this new law is going to protect personal data privacy is yet to be seen.

5. Acknowledgement
The authors would like to record the appreciation for the research guidance rendered by Assoc. Prof. Dr. Puteri Nemie Jahn Kassim, AIKOL, IIUM.

6. Conclusion

The governments of Australia and Malaysia provided legislative measures that could guide the businesses in collecting, using and storing the health data of individuals. With this legislative guidance the patients are guaranteed that abuse or misuse of health data in whatever form will not be tolerated and severe action will be taken against the individual and corporation that abuses the health data. In Australia, the public sector regulation provides enough protection for health data protection be it online or offline. The private sector regulation was designed to give more freedom to the businesses to decide to come up with the preferred set of rules on e-health data privacy which is to be approved by the Privacy Commission of Australia. The problem with this private sector regulation is that it exempts the small businesses. The Malaysian law on data protection which is intended to protect the e-health data too is still in the drafting stage since 1998. The first draft was modified and redrafted in year 2001 to accommodate various parties. The new draft promulgates two sets of principles. One is for the private sector and the other one for the public sector. The public sector regulations are very minimal and may not be able to strike a balance between the private interest of information privacy and the government's interest to collect, use and store the information.

7. References

[1] Health Online, A Health Information Action Plane for Australia, Retrieved January13, 2008 from www.health.gov.au/healthonline/her_rep.htm

[2] Joan, D. "Protecting eHealth Consumers Regulatory & Normative Issues", *World Health Organization*, USA, 2000, p.3.

[3] Harris Interactive, Survey on Medical Privacy, Louis Harris & Associates, New York, 2004 Retrieved December 13, 2007 from http://harrisinteractive.com/newsletters/HI_HealthCareNews2004Vol4_Iss13.pdf.

[4] Hurriyah-el-Islamy, Protection of Online Privacy & Its Impact on E-commerce, Retrieved December 12, 2007, from http://www.cljlaw.com.

[5] Taylor Nelson Sofres Interactive, Global E-Commerce Report, *Taylor Nelson Sofres Interactiv*e, USA, 2002, p. 2.

[6] Noor Raihan, Elena, & Jawahitha, "Security and Privacy Issues as Barriers to E-Commerce Growth: A Consumer Perspective," *Proceedings the 2003 International Business Information Management Conference*, Cairo, December16-18, 2003, p. 114.

[7] Privacy International, Survey: Malaysia, Retrieved December 15, 2007, from http://www.privacyinternational.org/survey/phr2003/countries/malaysia.htm.

[8] Jawahitha & Mazahir. "Protection of e-consumer Privacy in Malaysia," *International Conference on Intelligent Agents, Web Technologies, and Internet Commerce*, Gold Coast, 2004, pp. 12-14

[9] Abu Bakar Munir & Ganasegran, "The General Consumer Code: Towards Compliance by Internet Service Providers," *CTLR* (3), 2004, pp 64-68.

[10] Caslon.com, Caslon Analytics: Privacy Guide, Retrieved January 13, 2008 from http://caslon.com.au/austprivacyprofile3.htm.

[11] Malcolm, C. "What is Privacy," *Privacy and Security in the Information Age Conference,* August 16-17, 2001, Retrieved January 13, 2008 from http://www.privacy.govau/news/speeches/sp51note.html.

[12] Caslon.com, "Caslon Analytics Profile: Australian Privacy Regimes 2006", Retrieved January 13, 2008 from http://caslon.com.au/austprivacyprofile3.htm

[13] Federal Privacy Commission, Inquiring into the Provisions of Privacy Amendment (Private Sector)

Bill 2000, Retrieved January 13, 2008 from http://caslon.com.au/austprivacyprofile3.htm.

[14] Multimedia Super Corridor, from Retrieved January 13, 200, from http://www.msc.gov.my

[15] Mohamed Nor, "e-Privacy in the New Economy," *Presented in National Conference Management Science and Operations Research 2003*,(2), June 24-25, 2003, Kuala Lumpur, pp.241-245.

[16] Joel, R. R. "E- Commerce and Trans-Atlantic Privacy," *Houston Law Review*, (38) 2001, pp. 745.