BILETA

17th BILETA Annual Conference

April 5th - 6th, 2002.
Free University, Amsterdam.

E-COMMERCE AND PRIVACY ISSUES: AN ANALYSIS OF THE PERSONAL DATA PROTECTION BILL

Ida Madieha Azmi
(Private Law Department,Kulliyyah of Laws,
International Islamic University Malaysia.)

"That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection." [1]

1.0 Introduction

In 1890, Warren and Brandeis have already advanced the notion of privacy, albeit in a limited form of protection afforded to thoughts, sentiments, and emotions. Generally, the right of privacy, in its broadest sense of the right to be alone and anonymous, receives different manifestation, treatment and recognition by legislators[2].

The advancement in computing and net-working, aggravates further the fear of invasion into private lives. The usage of technical means to track down user's surfing and purchasing tendencies by the use of cookies, and sniffers to capture data while in the course of transmissions, has raised a lot of privacy concerns in the cyberspace. All of these anonymous data mining, although may not necessarily brings harm to customers, nevertheless is a form of intrusion into one's privacy in the cyberspace[3].

On this issue Mayor-Schonberger[4] describes the various stages of formulation of laws on privacy right and describe the current notion of privacy in cyberspace as the right to information self-determination. This is where the individual is able to determine how he or she would participate in the collection, processing and the usage of his/her personal data. It is for this purpose that the Malaysian legislators came up with the Personal Data Protection Bill. The importance of this factor is made clear in the explanatory statement of the personal data protection bill in Malaysia.

"New technologies, increasing data collection, changing market trends and the new global market place for electronic commerce are contributing to the increasingly important role of information in the global economy. As such information particularly has become a valuable commodity that can bring jobs, businesses and customer services. Hence, these factors have created a mounting pressure to collect, hold, process and use personal data, more than before. These factors also have reduced the level of privacy and consumer confidence is lacking in such environment."

The purpose of this paper is to examine the nature, manner and scope of personal data protection under the Malaysian Bill. As most of these provisions are based on the UK[5] and Hong Kong Data Protection legislations, decided cases in these two jurisdictions would be helpful in determining the scope of the provisions of the Personal Data Protection Bill[6]. With that in mind, the current ongoing debate between the EU legislative framework and the US self-regulating approach will not

be within the scope of this paper[7].

2.0 The definition of personal data

Under the Bill, the term "personal data" 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."[8]

The above definition will include in its scope:

- Any information or opinion, as long as it is identifiable to a living person, and
- Data which is processed both manually and electronically.

The kinds of data covered under the law are those personal and identifiable to a living individual. Where a particular database contains a combination or personal data and other data, there is a need to distinguish between the two. For example in the case of *R v Barry Rees*[9], the Court of Appeal distinguishes between two types of data in possession of the National Police Computer; i.e. information relating to a living individual who can be identified from that information (personal data) and information in relation to a vehicle or a business but not to any living individual (other data).

Accordingly, as one of the essential elements is the identifiability of the data, like the position in the UK and Hong Kong, anonymised data would not be falling under the definition[10].However, as found in *Ltd, R v. Department of Health Ex Parte Source Informatics*[11], anonymisation does not remove a duty of confidence towards the data subject (in this case in respect of patient's health file) to an action for breach of confidential information.

The definition is relatively broad as it covers not only personal information but also `opinion' and `indications of intentions' made by others on a living individual. For example, when someone approaches a bank with the purpose of gathering house loan, the banker could have made certain opinion on the individual's credit worthiness and hence eligibility for the loan. Such opinion is equally subjected to the personal data protection law. Secondly, the method of processing is irrelevant. The bill seems to govern manually processed data as well even though its explanatory statement makes an explicit reference to new technologies.

The bill further defines the term `data subject' and data user. `Data subject' means `an individual who is the subject of personal data'[12] and `data user' means `a person who either alone or jointly with other persons, controls the collection, holding, processing or use of the personal data but does not include any person who collects, holds, processes or uses solely on behalf of another person'[13]. This means that those who collect materials for a third party will not be falling under the definition.

Any type of processing of personal data will have to be in compliance with all the data principles. Here, the term process is defined widely to mean, `the carrying out of any operation or set of operation on any personal data and includes recording, amendment, deletion, organisation, adaptation, alteration, retrieval, consultation, alignment, combination, blocking, erasure, destruction or dissemination of the personal data[14]'. This means that where files are only retrieved, it is already considered as being processed, and therefore is subjected to the data principles.

The Bill sets up the appointment of a Commissioner for Personal Data protection[15] and a Personal Data Protection Tribunal.[16] Unlike the UK legislation, the Commissioner in Malaysia is answerable to the Minister[17]. This questions the neutrality of the Commissioner as he would be

expected to investigate complaints against government bodies for any breach under the law[18].

The Bill also makes way for the establishment of a code of practice, which would govern all data users[19]. This Code of Practice is to be drafted by a Code Forum, failing which the Commissioner, may himself, issue a code of practice on this area[20].

3.0 Application of the law

It is expressly stated in s 3 of the Bill that the law binds the government. This leaves the question whether the private sector is equally bound by the law or not. In this respect, it has to be borne in mind that the Australian laws have been extended to the private sectors.[21] A broader application of the laws would ensure that there is a comprehensive regime governing the holding, use, correction, disclosure and transfer of information that applies to every entity that involves in such practices.

4.0 Data principles

S 4 of the Bill requires that all the data principles in the schedule is to be complied with whenever any personal data is collected, held, processed or used by data user. These principles are:

Principle 1- Manner of collection of personal data

Data must be collected fairly and lawfully. The method of collection is very important. For this purpose, regards is to be made if the data user is deceived or misled as to the purposes for which the personal data are collected, held, processed or used.

Cookies are commonly used to mine data on the Internet. Such collection of personal data can hardly be considered as lawful or `fair' as it is done without the knowledge and explicit consent of the data subject and hence would seemed to be contrary to this principle[22]. However, as s 105 excludes the collection of data held outside Malaysia, this would mean that though the initial act of collection might be contrary to the first principle, but the storage and processing of data, if done overseas, will not be governed under the Malaysian law.

The data user must also be informed of when and what personal data is collected and the purpose for which the personal data are to be used.

Principle 2 - Purpose of collection of personal data

The purpose of collecting the data must be specified and lawful. In this regard, the collection of data is lawful if it relates directly to a function or activity of the data user, or necessary for that purpose. The data collected must also be adequate, relevant and not excessive in relation to the purpose.

Principle 3 - Use of personal data.

Personal data collected must only be used for the purpose in which the data is collected or any other purposes directly related to that. Once, the purpose of collecting the information ceases, the personal data must be erased, unless such erasure is prohibited under any law or against public interest.

Principle 4 - Disclosure of data

Personal data must not to be disclosed unless in relation to the purpose in which it is collected. In relation to this, s 42 contains certain exceptions such as:

- The data subject or relevant person has consented to the disclosure,
- The disclosure is necessary for the purpose of preventing or detecting crime,

- Disclosure is required under the law, or
- Disclosure is justified as being in the public interest.

The data subject may withdraw his consent for the disclosure of his personal data. In this instance, the data user has a duty to cease to hold, process or use, the personal data.

Principle 5 - Accuracy of personal data

The data user is expected to take all practicable steps to ensure that the data collected are accurate, complete, relevant, not misleading and up-to-date.

Principle 6 - Duration of retention of personal data

Personal data must not be kept for longer than is necessary for that purpose.

Principle 7 - Access to and correction of personal data

This right of access is further explained in s 32. The essential elements of this right are:

- To be informed of the collection of personal data, and this overlaps with principle 1,
- If collection is done through automated means, to be informed of the logic involved in the decision making.

The right of access is only available upon request in writing by the data subject. Under the Bill, the data user must comply with the request not later than 45 days of the request[23]. The Bill went further to determine circumstances in which the data user may refuse with the data subject's request. This is in a situation whereby:

- The request is not in writing,
- Insufficient information from the data subject,
- If the disclosure may lead to the revelation of another individual.

The data user must notify the data subject of such refusal as soon as practicable but not later than forty days after the request[24].

The right of access is intertwined with the right to correct data as the former is normally done to invoke the latter[25]. The Bill stipulates that the request to correct data must be complied with within forty-five days.[26] For this purpose, the Bill equips the same ground and the same notification requirement, equivalent to the right of access, for data user to refuse the data subject's request[27].

Corollary to the right to correct data is the right to prevent the collection of data that are likely to cause substantial damage or unwarranted distress to the data subject or to another individual[28].

With regards to personal data held for employment purposes, s 114 exempts the access right until the expiration of seven years after the appointed date.

Principle 8 - Security of personal data

The data user is expected to take all steps to safeguard against unauthorised or accidental access, processing or erasure to, alteration, disclosure or destruction of, personal data and against accidental loss of personal data. All these steps will be relevant:

- The place or location where the personal data is stored,

- The security measures incorporated into any equipment in which the personal data are stored,
- The measures taken for ensuring the reliability, integrity and competence of the personnel having access to the personal data,
- The measures taken for ensuring the secure transmission of the personal data.

Principle 9 - Information to be generally available.

The data user must inform the data subject of:

- Its policies and practices in relation to personal data,
- Be informed of the kind of personal data held by the data user; and
- The purpose for which the personal data held are to be used.

5. Duties of a data user

First and foremost, the Bill requires the registration of the data user. A data user is a person who either alone or jointly with other persons, controls the collection, holding, processing or use of the personal data but does not include any person who collects, holds, processes or uses solely on behalf of another person[29].

A data user is expected to submit a form filled with relevant particulars. Among the relevant particulars specified in the second schedule is:

- The name and address of the data user,
- A description of the personal data,
- A description of the purpose of which the data is held,
- A description of the source from which the data user wishes to obtain the personal data,
- A description as to whom the data user intends to disclose the personal data,
- The name of the place outside Malaysia which the data user intends to transfer personal data,
- Address/es for the receipt of request from the data subject for access to the personal data, and
- A description of measures to be taken for the purpose of complying with data protection Principle 8.

The data user return requirement is cumbersome as it delays the process of collection of data and if enforced would prove to be unpopular. At the moment, it would seem that all data users are subjected to this law as the Minister has not yet specified who are exempted from this duty. During the consultation process, many industries argue of the need to waive this requirement, as it is not only impractical but also difficult to implement. If enforced strictly many entities may fall foul of the law just because they fail to register and not because of non-compliance with the data principles[30].

6. Rights of the Data Subject

Generally under the Bill, a data subject is entitled for:

- Right of access to personal data[31],
- Right to correct personal data[32],
- Right to prevent the collection of data that is likely to cause damage or distress,[33]
- Right in relation to automated decision-takings,[34]
- Non disclosure of personal data[35],
- Withdrawal of consent for purposes of usage of data[36],
- Erasure of personal data that is no longer required.[37]

Most of these rights are intertwined with the data principles and are already covered earlier.

7. Direct marketing

The importance of personal data for direct marketing purposes is obvious. Targeted advertisement proves to be more efficient that mass advertisement. It is for this purpose that many companies that specialises on the collection and the profiling of users data operates on the Internet[38].

The Act of direct marketing is defined under the Act to mean:

(a) the offering of goods, facilities or services;

(b) the advertising of the availability of goods, facilities or services; or

(c) the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes, by means of-

(i) information or goods sent to any person by mail, facsimile transmission, electronic mail or other similar means of communication, where the information or goods are addressed to a specific person or specific persons by name; or

(ii) telephone call made to specific persons[39].

Under the Act the data user must inform the data subject about the use of his personal data and if so requested by the data subject, to cease the use of his data. This opt-out requirement is short of the expectation of the first data principle, which requires the opt-in consent of the data subject before collection is done. Another point which needs to be considered is the legality of using cookies to collect data on surfers. Some commentators argue that such use contravenes the first data principle that the manner of collection must be `fair'. Therefore, any banner advertising company that uses cookies to collect information must provide suitable notice to the data subject[40]. In this respect looking at how the US courts treats the issue of `authorization' in *In re DoubleClick Inc v Privacy Litigation*[41], one wonders whether `fairness' can easily be overridden by commercial needs. The same concern occurs *from R (On the Application of Robertson) v City of Wakefield Metropolitan Council*[42] where the Mr. Justice Maurice Kay dismisses the submission that the sale of electoral role amounts to a breach of the UK Data Protection Act 1998. He however accepted the submission that such sale without the consent of the data subjects may be a concern under the Human Rights Act.[43]

8. Matching procedure

The use of personal data for matching procedure is absolutely prohibited[44] unless both the data user and the Commissioner consents to the procedure following a request made in s 49. This prohibition, however, does not apply to government departments, so long as a notice to the effect is submitted to the Commissioner. The prescribed matters which needs to be notified to the Commissioner in this respect are underlined in the Third Schedule.

A matching procedure is defined under the Bill to mean:

"any procedure whereby personal data are collected for one or more purposes in respect of ten or more data subjects are compared (except by manual means) with personal data collected for any other purpose in respect of the data subjects where the comparison:

(a) is (whether in whole or in part) for the purpose of producing or verifying data that; or

(b) produces or verifies data in respect of which it is reasonable to believe that it is practicable that the data,

may be used, whether immediately or at any subsequent time, for the purpose of taking adverse action against any of the data subjects[45].

The restriction on `matching procedure' would pose considerable difficulties on industry that depends substantially on them such as the insurance and credit card industry. This prohibition was one of the major concerns of the private industries in Malaysia. During the consultation process some of them have requested for specific industry exemption from the application of the law.

9. Sensitive Personal Data

The Bill makes a distinction between personal data and sensitive personal data. The term 'sensitive personal data' is, however, not defined under the Act and is to be left entirely within the power of the Ministry to decide. Generally these types of information are considered as sensitive personal data:

- Racial or ethnic origins,
- Political opinions,
- Membership of political association,
- Religious beliefs or affiliations,
- Philosophical beliefs,
- Membership of a professional or trade association,
- Membership of a trade union,
- Sexual preference or practices,
- Criminal record,
- Individual health information[46].

For these types,of data, the collection, holding, processing or use of them is strictly prohibited except in accordance with the conditions specified in the Fourth Schedule of the Bill[47]. Certain categories of use of sensitive personal data is exempted under the Bill which includes:

- in connection with employment,
- for the purpose of any legal proceedings or legal advice and the administration of justice generally,
- collected by a healthcare professional for medical purposes, and
- use by NGOs, non-profit organisations and trade unions[48].

The basic premise behind the rigorous protection of personal data perishes with the demise of the `data subject'. In this instance, the Malaysian law provides that these sensitive personal data will be exempted from the data protection principles if they are still held by the data user ten years after the death of the data subject[49].

10. Data held outside Malaysia

Section 105 provides an explicit exclusion for data held outside Malaysia, unless in these circumstances:

- The personal data are used or intended to be used in Malaysia, or
- If the control of the collection, holding, processing or use of personal data is done through an agent in Malaysia.

The exclusion to data held outside Malaysia is again another express derogation from the general principles. The current practices of big and established foreign web site proprietors of using cookies to collect information on web site surfers will not be governed under the law. In fact, this is the major worry of some of the Internet users, that is, their personal data are anonymously collected, profiled and maintained by foreign entities through the usage of cookies[50]. In terms of

enforcement, it would be very difficult to catch all these practices under the domain of the data protection law. For example, one can imagine a situation in which a non-Malaysian company creates a web site, sends cookies to Malaysian internet surfers and collects cookies containing personal data from their hard disks. The information gathered is then sold to other non-Malaysian companies that start advertising their products or services to these targeted customers. This constitutes a violation of the Malaysian law, but enforcement would be very difficult.

11. Transborder data flow

The European Union was the first to come up with a regulation to restrict transborder data flow to a third country, unless that country ensures an "adequate level of protection" for data subjects[51]. The concern over the transborder flow of data is understandable given the border-less nature of the Internet. In this respect the Malaysian provision is broader as it also takes into account countries which has in force laws that serve the same purpose as that of personal data protection. The Malaysian provision thus provides that the transfer of any personal data is not allowed unless to places which:

- Has in force any law which is substantially similar to, or serves the same purpose as the personal data protection law, or
- Ensures an adequate level of protection for the rights of the data subject[52].

This provision leaves a lot of questions raised. In particular, how do we determine, and what criteria are we to take, whether a particular jurisdiction has `adequate level of protection' or `serves the same purpose as the personal data protection law? Would a country that practices self regulation, like the US, be considered as meeting the requirement? This notion is highly debatable as many critics are of the view that the US self-regulation system or the negotiated safe harbour[53] rules fall short of the expectation and therefore not `adequate'[54]. Equally debatable is third party verification services such as TRUSTe[55]. Website verification services assure consumers that the particular website bearing its seal is audited to ensure specified consumer safeguards. Would these services be considered as providing `adequate protection'?

Certain exceptions are provided under the Act, in relation to:

- Where the transfer of data is necessary for the performance of contract between the data user and the data subject or the taking steps with the view of entering into contract,
- The transfer is necessary for the conclusion and performance of a contract entered into between the data user and a person other than the data subject but is entered into at the request of the data subject,
- For the purpose of legal proceeding, obtaining legal advice and establishing, exercising or defending legal rights,
- To protect the vital interests of the data subjects,
- The recipient of the personal data is subject to a binding scheme or contract with the data user,
- The transfer is necessary for reasons of public interest[56].

These exemptions relates to circumstances in which either the data subject themselves require the transfer of data for the conclusion, performance of contract or when public interest overrides the interest of the data subject.

Exemptions

The Bill lays down a number of exemptions, depending on the urgency and justifiability of the use of personal data. On that basis, national security, defence or international relations is considered as a legitimate factor for the exemption of almost all of the data principles, with the exception of

principle 8[57]. This means that government bodies that require personal data for those purposes are only required to safeguard the security of personal data under Principle 8.

Next on the list are crime, taxation,[58] judicial appointment[59], staff planning[60] and relevant process[61]. All of these purposes are exempted from principles 3, 4, and 7. Personal data sought on any of these grounds will not need to comply with the principle of use, disclosure and accuracy of data.

All of these exemptions illustrate situations where `privacy' is a matter of "balance" rather than human right. In relation to the use of personal data for legal action, the case of *Totalise plc v Motley Fool Ltd* [62]will be of assistance. In this case the defendant (a financial web site) sought to raise DPA 98 as a defence to an action raised by the plaintiff (the internet service provider) who wanted to discover the identity of a subscriber who had been posting defamatory remarks about the plaintiff on the defendant's bulletin. The defendant removed the defamatory materials but argued that the disclosure of the identity of the subscriber would breach Data Protection Act 1998.

Robert Owen J held that s 35 permitted disclosure to be made if this were necessary for legal proceedings (including prospective legal proceedings) irrespective of the identity of the parties.

The list of the exemptions are enumerated in the following table:

Purpose	Exemptions
National security, defence or international relations	Principle 1,2,3, 4, and 9.
Crime, taxation	Principles 3, 4, 7
Health	Principle 7
Social work	Principle 7
Regulatory functions	Principle 7
Judicial appointment	Principle 3, 4, 7
Legal professional privilege	Principle 7
Domestic purpose	Total exemptions
Staff planning	Principles 3, 4, 7
Relevant process	Principles 3, 4, 7
Personal reference	Principle 7
Statistic and research purposes	Principles 3, 4
News activity	Principle 4
Sensitive personal data after death	Total exemptions
Information available to the public	Principles 4, 5, 7.

Conclusion

The Malaysian government is introducing a multi purpose smartcard to replace the existing ID cards. The card will have several applications, including personal details of the holder, driving licence, immigration, health details and also credit card. The idea is to have one card that contains all possible personal details of a person besides serving as a credit card. This idea, novel as it seems, may implicate privacy concerns as the potential of abuse is enormous[63].

In following the discourse on the interface between privacy and technology, it should not be forgotten that under the Malaysian Constitution, privacy is not a fundamental human right. Be it as it

is, the incentive to regulate against the invasion of individual's privacy either by the government or by the commercial sector does not reign supreme. It is because of this that the attempt to introduce laws to the effect is facing considerable objections by many industries and delaying the passing of the law.

Whatever praises the new law hails, it has to be borne in mind that it is hardly a privacy law that endorses the notion that `one must be left alone'. Instead this legislation is information laws, protecting data before people. Instead of being concerned with the full range of privacy and surveillance issues, it deal only with the way personal data is collected, stored, used and accessed'. Exploring that idea further Davies opines that the present data protection legislation suffers from two main flaws. The first and most obvious is that they tend to allow many privacy violations to occur through exemptions for law enforcement and taxation. It is on this point that the Malaysian Personal Data Protection Bill is a true testimony. The wide variety of exemptions available, in particular with respect to national security, defence or international relations, defeats the whole purpose of coming up with the law. The second is that data -protection law does almost nothing to prevent or limit the collection of information, it merely describes the manner of collection and processing of data[64].

With regards to the suggestion that data privacy be regulated by self regulation and not through government-made laws, it is submitted that in the face of commercial might, this may not be a viable option[65]. In Malaysia, recently, the Multimedia and Communication Commission has drafted a framework of Internet Code of Conduct for Internet users. While the Code of Conduct is an example of self-regulation, the implementation of the Code is strongly backed by legislation, i.e. the Communication and Multimedia Act 1998. In this respect, the new Bill is very much welcomed and its immediate promulgation and subsequent implementation is awaited anxiously by many quarters of the society.

---

[1] Warren & Brandeis, 'The Right to Privacy', *Harvard Law Review*, Vol IV, December 15, 1890.

[2] There are four types of privacy right, informational privacy, territorial privacy, personal privacy and communications and surveillance privacy. In Europe for example, *The Charter of Fundamental Rights of the European Union* (Official Journal 2000C 346/01) carries a broader notion of privacy right.

[3] See Eugene Clark & George Cho, `Privacy in an e-Business World: A Question of Balance', *Journal of Law and Information Science*, Vol. 11 No 1, 2000/2001.

[4] 'Data Protection in Europe', in *Technology and Privacy: the New Landscape*, edited by Philip E. Agre and Marc Rotenberg, (1998, MIT Press, Massachusetts). He views that in the west, privacy rules were developed out of concern over government surveillance on their citizens. With the advancement of computers, in the 1980s, there is a shift in the perception of privacy and privacy invasion, resulting in the formalisation of rules in the form of data-protection principles.

[5] For UK experience, read the useful advice given by Kenneth Meechan, `Time's up', *Solicitor's Journal*, 19 October 2001.

[6] There are a number of other countries that have similar legislations such as Spain, see Sonia Cortes, `Data Protection Under Spanish Law': [2000] *CTLR* 71. For Hong Kong, see, Mark Berthold & Raymond Wacks, `*Data Privacy Law in Hong Kong'*, (1997) Pearsons Professional (Hong Kong) Limited. For UK, see, David Bainbridge, *Introduction to Computer Law*, Pearson Education Limited (2000), Fourth Edition. See also Chan-Mo Chung, `Korea's Recent Legislation on Online Data Protection, *Privacy Law and Policy Reporter*, austlii database; Robyn Durie, `An Overview of the Data protection Act 1998', [2000] *CTLR* 88 and Bruce Leorgburu, `Doing Business Between the EU

and New Zealand: What Do You Have to Do to Protect Personal Information These Days', [2000] *CTLR* Issue 4 p. 94.

[7] For further reading on this issue, see, Overstraeten and Szafran, `Data Protection and Privacy on the Internet : Technical Considerations and European Legal Framework', [2001] *CTLR* 56.

[8] S 2 of the Bill.

[9] [2000] EWCA Crim 55, 20th October, 2000.

[10] See *R v DoH, ex p Source Informatics Ltd* [2000] 2 WLR 940, where the Court of Appeal held that the European Directive did not have any applicability to the use of anonymised data, although the Commissioner has expressed doubts as to how truly anonymous data can ever be made, and emphasizes that anonymising data will in itself constitute processing and have to comply with the Act.

[11] [1999] EWHC 315. In the words of Mr Justice Latham:

"Anonymisation (with or without aggregation) does not, in our view, remove the duty of confidence towards the patients who are the subject of the data. Apart from the risk of identification of a patient despite anonymisation, the patient would not have entrusted the information to the GP or the pharmacists for it to be provided to the data company. The patient would not have been aware of or have consented to the information being given to the data company, but would have given it to be used in connection with his care and treatment and wider NHS purposes. Anonymisation of the data (with or without aggregation) would not obviate a breach of confidence."

[12] Section 2 of the Bill.

[13] Section 2 of the Bill.

[14] Section 2 of the Bill.

[15] See section 5, on the terms of appointment, s 6 on the powers and functions of the Commissioner, s 7 on the power to delegate certain powers and s 8 on the duty to maintain secrecy.

[16] See s 9 on the establishment of the Tribunal, s 10 on the resignation and termination of appointment, s 11 on the suspension of members, and further s 12-17.

[17] Section 5(4) of the Bill.

[18] The Act applies both to the private sector and government bodies.

[19] Part V of the Bill.

[20] See s 25 of the Bill.

[21] See the amendment to the Australian Privacy Act 1988.

[22] This is the view of Dominic Callaghan, `Cookie Regulation in Australia', [2001] CTLR 106.

[23] S 33 of the Bill.

[24] S 34 of the Bill.

[25] S 36 of the Bill.

[26] S 37 of the Bill.

[27] S 38 of the Bill.

[28] S 40 of the Bill.

[29] The UK case of *R v Griffin*, (unreported) would be relevant here. In this case, Rise LJ and Waller J, of the High Court found that an accountant who prepared spreadsheets from accounting records provided by his clients and used them to prepare accounts for submission to taxation and other authorities on their behalf is a data user.

[30] See the result of *Re Griffith*, supra.

[31] S 32 of the Bill.

[32] S 36 of the Bill.

[33] S 40 of the Bill.

[34] S 41 of the Bill.

[35] S 42 of the Bill.

[36] S 43 of the Bill.

[37] S 44 of the Bill.

[38] See further Van Overstraeten and Szafran, supra.

[39] S 52(2) of the Bill.

[40] See Dominic Callaghan, Cookie Regulation in Australia, [2001] *CTLR* 106.

[41] 2001 U.S. Dist. LEXIS 3498. In this case, the US District Court for the Southern District of New York found that as the defendant collected data from their affiliated web sites, the submissions containing `personal data' made by users to defendant's affiliated web sites were all `intended' for those web sites, therefore the web sites' authorization was sufficient to except Doubleclick's access.

[42] [2001] EWHC Admin 915

[43] He made express reference to *X v United Kingdom* 30 DR 239 which concerned the compulsory completion of a census form which includes details of sex, marital status, place of birth and other personal details, *Ms v Sweden* 28 EHRR 313 which concerns the disclosure of medical records and *Regina v Chief Constable of North Wales Police, ex parte Thorpe* [1999] QB 396 which concerns the disclosure by the Police of the fact that local residents are convicted paedophiles..

[44] s 48 of the Bill.

[45] s 2 of the Bill.

[46] see Eugene Clark & George Ho, `Privacy in an e-Business World: A Question of Balance,

Journal of Law and Information Science, [2000] Vol 11, No.1, p.7

[47] S 54 of the Bill.

[48] Fourth Schedule of the Bill.

[49] s 85 of the Bill.

[50] The biggest litigation on privacy in the US is Double Click.com.

[51] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and of free movement of such data, Official Journal L 281, 23/11/1995 p. 0031-0050.

[52] S 55 of the Bill.

[53] See http://europa.eu.int/comm/internal_market/en/media/dataprot/news/safeharbor.htm.

[54] This is the view of Andrew Charlesworth in his article. For other countries that have been granted "adequate protection" status see Switzerland and Hungary. See also Tanguy Van Overstraeten and Emmanuel Szafran, `Data Protection and Privacy on the Internet: Technical Considerations and European Legal Framework', [2001] *CTLR*, 56.

[55] TRUSTe is a non-profit organization issuing a seal. The objective of TRUSte is to promote online privacy awareness and increase consumer confidence about the collection and use of private, personal information.

[56] S 55(5) of the Bill.

[57] S 72 of the Bill.

[58] S 73 of the Bill.

[59] S 77 of the Bill.

[60] S 80 of the Bill.

[61] S 81 of the Bill. "Relevant process" generally means the process whereby personal data are considered by one or more persons for the purpose of determining the suitability or eligibility of candidate or a particular job, promotion, contract or award, scholarship, hounours or for the purpose of disciplinary action.

[62] [2001] EMLR 29

[63] See `Chip cards on the Rise', *IT Malaysia*, April/May 1997 p.2.

[64] Simon G. Davies, `Reengineering the Right to Privacy: How Privacy Has Been Transformed From a Right to a Commodity', p. 156 in Philip E. Agre and Marc Rotenberg, `*Technology and Privacy: the New Landscape*, (1998, Cambridge University Press, Massachusetts)

[65] See the observation of Andrew Charlesworth on the downside of self regulation in his article, `Data Privacy in Cyberspace', in Lilian Edwards & Charlotte Waelde, `*Law and the Internet, a Framework for Electronic Commerce'*. (Hart Publishing, Oxford-Portland Oregon, 2000)