E- COMMERCE AND DATA PROTECTION LEGAL FRAMEWORK IN MALAYSIA: LESSONS FROM THE EXPERIENCES OF THE EUROPEAN UNION AND THE UNITED KINGDOM

MOHD BAHRIN BIN OTHMAN *

*PhD Researcher **
*Cyberlaw & Policy Centre, Faculty of Law, Universiti Teknologi MARA, 40450 Shah Alam, Selangor **
mohdb916@johor.uitm.edu.my , mohdbahrin@yahoo.com *

ABSTRACT

The use of customer data is often an essential part of any business but those involved in E-Commerce in particular make regular use of customer and user personal data for a variety of reasons. Multinational sourcing of data-based tasks is one of the practices that have become widespread as a result of the Internet. Data protection and privacy are a growing legal challenge for policy makers and corporations, as numerous countries have or are considering new laws to protect individual data and privacy. This paper is drawn from an ongoing doctoral research which is aimed at evaluating the state of global data protection legal framework from various regional and national perspectives and identifying a viable model for a comprehensive data protection law viable for Malaysia, that would enable the reconciliation of conflicting interests between the policy maker, organization and society, as well as between individual information privacy and trade interest. Examination into the Malaysian proposed Bill on Personal Data Protection, the European Union's Directive 95/46/EC and the Data Protection Act in United Kingdom in 1998 will be made.

KEYWORDS

E-Commerce, Personal Data, Data Protection, Privacy.

1. INTRODUCTION

The use of customer data is often an essential part of any business but those involved in E-commerce in particular make regular use of customer and user personal data for a variety of reasons. This data can range from the names and addresses of the customers to the usage statistics recorded by the e-tailer as a customer uses the website (Simons & Simons, 2001). Data protection and privacy are a growing legal challenge for policy makers and corporations, as numerous countries have or are considering new laws to protect individual data and privacy. This is part of a worldwide trend to give greater privacy protection to personal information in the private sector. These laws in large part reflect the growing concern of consumers that their personal information is not protected adequately (Bentivoglio et al., 2003).

This paper is drawn from the ongoing doctoral research on the viability of data protection legal framework in Malaysia. The collection and processing of personal data within the E-Commerce practices, the increasing relationship with the Internet, and subsequently the increasing importance of personal data for effective businesses will be discussed in the first section of this paper. The second section of this paper examine the data protection legal framework of the European Union and United Kingdom for the comparative aspects and highlights the issue of the complexity of the laws relating to the exchange of E-Customers' personal data. The third section of this paper describes the state and efforts of data protection in Malaysia. The paper ends by discussing the need to ascertain a model for data protection law in Malaysia which would reconciliate the conflicting interests between the policy maker, organization and society, as well as between individual information privacy and trade interest.

2. THE PROCESSING OF PERSONAL DATA IN THE E-COMMERCE ENVIRONMENT

"E-Commerce" refers to all forms of business transactions conducted over public and private computer networks. It is based on electronic processing and transmission of data, text, sound and video. E-Commerce includes transactions within global Information Economy such as electronic trading of goods and services, online delivery of digital content, electronic fund transfer, electronic share trading, electronic bills of lading, commercial auction, collaborative designs, engineering and manufacturing, online sourcing, public procurement, direct consumer marketing and after sales services (Sarabdeen Jawahitha, 2004).

The cyberspace intensive environment and flourishing of E-Commerce have created opportunities as well as posed new treats to the way we manage and share information about us. Individuals' personal data, for example, on an individual's financial and credit card records could easily be obtained, accessed, transferred, and illegally used by unauthorized persons (Samoriski, 2002). Furthermore, companies can now easily gather, analyze and market customer data throughout the world.

Multinational sourcing of data-based tasks is one of the practices that have become widespread as a result of the Internet. The low costs of storing and processing information and the ease of data collection have resulted in the prevalence of data warehousing[2] and data creep[3]. These trends result in an increasing amount of personal data collection and whenever any of these practices involve international transfers of data, differences in data protection schemes give rise to conflict (Moshell, 2005).

At the practical level, such activities raise at least four kinds of privacy concerns. First, databases can be used to process sensitive information which potentially embarrassing or highly personal information. Second, data matching can be created, composed of non-sensitive information in such enormous quantities that the database constitutes a highly detailed of a person's existence. Third, the information contained in consumer profiles can be quite inaccurate. Finally, there are no meaningful legal requirements that personal information in consumer profiles can be kept securely. If used improperly, the detail contained in consumer profiles can facilitate crimes such as identity theft, stalking or harassment (Richards, 2005).

From the businesses perspective, markets tend to achieve maximum economic efficiency with maximum information. In this context, privacy rights become an issue because strong privacy rights restrict the potential availability of highly relevant information potentially leading to adverse selection or inefficient allocation of resources. In contrast, a week data protection laws enable businesses to make more informed choices and mass customization of products (Dam, 2005). In addition, the public understanding of technology and data is arguably minimal. Accordingly, individuals may not have a strong sense of the information privacy they want or need. Some individuals may be very sensitive to use of their personal information and others may not notice or particularly care. Studies tend to show that consumers do not have a particularly good understanding of personal data collection. In such a climate, the adopted law should not have large loopholes and weak enforcement mechanisms (McKay, 2005). Another important issue is the compliance costs arising from the law. Economists argue that governments should minimize compliance costs imposed by legislation as much as possible because there is a negative impact on society and the economy where these costs are excessive. Specifically, excessive compliance costs divert resources away from the core interests the business is engaged (Harding, 2005). This leaves less money for expansion and investment in research and development.

These arguments reflect extreme positions. Whatever data concerning individuals is collected in the E-Commerce environment and however it is to be used, the laws governing data protection must be considered. Therefore, the need is to develop a balance approach to free trade and privacy protection.

---

2 Long-term storage of information

3 Collection of increasingly minute details about an individual that allow an extensive profile to be assembled

3. THE DATA PROTECTION LEGAL FRAMEWORK AND ITS IMPLICATION FOR E-COMMERCE

Because of the globalization of markets and increased use of the Internet, data protection laws are bound to become a major source of contention in the push to increase international commerce especially the E-Commerce. In fact, these laws have already created tension: those who wish to utilize the 'boundary free' nature of the Internet are realizing that data protection laws create de facto boundaries that can be just as effective physical borders. Information privacy is an important national concern as each country tries to bolster confidence in E-Commerce by providing data protection that it citizens want, without creating excessive regulatory compliance costs. Information privacy concerns arose long before the Internet, however, and have been the subject of policies and regulations throughout the world for many years (McKay, 2005).

The regulatory models on how to protect individuals' personal information varies significantly around the world. The European Union's ('EU') approach, comprehensive command and control data protection model with precise rules governing the handling of personal information, occupies one end of the regulatory spectrum. The United Kingdom ('UK') legislation governing data protection is the Data protection Act, 1998, ('DPA 1998') which flows directly from the EU Directives (Carey, 2004). On the other end is the self-regulatory and sectoral model like the United States that relies largely upon a market-based solution to privacy. In the middle is the Australian model, often called a 'co-regulatory' or 'light touch' model (McKay, 2005).

3.1 The European Union Data Protection Legal Framework

Privacy is a constitutional right in all the EU countries, which seek to safeguard personal information about their citizens. Each of the EU Member States[4] has its own data protection commissioner, a privacy watchdog. Europe's enthusiasm for privacy is part of the response to the region's experiences in World War II. In 1950 the EU Convention on Human Rights and Fundamental Freedoms was ratified. Among other rights it guaranteed European citizens an explicit right to have their private and family life, home and correspondence protected from state interference without a lawful justification. In 1980 the Organization for Economic Cooperation and development (OECD) adopted guidelines governing the protection of privacy and transborder flows of personal data (Jay, 2004).

The EU approach to data privacy protection stems from the basic principles of Guidelines and the Conventions. The EU Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data ('EU Directive) was passed in October 1995. It set forth a general framework for European data protection law with the intent to create uniformity in the processing of personal information across member states (L.Rustad and H.Koenig, 2005).

The Data Protection Principles provided by Article 6(1) of the EU Directive, form the backbone of the EU Directive. In the case of *Rechnungshof v Osterreichischer Rundfunk and others (2003)*, the European Court of Justice recognized that the EU Directive is adopted on the basis of Article 100a of the Treaty. It intended to ensure the free movement of personal data between Member States through the harmonization of national provisions on the protection of individuals with regard to the processing of such data. Article 1, which defines the objectives of the EU Directive, provides in paragraph 2 that Member States may neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection of the fundamental rights and freedoms of natural persons, in particular their private life, with respect to the processing of that data. Since any personal data can move between Member States especially in E-Commerce, the EU Directive requires in principle compliance with the rules for protection of such data with respect to any processing of data defined by Article 3. Simultaneously any processing of personal data in the E-Commerce environment , in the community must be carried out in accordance with the law of one of the member states.[5]

The EU Directive consists of a number of obligations, with which European data controllers must comply when processing personal data (Carey, 2004). Member State shall provide that personal data must be[6], firstly, processed fairly and lawfully. Secondly, collected for specified, explicit and legitimate purposes

---

4 The European Union members are Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, Netherlands and the United Kingdom

5 Preamble (18) of the EU Directive 95/46/EC

6 Article 6(1)(a)(b)(c)(d)(e) of the EU Directive 95/46/EC

and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards. Thirdly, adequate, relevant and not excessive in relation to the purposes for which they are collected/or further processed. Fourthly, accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified. Fifthly, kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use. Article 5 additionally provides that Member States shall within the limits of the provisions of the EU Directive determine more precisely the conditions under which the processing of personal data is lawful.

Under the EU Directive, the personal data must not be processed without the consent of the data subject unless that processing is necessary for performance of a contract with the data subject or a specific exception applies (Moshell, 2005). Personal data stored on a company Web site or internal IT network must also be kept up to date or discarded if no longer needed. If someone buys something through E-Commerce from a company once and the company keeps that customer's personal details for twenty years that retention could be considered unreasonable under data protection law. Any personal data that a company retains must be pertinent to the business (Cohen, 2003). E-Customer records no longer relevant to a business must be destroyed responsibly under the EU Directive. The EC Directive provides that the E-Customer has the right of access to and the rectification or erasure of his personal data. In other words, an E-Customer has the right to inspect personal data and to check that the company is using it for a good reason. If the E-Customer not satisfied that this is the case, he can complain to data protection authorities, which would carry out a formal investigation (Cohen, 2003).

The EU Directive covers all sectors of EU Member States economics and grants strong protection to data containing individuals' personal information. E-Customers are given the right to sue over alleged breaches, and member states have an obligation to form government privacy agencies that will enforce the law and educate the public on privacy (McKay, 2005). Since October 1998, the European member States have been enacting national privacy statutes to comply with the EU Directive (L.Rustad and H.Koenig, 2005).

Dissatisfied with the mere implementation of the Directive in the member states, the EU issued Regulation 45/2001 in 2000, creating the European Data Protection Supervisor who is an independent supervisory authority[7], for the monitoring[8] of applications of the EU Directive by the EU institutions and bodies.

These comprehensive command and control model is preferred by nations that have no existing system for protecting personal data and are just beginning to implement data protection protocols, primarily because the key concept behind the comprehensive model is enforceability. The comprehensive approach works particularly well in countries that strictly adhere to a system of general law and government oversight (Moshell, 2005).

The EU Directive is often accused of failing to address privacy coherently because it does not account of those that it governs. The Directives failed to take into account the vast differences in rights, powers and incentives between the European Union member states' respective governments and the private industry. This resulted in the divergence of privacy standards between the EU member states (Moshell, 2005). Furthermore the government control would occur because the central provisions of the EU legislation give the government greater control over personal data, despite information privacy being characterized as fundamental human rights. The EU Directive effectively expands government influence rather than curtails it (Moshell, 2005).

The EU Commission reasoned that the Directive's lack of success is attributable to inexperience on the part of member states, incorrect application of the Directive's principles and attempts by governments to reduce the private sector's compliance burdens. The Commission also admitted that enforcement of the Directive after implementation is a problem, primarily because, first, supervisory and enforcement authorities usually do not have access to sufficient resources. Second, violators' low risk of being apprehended. Third,

---

[7] The Supervisor is an entity completely independent from European Parliament and Commission, taking no instruction from external authority

[8] The Supervisor is in charge of hearing and investigating complaints and generally advising the entirety of the European community on data protection matters, either upon request or on the office's own initiative.

lack of enforcement (Moshell, 2005). The EU also carries international implications. It is suggest an attempt by the European Union to exercise jurisdiction over foreign activities .

3.2 The United Kingdom Data Protection Legal Framework

The United Kingdom ('UK') legislation governing data protection is the Data protection Act, 1998, ('DPA 1998') which flows directly from the EU Directive. The DPA 1998 came into effect in March 2000. This Act implements into the domestic law of the UK the EU Directive. Having the same standards of data protection across the EU means that personal information may travel freely between the EU Member States. The DPA 1998 replaces the Data Protection Act, 1984, and represents a major progression in the law with regard to how personal information or personal data may be treated (The Joint Information Committee, 2006).

The DPA 1998 seeks to strike a balance between the rights of individuals and the competing interests of those with legitimate reasons for using personal information. It gives individuals certain rights regarding information held about them. It places obligations on those who process data ('data controllers') while giving rights to those who are the subject of that data ('data subjects')(Information Commissioner's Office, 2006).

The DPA 1998 sets out a clear framework on how those dealing with data may treat personal data. The Act allows the E-Customer (the data subject), to assert greater control over how his personal information is gathered, used, housed and shared by providing for a number of rights and remedies which are easily applicable. In addition to actively promoting security and privacy of information in general, the Information Commissioner is the supervisory authority of the DPA 1998 and the Freedom of Information Act, 2000 (The Joint Information Committee, 2006).

The drafters in producing the Eight Principles in Schedule 2 to the DPA 1998, reproduced the obligations in Article 6, Article 8 (sensitive personal data), Article 10 and 11 (information to data subjects), Article 12 to Article 15 (rights of data subjects), Article 17 (process personal data securely) and Article 25 (overseas transfers) of the EU Directive (Carey, 2004). The Principles[9] are, firstly, personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Schedule 2 is met, and in the case of sensitive personal data, at least one of the conditions in Schedule 5 is also met. Secondly, 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. Thirdly, personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. Fourthly, personal data shall be accurate and, where necessary, kept up to date. Fifthly, personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. Sixthly, personal data shall be processed in accordance with the rights of data subjects under this Act. Seventhly, appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Finally, personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Section 4(4) provides that it shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller.

3.3 The Complexity Of The Laws Relating To The Exchange Of E-Customers' Personal Data

The Member States will no longer be able to restrain the free movement between them of E-Customers' personal data on the grounds relating to the protection of the rights and freedoms of individuals.[10] It also introduced regulations that made transfer of such data to countries outside the EU dependent on 'adequate level of protection' there.[11] In other words, while facilitating trade within the EU, the Directive could become a serious obstacle to E-Commerce with countries outside EU, if their level of protection was judged to be inadequate (Busch, 2005).

---

9 Part 1 of Schedule 1of the Data protection Act, 1998

10 Preamble Section 9

11 Article 25

This provision is intended to protect the E-Customers located in the EU. With the passage of time Europe is increasing its effort to balance the needs of European individuals to receive rights and a level of protection to which they have accustomed, with the practices of foreign companies, especially American companies, which have been used to operate in a different cultures, and rely on different values to conduct business (Gilbert, 2005).

The issue of transborder data flows relating to the exchange of E-Customers' personal data can be approached from different viewpoints, and different actors can take different positions with respect to these viewpoints. For the issue of transborder data flows, three different frames can be hypothesized to exist. One can be labelled 'economic interests' and focuses on questions of cost effectiveness, profit and market extension. Another one can be labelled 'safety interests' and is concerned with such things as reduction of risk and prevention of misuse. A third one can be described as 'civil liberty interests' and centres on such issues as privacy and freedom of information (Busch, 2005).

A recent development in the transborder data flows is in the airlines industry. European airlines recently faced the dilemma of which of these options to choose because of a conflict between the US Aviation and Transportation Security Act of 2001 and the EU Directive. The conflict left the European airlines entering the US without recourse. The EU and the US have reached an agreement over this conflict, but that does not mean the underlying issues are finally resolved (Roos, 2005).

A recent case is the *European Parliament v European Council (2006)*. Following the terrorist attacks of 11 September 2001, the United States passed legislation in November 2001 providing that air carriers operating flights to or from the US or across US territory had to provide the US customs authorities with electronic access to the data contained in their automated reservation and departure control systems, referred to as 'Passenger Name Records' (PNR data) (which contains inter alia passenger's full name, date of birth, citizenship, sex, passport number). While acknowledging the legitimacy of the security interest at stake, the Commission informed the US authorities that those provisions could come into conflict with the EU and member state legislation on data protection. The problem in Europe is that the EU Directive provides that personal data may only be transferred to third countries if the specific country ensures an adequate level of protection. The Commission decides which countries have adequate laws, but, only a few countries, not including the US, have met the criteria.

Nevertheless, on 14 May 2004, the European Commission adopted the Commission Decision (EC) 2004/535 (on adequate of personal data contained in the PNR of air passengers transferred to the US Bureau of Customs and Border Protection) holding that the US Bureau of Customs and Border Protection offered a sufficient level of protection for personal data transferred from the EU. The European Parliament sought the annulment of the Agreement on the basis, inter alia, that the adoption of the decision on adequacy was *ultra vires*.

The European Court of Justice held that the EU Directive could not justify Community competence to conclude the Agreement. The ECJ found that because the transfer of data was related to national security, public safety or criminal purposes, the Directive did not apply. The transfer fell outside the scope of the Directive. Consequently, the Agreement could not have been validly adopted on the basis of the EU Directive.

The judgment has stripped EU citizens of data protection when it comes to criminal and security matters. The ruling had seemed a victory for data protection activists, but the principal legal basis of the decision creates a 'loophole' whereby their data are now used for law enforcement purposes (OUT-LAW, 2006). Following the decision, the European Commission announced that it will start a new deal with a different legal structure but the same essential content as the Court had not critised the content of the agreement. In fact, the Court never considered the content because the legal structure was flawed (Europa, 2006).

4. THE MALAYSIAN PROPOSED BILL ON PERSONAL DATA PROTECTION

The existing statutory framework in Malaysia does not directly protect the misuse or unauthorized disclosure of the individual personal data. It only confers limited protection on a piecemeal basis such as by the provisions in the National Registration Act, 1959 and the National Registration Regulations, 1990[12];

[12] It is an offence for any public officer to publish or communicate to any person the information contained in the register or any record

Communications and Multimedia Act, 1988[13]; Banking and Financial Institutions Act, 1989[14] and the Computer Crimes Act, 1997.[15] This is not surprising, since the existing statutes have been developed to pursue different policies and are enforced by diverse agencies such as the National Registration Department, Malaysian Communication and Multimedia Commission and the Bank Negara Malaysia. Consequently, the protection against misuse or unauthorized disclosure of the personal data is merely incidental to the protection of other interests recognized by the common law under particular torts (Thomas, 2004).

Hence, the need for personal data protection law in Malaysia cannot be overstated. The need is imperative as an instrument to regulate privacy-invading technology, and as a prerequisite to outsourcing business in international trade since globalisation markets has resulted to transborder data transfer.

The Ministry of Energy, Water and Communication has come up with a draft of Personal Data protection Bill in 2000 ('proposed Bill'). The proposed Bill which contains nine data protection principles is envisaged to be a world class leading edge cyber law that provides for higher level of personal data protection law. The Bill is drafted as a mechanism for Malaysia to be a preferred trading partner in the communications and multimedia industry that provides international standards of personal data protection (The Ministry of Energy Water & Communication).

Although described as principles, they carry the full force of the law. They are fully enforceable legal rules in the sense that their substance has been incorporated into the proposed Bill. Section 4(1) provides that the principles are binding on the data user unless exempted by the Act. Section 4(2) provides the statutory power to the Minister to amend the First Schedule upon the recommendation of the Commissioner. Therefore, it is the duty of the Commissioner to revise the suitability of the principles and to advise the Minister accordingly.

The proposed Bill is set up in three ways to enforce the data protection principles (Abu Bakar Munir and Siti Hajar Mohd Yasin, 2002). First, through a system of compulsory registration of all data users supervised by the Commissioner and backed up by the criminal law. Second, on receipt of complaint by a data subject to the Commissioner alleging the contravention of the principles. Third, by providing data subjects with rights arising out of some of the principles.

The Principles are firstly[16], personal data shall be collected fairly and lawfully. Secondly, personal data shall be held for one or more specified and lawful purposes. Thirdly, personal data held for any purpose shall not, without the consent of the data subject, be used for any purpose other than the purpose for which the personal data were to be used at the time of the collection of the personal data or directly related to it. Fourthly, personal data shall not, without the consent of data subject be disclosed unless the disclosure of the personal data is done for the purpose in connection with which the personal data was obtained or is directly related to it. Fifthly, all practical steps shall be taken to ensure that personal data are accurate, complete, relevant, not misleading and up-to-date, having regard to the purpose for which the personal data are to be used. Sixthly, personal data held for any purpose shall not be kept for longer than is necessary for that purpose. Seventhly, an individual shall be entitled at reasonable intervals to be informed by any data user whether he holds personal data of which that individual is a subject; to have access to any such personal data held by a data user; to be informed of the logic involved in the decision taking in regards with processes by automatic means; and where appropriate to have the personal data corrected. Eighthly, all practical steps to ensure security shall be taken against unauthorized or accidental access, processing or erasure to, alteration, disclosure or destruction of, personal data and against accidental loss of personal data. Finally, all practical steps shall be taken to ensure that a person can ascertain a data user's policies and practices in relation to personal data, and be informed of the kind of personal data held by a data user.

However, the proposed Bill has received considerable criticism based on numerous grounds and has yet been tabled in the Parliament. The proposed Bill prohibits the transfer of personal data to a third country without efficient protection. This provision creates questions as to the basis of the determination as whether a particular country has the adequate level of protection. The proposed Bill excludes the data held outside Malaysia from being protected under the proposed Bill. This exclusion certainly limits protection afforded to consumers since the current practice of foreign companies who are collecting consumer data would not be regulated by this law. The proposed Bill lays down number of exceptions. These exceptions are relating to

---

13 Any person who without lawful authority intercepts any communications or discloses such intercepted communications by means of any network facilities or network service commits an offence punishable by a term of imprisonment not exceeding one year, or a fine not exceeding RM50,000.

14 Prohibit the unauthorized disclosure of financial information which is identifiable to a particular individual.

15 Provides for offences relating to the misuse of computers. Any person who, without authorization, uses a computer to access any program or data held in any computer or computer network, commits an offence.

16 First Schedule, Section 4 of the proposed Personal Data Protection Bill

circumstances in which either the data subjects themselves require the transfers or such transfer is inevitable for the sake of the public interest and national security (Sarabdeen Jawahitha, 2004). It is also observed that, first, arguably the Ministry concentrated only at such jurisdictions which adopted the command and control models and overlooked both the self-regulation and co-regulatory models. Consequently, not only the proposed Bill was deprived of the benefits and experiences that could be adopted from the self-regulation and co-regulatory models, but it also adopted both the advantages and disadvantages of the command and control model. Second, the delay in the tabling of the proposed Bill arguably could signify some strains foreseeable by the Ministry especially of an acceptable standard that could easily adopted and enforced by the government and complied by industry.

Taken as a whole, the deficiencies inherent in the existing statutory framework and the hurdles within the common law in Malaysia expose an urgent need for a data protection legal framework to address the issues of misuse or unauthorized disclosure arising from processing and usage of personal data.

5. CONCLUSION

Compliance with data protection and privacy law is at its core about a company being able to justify its use of personal data, controlling the use of that data, and updating and discarding the data when required. Above all, the key is to take, and be seen to be taking, privacy and data compliance seriously. If management can achieve that objective, then the company should be able to maneuver through the data protection legal minefield unscathed (Cohen, 2003).

It is important to understand that, whatever data concerning the E-Customers is collected and however it is used, the laws governing data protection must be considered. On the same note, the need for personal data protection law in Malaysia cannot be overstated. The need is imperative as an instrument to regulate privacy-invading technology, and as a prerequisite to outsourcing business in international trade since globalization markets has resulted to transborder data transfer.

However, arguably the current model of the proposed Personal Data Protection Bill in Malaysia is flawed. A more appropriate proposed model should be ascertained. Accordingly, several questions need to be explored. First, whether the proposed Personal Data Protection Bill provides viable protection to the individual's information privacy as against trade interests? Second, what are the benefits that we can gain from the data protection directives and law in the European Union and the United Kingdom, and their respective experiences, and would all these models of data protection which incorporated the western concept of individualism are suitable to our Asian's communitarian values? The answers to the above questions will enable us to critically examine the strength and weaknesses of the proposed Personal Data Protection Bill in Malaysia and the data protection legal framework in the European Union and the United Kingdom, for the comparative analysis of the law. Finally we would enable us to ascertain a model for data protection law in Malaysia which would reconciliate the conflicting interests between the policy maker, organization and society, as well as between individual information privacy and trade interest.

CASES

Rechnungshof v Osterreichischer Rundfunk and others [2003] ECJ CELEX NEXIS 209,online, accessed on 5 June 2006,available at http://web.lexis-nexis.com/universe/document;

European Parliament v European Council [2006] All ER (D) 05 (Jun),online, accessed on 28 June 2006,available at http://web.lexis-nexis.com/universe/document

REFERENCES

ABU BAKAR MUNIR & SITI HAJAR MOHD YASIN (2002) *Privacy and Data Protection: A Comparative Analysis with Special Reference to the Malaysian Proposed Law,* Petaling Jaya, Sweet & Maxwell Asia;

BENTIVOGLIO, J., CORTEZ, N. & KIRK, S. (2003) Global Privacy Law Update. *Computer and Internet Lawyer* 20**,** 1 online, accessed on 28 June 2006, available at http://proquest.umi.com/;

BUSCH, A. (2005) The Politics of Transborder Data Flows: Competing Values, Interests, and Institutions. *Oxford Internet Institute* 11 online, accessed on 26 January 2006, available at http://web.lexis-nexis.com/universe/document;

CAREY, P. (2004) *Data Protection: A Practical Guide to UK and EU Law,* Oxford, Oxford University Press;

COHEN, L. M. (2003) If It's Personal, It's Protected. *Security Management* 47**,** 93 online, accessed on 28 June 2006, available at http://proquest.umi.com/;

DAM, S. (2005) Remedying A Technological Challenge: Individual Privacy And Market Efficiency; Issues and Perspectives On The Law relating To Data Protection. 15**,** 337 online, accessed on 13 September 2005, available at http://web.lexis-nexis.com/universe/document;

EUROPA (2006) Transfer of Passenger Name Records: The Commission Adopts Two Initiatives to Comply With The Rulling of the European Court of Justice on the Transfer of PNR to the United States of America. online, accessed on 26 June 2006, available at http://europa.eu.int/rapid/pressReleasesAction.do;

GILBERT, F. (2005) Transborder Data Transfers: New Set of Standard Contractual Clauses. *ractising Law Institute Order Number 6080* 9 online, accessed on available at http://web2.westlaw.com;

HARDING, E. (2005) Compliance Costs and the Privacy Act 1993: Perception or Reality For Organisations in New Zealand? *Victoria University of Wellington Law Review* 36 529 online, accessed on 27 June 2006, available at http://web.lexis-nexis.com/universe/document;

INFORMATION COMMISSIONER'S OFFICE (2006) Data Protection Act: Media Fact Sheet. online, accessed on 3 April 2006, available at http://www.ico.gov.uk/eventual;

JAY, R. (2004) International Developments in Privacy Law. Practising Law Institute.;

L.RUSTAD, M. & H.KOENIG, T. (2005) Harmonizing Cybertort For Europe and America. *ournal of High Technology* 5**,** 13 online, accessed on 7 June 2005, available at http://web.lexis-nexis.com/universe/document;

MCKAY, A. T. (2005) Privacy Act: A First Step On The Road To Privacy. *Pacific Rim Law & Policy Journal* 14**,** online, accessed on 24 May 2006, available at http://web.lexis-nexis.com/universe/document;

MOSHELL, R. (2005) …And Then There Was One: The Outlook For A Self-Regulatory United States Amidst A Global Trend Toward Comprehensive Data Protection. *Texas Tech Law Review* 37**,** 357 online, accessed on 6 July 2005, available at http://web.lexis-nexis.com/universe/documen;
t

OUT-LAW (2006) Passenger Data Judgment Attacked By Privacy Chief. *OUT-LAW News* online, accessed on 26 June 2006, available at http://www.out-law.com/page-6960;

RICHARDS, N. M. (2005) Reconciling Data Privacy And The First Amendment. *University of Carlifornia Law Review* 52**,** 1149 online, accessed on 6 July 2005, available at http://web.lexis-nexis.com/universe/document;

ROOS, M. (2005) Safe on the Ground, Exposed in the Sky: The Battle Between the United States and the European Union Over Passenger Name Information. *Transnational Law & Contemporary Problems* 14**,** 1137 online, accessed on 28 June 2006, available at http://web-lexis-nexis.com/universe/document;

SAMORISKI, J. (2002) *Issues in Cyberspace : Communication, Technology Law, and Society on the Internet Frontier,,* Boston, Allyn & Bacon;

SARABDEEN JAWAHITHA (2004) Consumer Protection in E-Commerce: Analyzing the Statutes in Malaysia. *Journal of American Academy of Business, Cambridge* 4**,** 55 online, accessed on 28 June 2006, available at http://proquest.umi.com/;

SIMONS & SIMONS (2001) *E-Commerce Law,* Isle of Wight, Palladian Law Publishing Ltd;

THE JOINT INFORMATION COMMITTEE (2006) The General Issues of Data Protection online, accessed on 3 April 2006, available at http://www.jisc.ac.uk/uploaded-document;

THE MINISTRY OF ENERGY WATER & COMMUNICATION Personal Data Protection. online, accessed on 28 March 2006, available at http://www.ktkm.gov.my/;

THOMAS, M. (2004) Is Malaysia's MyKad The 'One Card To Rule Them All?'The urgent Need To Develop A Proper Legal Framework For The Protection Of Personal Information In Malaysia. *Melbourne University Law Review* 28**,** 474 online, accessed on 19 July 2005, available at http://web.lexis-nexis.com/universe/document