Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 6 (2011) pp. 407-414

E-Commerce Security: A Comparative Analysis of the Law in the UK and Malaysia

Siew Wei Gan

Nottingham University Business School,
The University of Nottingham Malaysia Campus
Jalan Broga, 43500 Semenyih, Selangor, Malaysia
wendy.gan@nottingham.edu.my

***Abstract*: Electronic commerce (e-commerce) is shaping business strategies and purchasing behaviours of consumers because it offers new opportunities for business, and convenience and added value to consumers. However, security concerns are still preventing e-commerce from achieving its full potential. Computer security technologies and management policies need to be accompanied by sound legal frameworks to provide effective security and promote trust in e-commerce. Despite the efforts of the government to promote Malaysia as a regional centre for information technology and e-commerce, security issues are preventing e-commerce from flourishing in this country. This paper seeks to examine the adequacy of cyber laws in Malaysia in addressing the issue of security in e-commerce transactions. The research adopts a comparative method with a qualitative analysis and uses the conceptual framework of e-commerce security requirements as a guide for analysis and deduction. UK legislation has been identified as a target of comparison because of the antecedents and influence of English law on the Malaysian legal system, as well as the relative popularity and rapid growth of e-commerce in the UK. The comparison involves cross-national analysis and identification of variables in these two jurisdictions to identify implications of the variables. Findings provide a basis for determining the adequacy of the legal infrastructure supporting security aspects of e-commerce in Malaysia and to suggest proposals for improvement in this rapidly evolving area of law.**

***Keywords*: E-Commerce, Legal Framework, Malaysia, UK.**

I. Introduction

E-commerce is shaping business strategies and purchasing behaviours of consumers because it offers new opportunities for business, and convenience and added value to consumers. The rapid growth of e-commerce is buffeted by cheaper access costs and supporting technological developments such as broadband and cable modem technology. However, despite the government's efforts to promote e-commerce through implementation of the National E-commerce Master Plan, the growth of e-commerce in Malaysia has been sluggish. The Malaysia Communications and Multimedia Commission statistics for 2008 puts the internet penetration rate for Malaysia at over 40% of its population, but only a mere 9% of the internet users have ever shopped online. Despite being one of the leading digital economies according to UNCTAD (2003) where the government has pushed for the development of the information society, the growth of e-commerce has not taken off as expected. In a study of factors influencing decisions to participate in e-commerce, Suki (2002) concludes that privacy and security issues are among major inhibitors for online transactions. Despite efforts to establish and revise regulatory guidelines in light of the rapid technological changes in this area, security and privacy issues remain a major inhibitor of online transactions (Kaur, 2005). Computer security technologies and management policies need to be accompanied by legal frameworks which are able to keep in step with technological developments supporting online businesses conducted through the internet. This paper discusses the security requirements for e-Commerce, and compares the laws of the UK and Malaysia to examine the adequacy of the Malaysian legal framework in addressing the issue of security in e-commerce transactions with reference to a framework for security in an e-commerce environment, and suggests proposals for improvement in this rapidly evolving area of law.

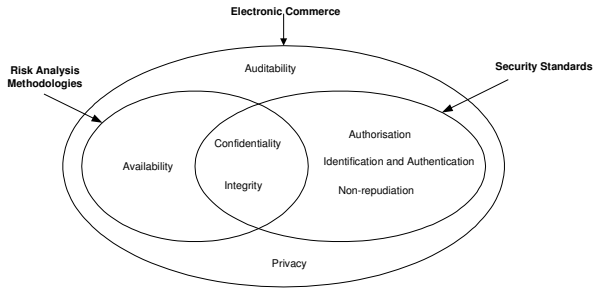
II. Methodology

Being a part of the rural research community, legal research does not usually employ methodologies based on empirical investigation as commonly used in the sciences. Rather, it is concerned with qualitative analysis and doctrinal research. The process is analysis and not data collection and therefore legal research methodology may not have the elements similar to other social sciences or scientific research (Chynoweth, 2008). As such, this research adopts a comparative method with a qualitative analysis and uses the conceptual framework of e-commerce security requirements as a guide for analysis and deduction. The first part analyses the law in the area of e-commerce security, using a methodology involving deductive logic in analysis rather than a formal "research methodology" as understood by researchers in other disciplines, to develop arguments relating to the legislative provisions. The second part is the comparative approach involving cross-national analysis and identification of

variables (legal provisions) in two contrasting jurisdictions to identify implications of the variables (Ragin, 1987). The comparative design is used to identify similarities and highlight differences between e-commerce legislation in these two jurisdictions and, through a process of deduction, to examine whether the legal infrastructure supporting security aspects of e-commerce in Malaysia is adequate.

III. Security Requirements for E-Commerce

Security issues in e-commerce can be identified by analysing a typical e-commerce transaction encompassing the participation of the client, the merchant and the bank/financial institution. Clients are internet users who browse the web and decide to conduct an online purchase. Merchants use websites to advertise their products and provide relevant information and services to sell their products. The client will provide order details and payment information to the merchant. The payment information will be forwarded to the bank for verification. Upon receipt of the verification from the bank, the merchant will forward it to the client and honour the transaction by agreeing to the sale. Then, the merchant will forward payment instructions to the bank. The bank will make the payment and provide proof of payment to the merchant. Lastly, the merchant may use information gathered from these transactions for internal analysis and planning. This framework assumes inter-bank transactions occur and that the whole network of banks is a single unit. Based on this, eight security requirements can be identified. A model of these requirements is presented in Figure 1.



Source: Labuschagne, L. 2000 *A Framework For E-Commerce Security* pp 441-450 in Qing, S. and Eloff, J. H. P. (Eds.) Information Security for Global Information Structures. Kluwer Academic Press

Figure 1. Security requirements for electronic commerce

This model combines conventional risk analysis elements (confidentiality, integrity, availability) with security requirements provided in international security standards (identification and authentication, authorisation, confidentiality, integrity, non-repudiation) and includes additional requirements of privacy and auditability. These additional requirements take into account the internet as an open medium of communication and the nature of online transactions which do not involve written documents. Table 1 provides the definitions for each of the security requirements and Figure 2 shows a summary of a typical e-commerce transaction and the associated security requirements for each component of the transaction.

Security Element	**Definition**
Identification and Authentication	The ability to uniquely identify a person or entity and to prove such identity.
Authorisation	The ability to control the actions of a person or entity based on its identity.
Confidentiality	The ability to prevent unauthorised parties to interpret or understand data.
Integrity	The ability to assure that data has not been changed by any unauthorised parties.
Non-Repudiation	The ability to prevent the denial of actions by a person or entity
Availability	The ability to provide uninterrupted service
Privacy	The ability to prevent unlawful or unethical use of information or data
Auditability	The ability to keep an accurate record of all transactions for reconciliation purposes.

Adapted from Labuschagne, L. (2000) *A Framework For E-Commerce Security.* pp 441–450 in Qing, S. and Eloff, J. H. P. (Eds.) *Information Security for Global Information Structures*. Kluwer Academic Press. Boston.

Table 1. Definitions of security requirements

The security requirements discussed above must be adequately addressed in order to establish a sufficient level of consumer's trust to make the internet a viable medium for commercial transactions. These requirements can be fulfilled by using appropriate technologies for securing electronic transactions in conjunction with sound management policies and supporting legal frameworks (Ford and Baum, 2001). In terms of technology, cryptography is used to ensure security requirements of identification and authentication, integrity, confidentiality, non-repudiation, authorisation and privacy are satisfied. Firewalls, well configured web server operating systems and defensive software tools are technologies which can ensure availability of websites for e-commerce transactions. Management policies for data management such as back-ups and secure permanent storage of transaction details will help ensure auditability of transactions.

	Component								
	1	2	3	4	5	6	7	8	9
Participants	Connect to merchant's website	Give order & payment details	Send order sum & payment details	Request to verify payment details	Check and Send verification	Confirm verified & honour transaction	Send payment instruction	Pay and provide proof of payment	Analyse and plan
Client	X	X				X			
Internet	X	X	X						
Merchant	X			X	X	X	X	X	X
Bank				X	X		X	X	
Security Requirements									
Identification & Authentication	X	X		X			X		
Authorisation					X		X		
Confidentiality		X	X	X		X	X	X	
Integrity		X	X	X		X	X	X	
Non-repudiation		X		X		X	X	X	
Availability				X					
Privacy	X								X
Auditability					X	X	X	X	

Adapted from Labuschagne, L. (2000) *A Framework For E-Commerce Security.* pp 441–450 in Qing, S. and Eloff, J. H. P. (Eds.) *Information Security for Global Information Structures*. Kluwer Academic Press. Boston.

Figure 2. Security Requirements for e-commerce transaction components

A. E-commerce: technology, management and law

The technologies and management practices supporting e-commerce security requirements described above will only be effective in providing trust to consumers when it operates within defined parameters and is supported by adequate legal provisions governing their use. Therefore, legal frameworks for e-commerce security must be formulated to confer rights and liabilities for the use of encryption and digital signatures. The functions of certification authorities and the registration of these organisations must also be governed by law. The existence of secure transmission and storage facilities for sensitive information does not guarantee privacy for consumers as a company may choose to sell or transfer the information to any third party. In order for customers to know and enforce their right of privacy, there needs to be legal provisions relating to data protection and the powers of the law enforcement and security agencies in carrying out interception and surveillance of communication over the internet and accessing data held by organisations. Although there are arguments for minimal state interference in the governance of the internet due to its trans-boundary nature and rapid technological development (Low, 2000), proper regulatory frameworks are still necessary in order to give consumers confidence in e-commerce and establish trust in the security of their interests and the enforceability of their rights as customers. The next section considers the legal infrastructure of the UK and Malaysia in the context of the eight security requirements for e-commerce described above.

IV. E-Commerce Law: UK and Malaysia

The majority of electronic commerce laws in the United Kingdom were enacted in compliance with the Directives adopted by the European Parliament and of the European Council . Six directives relating to the regulation of electronic commerce were: Directive 1995/46/EC on Data Protection, Directive 1997/7/EC on the protection of consumers in respect of distance contracts, Directive 1999/93/EC on a Community framework for electronic signatures, Directive 2000/21/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market, Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society and Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector. These directives are binding on member states as regards the results to be achieved within specified time frames but do not dictate the method of achieving them (Borchardt, 2000). As a member of the European Union, the UK has enacted and amended laws to comply with these directives. Provisions in the Electronic Communications Act 2000 (ECA) (2000 c. 7), the Computer Misuse Act 1990 (CMA) (1990 c.18) and the Data Protection Act 1998 (DPA) (1998 c. 29) relating to e-commerce security elements will be discussed.

The Electronic Communications Act 1990 lays down principles of law governing the use of cryptography and regulation of cryptography support service (Part I), facilitation of electronic commerce, electronic data and electronic signatures (Part II) and modifications to telecommunications licences (Part III). The Computer Misuse Act 1990 regulates offences relating to unauthorised access and modification of programmes or data held on a computer while the Data Protection Act 1998 governs the protection and proper processing of personal data.

The Malaysian Government in its efforts to provide a comprehensive regulatory framework of cyber laws to facilitate and encourage e-commerce has enacted the Digital Signature Act 1997 (DSA), which provides an avenue for secure online transactions through the use of digital signatures; the Computer Crimes Act 1997 (CCA) to address the threat of illegal access to and use of information stored on computer systems; and recently passed the Personal Data Protection Bill in June 2010. The CCA and the Personal Data Protection Act 2010 (PDPA) are modeled after similar legislation in the UK while the DSA was modeled on the Digital Signature Act enacted in the state of Utah in America.

A. Analysis of the provisions in the laws of the UK and Malaysia

The eight elements of e-commerce security requirements are

identification and authentication, authorisation, confidentiality, integrity, non-repudiation, availability, privacy and auditability.

1) Identification and Authentication

In the UK, this requirement is supported by the ECA which recognises cryptography and digital signatures as a means to secure the authenticity of a particular piece of electronic communication. Sections 1 to 6 of the ECA which governs the activities of the cryptographic service providers further supports the operation of digital signatures to achieve these requirements, giving assurance to e-commerce users of the validity of digital signatures as identification documents. Section 7 (1) states that the use of an electronic signature incorporated or logically associated with an electronic communication or data and certified as such by the signatory is admissible in evidence to prove its authenticity or integrity. No distinction is made between electronic signatures (such as scanned images of written signatures) and secure digital signatures (created with encryption technology). The position is very similar in Malaysia, where digital signatures are recognised as valid instruments for identification and authentication (Section 2 and Section 62, DSA). These provisions adopt the "functional equivalent" approach, giving digital signatures and electronic messages equal effect as conventional signatures and paper documents.

2) Authorisation

Laws governing the use of digital signatures and the function of certification authorities in both jurisdictions enable e-commerce participants to rely on digital signature certificates as proof of authorised use and support the security requirement of authorisation especially when they are used to facilitate electronic payments. Sections 1 to 6 of the ECA provides for the registration and regulation of cryptography support service providers (commonly referred to as a trusted third party) which help ensure confidence to e-commerce users relying on a digital signature that the signatory has the authority to use the signature. In Malaysia, the regulation of certification authorities under the DSA is more stringent compared to the UK position. Although there are no restrictions limiting the eligibility of any person to operate as a certification authority in both countries, it is mandatory for all certification authorities to be licensed under the DSA, as provided for in Section 4 (1). In the UK, in line with the EC Directive on Electronic Signatures which prohibits Member States from setting requirements for the provision of certification services to be subject to prior authorisation and which encourages Members States to introduce voluntary accreditation systems, any service provider or trusted third party will be able to offer its services legally without having been registered as an approved provider.

Offences punishable under the CMA (Section 1, 2 and 3) in the UK and CCA (Section 3, 4 and 5) in Malaysia include unauthorized access, identity theft and impersonation, with the presumption that only the person with genuine payment details and personal information is authorised to request for payment from his/her bank for purchase of goods and services. Section 1 of the CMA makes it an offence for a person to 'cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer' and that person knows at that time that the access is unauthorised. The intention of the person to gain unauthorised access need not be targeted at any particular program or data held in any particular computer . Therefore, an employee who is authorised to access the employer's computer system may be criminally liable if he/she uses data stored in the system for personal interest.

Section 2 of the CMA makes it an offence to access any program or data held in any computer without authorisation with the intention of committing or facilitating the commission of a further offence, even if the commission of the further offence is impossible. For example, a hacker who accesses customer account information held by an e-commerce business with the intention of using it to make fraudulent purchases by impersonating the account holder would be criminally liable under this section, even if in fact the computer system is designed not to process his purchase for any reason.

In Malaysia, the offence of gaining unauthorised access with intent to commit a further offence specifically refers to further offences of fraud, dishonesty or injury, giving emphasis to wrongful acts of accessing computer systems to obtain credit card and other payment details in order to commit fraud or dishonesty, particularly in an e-commerce environment. Further, there is an additional offence in Section 6 of the CCA of unauthorised disclosure of access mechanisms (such as usernames and passwords) which allows unauthorised persons to gain entry to computer systems. It is irrelevant whether the disclosure in fact caused unauthorised access. This is a preventive step to ensure that those entrusted with access rights to computers comply with the duty of secrecy, so that the security of computer systems is not compromised (Annamalai, 1997).

3) Confidentiality

In the UK, Section 6 of the ECA gives legal recognition to cryptography as a method for ensuring confidentiality in electronic communication. Section 6 (1) (a) of the ECA states that cryptography services are those provided for the purpose of inter alia 'securing that such communications or data can be accessed, or can be put into an intelligible form, only by certain persons'. The CMA also provides deterrence against access to confidential communication and data, giving legal effect to the need for confidentiality in electronic communication and punishing unauthorised access to confidential information and communication. Under section 4 of the DPA, the data controller (such as the owner of an e-commerce business) is under a duty to ensure that data held are secure against unauthorised and unlawful processing, increasing the protection of consumers against breach of their confidential information by both internal staff and external hackers.

The Malaysian CCA is modeled after the CMA and deals with similar offences. Like the UK CMA, it applies to offences within and outside the country, as long as they relate to computer systems in the country or connected to a computer

used in the Country (Section 9, CCA). The PDPA also contains provisions requiring a data user to take 'practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction…' (Fourth Data Protection Principle, PDPA).

4) Integrity

Provisions supporting integrity in e-commerce transactions can be found in the laws giving recognition to digital signatures. In defining digital signatures, the UK provision states that digital signatures are those which are associated with a message 'for the purpose of being used in establishing …. the integrity of the communication or data' (Section 7 (2) (b) ECA), while the Malaysian DSA states that digital signatures are those which can be used 'to accurately determine whether the message has been altered since the transformation (using an asymmetric cryptosystem) was made' (Section 2 (1) DSA). By providing that a person relying on the digital signature attached to a message can determine whether the message was altered after it was signed, the security requirement of integrity is fulfilled.

5) Non-Repudiation

An electronic communication cannot be repudiated if it can be proven that it originates from the person who is attempting to repudiate it. Provisions giving legal effect to cryptographic techniques and digital signatures used to establish the authenticity and integrity of an electronic communication found in Section 6 (2) (b) and Section 7 (2) (b) ECA of the UK, and Section 2 (1) and Section 29 of the Malaysian DSA support the security requirement of non-repudiation because the actions of the party sending the electronic communication cannot be later denied by him/her since his/her identity and the integrity of the message cannot be disputed. Section 64 of the DSA states that 'a message shall be as valid, enforceable and effective as if it had been written on paper if it bears in its entirety a digital signature and that digital signature is verified by the public key listed in a certificate which was issued by a licensed certification authority and was valid at the time the digital signature was created', giving digital signatures the same level of enforceability as normal written signatures and embodying the principle of functional equivalence adopted by the UK ECA. Any party relying on a valid certificate can presume that the signer is authorised to use the digital signature and is not allowed to repudiate his/her actions in accordance with the message which accompanies the signature (Chong, 1998).

Provisions relating to unauthorised access to commit offences in Section 2 of the UK CMA and Section 4 of the Malaysian CCA also support the security element of non-repudiation as they seek to deter unauthorised credit card purchases and payment fraud.

6) Availability

Availability in e-commerce security refers to the uninterrupted access to websites and payment services offered by e-commerce businesses and banks. To deter attacks on websites, both the UK and Malaysia have enacted laws to penalise offenders who gain unauthorised access to computer systems and cause disruption to websites and electronic services. The CMA in the UK provides for punishments of up to six months imprisonment and a possible fine for unauthorised access (Section 1 CMA) while in Malaysia the punishment could be a fine and up to five years imprisonment (Section 3 CCA). For other offences the maximum term of imprisonment under CMA is five years (Sections 2 and 3 CMA) while in Malaysia it can reach a maximum of ten years (Section 4 and 5 CCA). Therefore, it is clear that in Malaysia the punishment can be more severe, reflecting the intention of legislators to effectively curb computer crimes through the CCA and promote electronic communication and commerce. Malaysia has also made it an offence for anyone to communicate any computer systems access mechanisms to an unauthorised person (Section 6 CCA).

7) Privacy

The DPA in the UK protects the privacy of data subjects by requiring compliance with eight data protection principles listed in its First Schedule. There are very similar data principles in the PDPA of Malaysia. The DPA applies to all data controllers established in the UK or those not established in the UK but use equipment in the UK for data processing. The DPA specifies the data controllers which are governed under the Act, and these include public authorities and private entities that are established in the UK or use equipment in the UK to process data. On the other hand, under the Malaysian PDPA, Section 3 specifically states that the law does not apply to the government. The application of the act is limited to commercial transactions in respect of data controllers established in Malaysia or those not established in Malaysia but use equipment in Malaysia for data processing.

Apart from non-application of the PDPA to governmental bodies, another significant aspect of distinction between the UK provision and Malaysia's PDPA relates to the appointment and powers of the Data Protection Commissioner. In the UK the Commissioner is appointed by Her Majesty the Queen by Letters Patent, making the office independent of government (Lloyd, 2000). However, the Malaysian Commissioner for Personal Data Protection is answerable to the Minister (of Information, Communication and Culture) according to Section 5 of the PDPA. This may conflict with the duty of the Commissioner particularly when investigating complaints involving private entities which are established under the authority of the government for alleged contravention under the law (Azmi, 2002).

8) Auditability

The DPA of the UK and the PDPA of Malaysia both provide that data controllers and data users must take steps to prevent the loss or destruction of personal data (Seventh Data Protection Principle, DPA and Fourth Data Protection Principle, PDPA). This provision supports the security requirement of auditability by ensuring that personal data is kept securely and available for audit purposes where necessary. Other generic laws which deal with proper storage of transaction records include laws governing taxation and financial institutions.

Table 2 provides a summary for laws which support each of the security requirements for both jurisdictions.

Security Requirement	UK Law	Malaysian Law
Identification & Authentication	Sections 1 to 7 ECA	Section 2, 62 & 64 DSA
Authorisation	Section 1 to 3 CMA	Section 2, 62 & 64 DSA, Section 4, CCA
Confidentiality	Section 6 ECA Sections 1 to 3 CMA Section 4 & Schedule 1 DPA	Section 3, 4, 5 & 6 CCA Section 5 & 9 PDPA
Integrity	Sections 6 & 7 ECA	Section 2, 62 & 64 DSA
Non-Repudiation	Section 6 (2) (b) and Section 7 (2) (b) ECA Section 2 CMA	Section 29 DSA Section 4 CCA
Availability	Section 1 to 3 CMA	Section 3, 4, 5 & 6 CCA
Privacy	Section 4 & Schedule 1 DPA	Section 5 to 12 PDPA
Auditability	Section 4 & Schedule 1 DPA	Section 9 PDPA

Key:
ECA – Electronic Communications Act 2000 (UK)
CMA – Computer Misuse Act 1990 (UK)
DPA – Data Protection Act 1998 (UK)
DSA – Digital Signature Act 1997 (Malaysia)
CCA – Computer Crimes Act 1997 (Malaysia)
PDPA – Personal Data Protection Act 2010 (Malaysia)

Table 2: Comparison of UK and Malaysian Legal Provisions for E-Commerce Security

B. Summary

In the UK, it is found that most of the elements of security in e-commerce transactions have been addressed directly or indirectly by legislation. The Electronic Communications Act 2000 (ECA) identifies the technologies which can be used to support security requirements of identification and authentication, confidentiality, integrity and non-repudiation. It recognises encryption technology as a means to provide confidentiality. It also provides for the use of digital signature as a means of providing identification and authentication, integrity and non-repudiation in electronic communication and transactions.

The Computer Misuse Act 1990 (CMA) addresses the threat of unauthorised use of credit card or other payment details obtained through illegal access to computer systems, supporting the security requirements of authorisation and non-repudiation. By making it an offence to access any computer system without proper authorisation or to modify its contents, the CMA seeks to deter hacking activities which disrupt the services provided by e-commerce businesses, thus supporting the security requirement of availability.

Privacy is addressed by the Data Protection Act 1998 (DPA) which regulates the collection, processing and safekeeping of personal data as well as the rights of data subjects. By providing for secure storage and recording of data, the DPA supports security requirements of confidentiality and auditability.

Provisions dealing with each of the e-commerce security requirements in Malaysia closely resemble those found in UK legislation. The Digital Signature Act 1997 (DSA) which has similar regulatory frameworks as the ECA of the UK, establishes rules governing the validity and use of digital signatures. Security requirements of identification and authentication, authorisation, integrity and non-repudiation are supported through the recognition and legal effect given to the use of digital signatures in online transactions. Provisions relating to computer based offences found in the Computer Crimes Act 1997 are identical or very similar to provisions in the UK CMA. They support the requirements for confidentiality, authorisation, non-repudiation, and availability. The CCA extends to offences committed in other countries as long as they relate to computer systems and data in Malaysia.

Before 2010, the major lacunae found in the Malaysian law in relation to security requirements identified are laws governing privacy and auditability. With the passing of the Personal Data Protection Act in 2010, the processing and use of personal data of e-commerce customers is now regulated. Within the framework of the Act, consumers now have some guarantees that their personal information will be kept securely and that it will not be used without their consent or for purposes contrary to their interests.

Compared to the UK, Malaysia can be considered as having comparable e-commerce security legal frameworks in place. Furthermore, for certain areas of law such as those dealing with certification authorities and digital signatures, Malaysia has more comprehensive and extensive provisions compared to the UK. The UK laws dealing with computer crimes are however much more complex than the Malaysian provisions - the UK CMA has a total of 18 sections and several provisions regarding jurisdiction and powers of the court and jury while the Malaysian CCA has 12 sections and only 1 section deals with jurisdiction and powers of the court.

V. Conclusion and Recommendations

It is important to note that the existence of these legal provisions is only one of the pillars to support e-commerce security and needs to be complemented by suitable technology and sound management policies. However, a weak legal framework may well be the cause of sluggish e-commerce growth. Further research may be conducted to examine other possible related causes preventing rapid e-commerce growth in Malaysia, which could include a lack of implementation of these laws, the extent of their effectiveness in enhancing e-commerce security due to the unique nature of electronic transactions. Trans-border data flow is an issue which poses a challenge to the implementation of data protection laws in an

e-commerce environment. Even though both the UK and Malaysia have provisions limiting trans-border data transfer to countries with adequate data protection regulations, determining the level of adequacy and practical steps which could be taken to prohibit transfer of data raises implementation problems to which there are no easy answers (Swindells and Henderson, 1998).

The issue regarding the status and protection for certificates with digital signatures verified by foreign certification authorities which are not registered under the Malaysian Digital Signature Act is unclear. E-commerce businesses may reject these certificates on this basis and cause many difficulties to customers having certificates issued by unregistered certification authorities, whether they are local or foreign customers.

The e-commerce security framework used in this research is based on the elements of security identified in a typical e-commerce transaction. Although it encompasses all the major areas of online security, some of the security requirements presented in the framework (such as auditability) do not relate directly to e-commerce laws and may be better supported by other generic legal provisions such as evidence, banking and taxation laws. Furthermore, other security requirements that may be relevant to online transactions such as time-date stamping (which shows the time and date when a message associated with it is created, sent and/or received) and electronic contracts formation which require proper legal regulation are not included in the framework.

E-commerce security is one of the most crucial factors influencing the growth of e-commerce worldwide. Governments, security experts, consultants and businesses are continually searching for new solutions to security problems that challenge electronic communications and business as increasing new technologies make security threats more rampant. In Malaysia, with the formulation of the cyberlaws and other internet related legislation, the legal provisions governing e-commerce security have addressed many requirements in this area. With the passing of the Personal Data Protection Act, Malaysia moves a step closer to a creating a comprehensive legal framework for e-commerce. However, issues which arise in the implementation and enforcement of these laws, as well as non-legal aspects of e-commerce security such as management policy, security expertise, public perception and infrastructure security merit in depth consideration and research in the awesome task of creating a conducive and dynamic environment in order for e-commerce to flourish.

References

[1] Annamalai, N. "Cyber Laws Of Malaysia - The Multimedia Super Corridor" *Journal of International Banking Law* 12(12): 473-481, 1997.

[2] Azmi, I. M. "E-Commerce and Privacy Issues: An Analysis of The Personal Data Protection Bill". In *17th Belita Annual Conference,* 5-6 April 2002. Free University. Amsterdam.

[3] Borchardt, K. "The ABC of Community Law". *European Commission,* Brussels, 2000 http://europa.eu.int/eur-lex/en/about/abc_en.pdf (accessed July 1, 2003)

[4] Chynoweth, P. "Legal Research", in: *Advanced Research Methods in the Built Environment*, Knight, A & Ruddock L (eds.), Wiley-Blackwell, Chichester, West Sussex, 2008.

[5] Computer Crimes Act 1997 (Act 563) Acts of the Malaysian Parliament

[6] Computer Misuse Act 1990 (1990 Chapter 18) Acts of the UK Parliament

[7] Data Protection Act 1998 (1998 Chapter 29) Acts of the UK Parliament

[8] Digital Signature Act 1997 (Act 562) Acts of the Malaysian Parliament

[9] Electronic Commerce Act 2006 (Act 658) Acts of the Malaysian Parliament

[10] Electronic Communications Act 2000 (2000 Chapter 7) Acts of the UK Parliament

[11] Ford, W. and Baum, M S. *Secure Electronic Commerce – Building the Infrastructure for Digital Signatures and Encryption,* Prentice Hall, Upper Saddle River, NJ, 2001

[12] Hummerston, A. "Taylor Nelson Sofres Interactive: Global E-Commerce Report – June 2002" *TNS Plc.* http://www.tnsofres.com/ger2002/download/ger2002fullreport.zip (accessed June 5, 2003)

[13] Kaur, K. "Consumer Protection in E-Commerce in Malaysia: An Overview", *University of New England Asia Centre - Asia Papers 10*. pp 1-14, 2005 http://www.une.edu.au/asiacentre/PDF/KKaur.pdf (accessed January 2, 2009)

[14] Labuschagne, L. "A Framework For E-Commerce Security" , in *Information Security for Global Information Structures,* Qing, S. and Eloff, J. H. P. (eds.) Kluwer Academic Press, Boston, 2000.

[15] Lloyd, I. J. *Information Technology Law (3rd ed.)* Butterworths, London, 2000.

[16] Low, L. "Internet Governance: Role of State and Society", *Media Asia* 27 (3) 158-164, 2000.

[17] Personal Data Protection Bill, Malaysia

[18] Personal Data Protection Act 2010 (Act 709) Acts of the Malaysian Parliament.

[19] Ragin, C. *The Comparative Method: Moving Beyond Qualitative and Quantitative Strategies*, University of California Press, Los Angeles, California, 1987.

[20] Swindells, C. and Henderson, K. "Legal Regulation of Electronic Commerce", *The Journal of Information, Law and Technology* (3), 1998. http://elj.warwick.ac.uk/jilt/98-3/swindells.html (accessed 2 June, 2003)

[21] Suki, N. M. "Motivation and Concern Factors for Internet Shopping: A Malaysian Perspective", *The Electronic Journal for E-Commerce Tools and Applications* 1 (2), 2002. http://minbar.cs.dartmouth.edu/greecom/ejeta/second-issue.php?download=ejeta-2002.05.14.04.09.49.pdf (accessed 20 June, 2003)

[22] UNCTAD "E-Commerce and Development Report 2003", United Nations, New York and Geneva, 2003.

Author Biographies

Siew Wei Gan Kuala Lumpur, Malaysia. MSc Management and Information Systems, University of Manchester, Manchester, UK, 2003. The author's main areas of research include cyberlaws, e-commerce security and de--velopment informatics.