SUSTAINING THE RIGHT TO PRIVACY IN E- COMMERCE ENVIRONMENT: THE LEGAL APPROACH

Duryana binti Mohamed [a]
[a] Department of Legal Practice, Ahmad Ibrahim Kuliyyah of Laws,
International Islamic University Malaysia(IIUM), Jalan Gombak, Kuala Lumpur, Malaysia.
[a] Corresponding author: mduryana@iium.edu.my

 ISSN 1923-6654 (print)
ISSN 1923-6662 (online). Available at http://www.ssrn.com/link/OIDA-Intl-Journal-Sustainable-Dev.html

Abstract: The right to privacy is a fundamental human right as declared in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights. Some countries recognise this right as constitutional right of individuals. The importance of this right is also underlined with the enactment of legislation by most countries. In Malaysia, the privacy protection is available under the Personal Data Protection Act passed in 2010. This Act seeks to regulate the processing of personal data of individuals involved in commercial transactions by data users so as to provide protection to the individual's personal data, thereby safeguarding the interests of such individual. Since this privacy right is important in e-commerce, this paper will examine the extent of privacy protection available under the existing law and whether such law and other relevant laws provide adequate protection to the personal data when dealing with online transaction. The aim of this paper is to establish justice to the online consumers and to provide information that their right is protected under the law.

Keywords: E-Commerce, Personal Data, Privacy Right, the Laws

Introduction

Electronic commerce is conducted on the World Wide Web (WWW). According to WTO definition, e-commerce involves 'the production, distribution, marketing, sale, or delivery of goods, and services by electronic means.' [1] It also means the ability of purchasing various goods through the Internet using secure protocols and electronic payment services. [2] Through this medium, businesses are able to communicate with the consumers directly. This method allows the people to carry out business at anytime and anywhere. In fact, there are many benefits and advantages of e-commerce besides the disadvantages. [3]

Privacy is one of the most important issues in e-commerce. This privacy right is recognised as a fundamental human right and declared in Article 12 of the Universal Declaration of Human Rights 1948 and Article 17 of the International Covenant on Civil and Political Rights. Some countries established this right under their constitution and the people can enforce their right under the existing laws. However, the enforcement of this right may differ from one country to another depending on the available laws and government policies in that particular country.

This paper will discuss on the right to privacy in e-commerce and how such right is maintained and protected under the available laws. The discussion will also cover the aspects of e-commerce and the governing laws, privacy protection and the relevant laws in few selected countries, namely the United States, the European Union, the United Kingdom, Australia and Malaysia. The challenges in protecting personal information and legal remedies on the invasion of privacy will also be highlighted.

Privacy: Definition and Scope

According to Warren and Brandeis, the word 'privacy' refers to the right to one's personality that provides 'for the protection of the person and for securing to the individual what Judge Cooley calls 'the right to be let alone.' [4] The scope of privacy is not limited to personal privacy only but extends to territorial, physical or bodily and communication privacy.

As mentioned above the right to privacy and protection of personal data depends very much on the available laws in that country. For example, in Australia the right to privacy is regulated by the Privacy Act while in the UK, the personal data is protected by the Data Protection Act 1998 and other relevant laws.

E-commerce: The governing laws and Regulations in selected countries

There are several laws and regulations that governed e-commerce activities. Some countries have enacted comprehensive laws on e-commerce while some others are still in the process of enacting laws. Some e-commerce laws were developed and reviewed in order to keep up with the changes in technology. This part will briefly discuss on e-commerce laws and regulations in few selected countries including the United States (US), the European Union (EU), the United Kingdom (UK), Australia and Malaysia. In fact, the US and the EU are two entities that have issued policies which later dictated by other countries.

i. The United States (US)

In the US, e-commerce is governed by the Uniform Commercial Code (UCC), Uniform Electronic Transactions Act (UETA) and Uniform Computer Information Transactions Act (UCITA). Some electronic commerce activities are also regulated by the Federal Trade Commission (FTC). These activities include the use of commercial e-mails, online advertising and consumer privacy. The Federal Trade Commission Act regulates all forms of advertising, including online advertising, and states that advertising must be truthful and non-deceptive. [5] There is also the CAN-SPAM Act of 2003 which establishes national standards for direct marketing over e-mail.

ii. The European Union (EU)

The European Union and its member countries have their own policies, Directives and Regulations pertaining to e-commerce. Some of them include Convention on the Law Applicable to Contractual Obligations (80/934/EEC), 1980 OJ L266, Electronic Commerce Directive (EU) 2000/31/EC, the Electronic Commerce (EC Directive) Regulations 2002 and the Directive on Unfair Commercial Practices. Although each Directive has its own definition and purpose the aim is to protect the interest of the consumer in e-commerce activities.

Since e-commerce is borderless the data supplied online may also cross the borders. In this regard, the European Union has adopted a specific regulation that restricts the transborder data flow to a third country. The restriction is lifted if the third country can ensure adequate level of protection for data subjects. [6]

iii. The United Kingdom (UK)

In the UK, electronic commerce is governed by the Electronic Commerce (EC Directive) Regulations 2002/2013. This Directive actually implements the EU's EC Directive into UK law. Other related laws include the Consumer Protection Act 1974, Contract (applicable Law) Act 1990, Unfair Contract Terms Act 1977 and Unfair Terms in Consumer Contracts Regulations 1999/2083.

iv. Australia

The electronic commerce in Australia is governed by different laws at different territories. The laws include Commonwealth Electronic Transactions Act 1999, [7] Electronic Transactions Act 2003 (Western Australia), Electronic Transactions Act 2000(South Australia including New South Wales) [8] and Electronic Transactions Act 2001 (Australian Capital Territory). Although they are different the objectives of these Acts are similar. The objectives are to recognises the importance of the information economy to the future economic and social prosperity; to facilitate the use of electronic transactions; to promote business and community confidence in the use of electronic transactions; to enable business and the community to use electronic communications in their dealings with government. [9]

v. Malaysia

The Electronic commerce in Malaysia is still developing. However, there is a specific law governing e-commerce activities in Malaysia namely, the Electronic Commerce Act 2006. Other laws that support the application of e-commerce act include the Digital Signature Act 1997, the Contracts Act 1950, the Hire Purchase Act 1967, the Personal Data Protection Act 2010 and the Consumer Protection Act 1999. These Acts have different objectives but are related to e-commerce.

Privacy and protection of personal data in e-commerce: The governing laws in selected countries

The right to privacy and protection of personal data in e-commerce are raised when the personal data of consumers are collected by the websites owners in the online transactions. When the consumers provide personal information and credit card number they expect such information to be kept properly and protected. However, in some cases, the data collectors (data users) have used such information for unspecified purposes including selling the personal data to a third party.

In this regard, it is important for each and every individual to maintain his privacy right over his personal data. The consumers must ensure that there is a proper protection on their data and on their online communication with the businesses. Hence, the governing laws would include not only the e-commerce law and the privacy law but also the communication law or media law and the consumer law.

As mentioned earlier, protection of personal data is important in business or commercial activities. Following this need, the OECD (Organization for Economic Co-Operation and Development) has introduced a specific guideline on privacy protection. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data was then adopted and applied in 1980 [10] by its member countries consisting of Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden and the United States, Belgium, Iceland, the Netherlands, Spain and Switzerland. Such adoption was important in order to have comprehensive data protection system throughout Europe. Part 1 of the Guidelines defines ‘personal data" as any information relating to an identified or identifiable individual (data subject) and ‘transborder flows of personal data" means movements of personal data across national borders. [11]

Following this Guidelines, more laws and regulations that govern the right to privacy were introduced by several countries. In fact, in August 2012 the European Consumer Organization (BEUC) welcomes the European Commission’s proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). This proposal aims to enhance the rights of data subjects which include right to personal data protection. [12]

i. The United States (US)

In the US population, for instance, they are very concern about its privacy, but is willing to trade personal data for some benefit (e.g customer service). [13]There are few laws that control the use of personal data and provide privacy protection. Some of the laws are the Freedom of Information Act (FOIA) and the Privacy Act 1974, [14] Wiretap Act 1968, Electronic Communications Privacy Act 1986 (ECPA) and Computer Fraud and Abuse Act 1986 (CFAA). ECPA imposes civil and criminal penalties for the intentional interception, disclosure, or use of electronic communications that affect interstate or foreign commerce. There is also Children’s Online Privacy Protection Act 1998 (COPPA) that protects privacy of children under the age of 13 years old. The latest bill is on Consumer Privacy Protection 2011. [15] Other relevant source includes Fair Information Practices Principles. [16]

In December 2010, the Federal Trade Commission (FTC) has also proposed new frameworks in order to protect consumer privacy. [17]Among the proposed frameworks include the companies should promote consumer privacy throughout their organizations, companies should simplify consumer choice and companies should increase transparency of their data practices. These frameworks are good for consumer privacy protection.

ii. The European Union (EU)

In EU, the personal data of an individual may only be obtained when the individual gives consent and such data may only be used for specified purposes. The privacy protection in EU is governed by the EU Data Protection Directive 95/46/EC. [18] This directive is adopted by the European Union designed to protect the privacy and protection of all personal data collected for or about citizens of the EU, especially as it relates to processing, using, or exchanging such data. Under this Directive collecting and processing the personal data of individuals is only legitimate in

one of the following circumstances laid down by Article 7 of the Directive namely, [19]

(a) Where the individual concerned, (the 'data subject'), has unambiguously given his or her consent, after being adequately informed; or if data processing is needed for a contract, for example, for billing, a job application or a loan request; or if processing is required by a legal obligation; or

(b) if processing is necessary in order to protect the vital interest of the data subject, for example, processing of medical data of a victim of a car accident; or

(c) if processing is necessary to perform tasks of public interests or tasks carried out by government, tax authorities, the police or other public bodies; or

(d) if the data controller or a third

Under EU law, personal data can only be gathered legally under strict conditions, for a legitimate purpose. Furthermore, persons or organisations which collect and manage your personal information must protect it from misuse and must respect certain rights of the data owners which are guaranteed by EU law. [20]The current EU legal framework for protecting personal data is from 1995. The reform on European law on data protection is ongoing and from public consultations it is confirmed that the underlying principles of the current EU data protection legislation are still very much valid and have stood the test of time. However, it became equally clear that the EU needs a more comprehensive and more coherent approach in its policy for the fundamental right to personal data protection. Then, there was a review on E-Privacy Directive (2002/58/EC) which is also part of a review of telecommunications and electronic communications in the EU. [21]

iii. The United Kingdom

In order to protect the privacy right in online communication, the UK government has introduced the Data Protection Act 1998, [22] The DPA provides definition on ‘data’, ‘personal data’, rights of data subjects and others which include also right of access to personal data and the exemptions. According to this Act, ‘sensitive data’ includes the following:
(a) the racial or ethnic origin of the data subject,

(b) his political opinions,

(c) his religious beliefs or other beliefs of a similar nature,

(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) his physical or mental health or condition,

(f) his sexual life,

(g) the commission or alleged commission by him of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings [23]

Although the DPA seems to provide adequate protection on personal data, it was argued and commented by some people that the current penalties provided by the Act are inadequate which means stronger penalties are needed to punish the offender. They want the data criminals to be imprisoned. Nevertheless, the power to jail data protection offenders by the Ministers had not yet been enforced. [24]

Other than the DPA, there is also a Privacy and Electronic Communication (EC) Directive Regulations 2003. Under this Regulation, it is unlawful to, amongst other things, transmit an automated recorded message for direct marketing purposes via a telephone, without prior consent of the subscriber. [25] This Regulation is importance for every business to comply with since failure to comply with the ECR will result with fine or even criminal sanctions. This action can damage the reputation of the business and adversely affect the goodwill of the customers. So, if one uses electronic communications as a marketing tool, he should ensure that each communication is clearly identifiable as relating to the advertising or marketing of a product. This means that any commercial communication sent by email or text message should be clearly identifiable as such through its header - other required information can then be set out in the main body of the communication. [26]

But the Regulation was amended on 26 May 2011 to be ‘The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (SI 2011/1208)’. The amended Regulations implement the revised E-Privacy Directive (2002/58/EC Directive) on privacy and electronic communications in the EU. The amended legislations have introduced several things. Among them include a provider may now only place a cookie on a machine with the user’s consent, direct marketers are restricted on spending ‘spam’ and the Internet service providers (ISPs) and telecommunications service providers must implement security policies on processing personal data.[27]

Other than the above law the companies in UK have also been required to adopt Privacy Impact Assessment (PIA) which is available in PIA Handbook. The aim of the PIA is to help organizations assess and identify any privacy concerns. [28]

iv. Australia

Apart from the electronic commerce laws, there is also a specific law on privacy at the federal level namely, the Privacy Act 1988 (Cth). Under this Act, organisations must comply with all of the provisions of the Act together with the 10 *National Privacy Principles* (NPPs) in all of its dealings with the personal information of individuals. The Act also defined personal information as to be any information about an individual that identifies the individual or from which the identity of an individual can be reasonably ascertained, and can include a series of data that, when pieced together, reveals the identity of the individual, even if, for example, their name is not published. [29] However, this Act only regulates information privacy i.e the protection of people's personal information.

In addition, there are also two regulations regulating the privacy issues in Australia namely, Privacy (Private Sector) Regulations 2001 and Privacy Regulations 2006. Nevertheless, there were 295 recommendations for reform in the Law Commission's report which among others include:-

(a) the introduction of a set of unified privacy principles, to apply to both the public and private sector;

(b) the repeal of the small business exemption, which means that all private sector businesses in Australia, regardless of annual turnover, may be required to comply with the Privacy Act;

(c) removal of the employee records exemption, which will have the effect of all employers around the country being required to review their privacy practices with respect to employee (both present and past) files;

(d) the introduction of personal information protection provisions for deceased persons; and

(e) the reform of the credit reporting provisions of the Privacy Act, in order to simplify their application. [30]

In the event of any breaches of privacy complaints on such breaches may be lodged to the Privacy Commissioner office who will then investigate the matter and prepare case notes about the complaints. Normally, the complaints are resolved by way of reconciliation under s27(1) (a) of the Privacy Act 1988. [31]

There are also other legislations such as Telecommunication Act 1997 that deal with such breaches. This Act can be enforceable by the Australian Communications and Media Authority. However, the above laws are federal laws that do not deal with state and territorial matters. Hence, the privacy law in New South Wales, for instance, is governed by the Privacy and Personal Information Protection Act 1998 (PPIP Act) and other relevant legislations in that territory. PPIP deals with how all New South Wales public sector agencies manage personal information. It also sets out the role of the Office of the New South Wales Privacy Commissioner. [32]

v. Malaysia

In Malaysia, the right to privacy is not recognised as a fundamental right under the Federal Constitution. However, with the development of e-commerce a new law was passed in January 2010 which is known as a Personal Data Protection Act 2010 (PDPA). This Act seeks to regulate the processing of personal data of individuals involved in commercial transactions by data users. It also provides protection to the individual's personal data, thereby safeguarding the interests of such individual. [33] This Act defines the meaning of 'personal data' and 'sensitive personal data'. It also outlines the data protection principles and the exemptions, right of data subject including right to access personal data, to correct it, to prevent its processing for unlawful purposes and what amount to criminal offences under the Act. [34]

Nevertheless, there are comments on the adequacy of the above Act in protecting the consumer's individual privacy right. [35] The Act does not apply to non – commercial activities and it has not complied with certain requirements needed by the EU which requires all its member states to have adequate Data Protection Laws. [36] Following the introduction of this law, the Government of Malaysia has also planned to set up a specific department to monitor the implementation of the PDPA. [37]

Since privacy issue is also related to online communication, the Communication and Multimedia Act 1998 (CMA) is also relevant to be cited as reference. This can be seen in the case of *Telekom Malaysia Berhad* v *Tribunal Tuntutan Pengguna & Anor* [38] where issues on wiretapping, claims under Consumer Protection Act 1999 and CMA 1998 were raised by the parties.

The privacy issues further gained attention here when there was an argument that the private companies such as the credit reporting agencies (CTOS) have no right to keep data of individuals except the government since personal data is considered as a privileged information. [39]

Challenges in Protecting Personal information

Maintaining personal information of consumers or data subjects is very important in business and in any other transactions. This task is very challenging since the technology keeps developing and there are many attempts to invade privacy of consumers. With the online transactions become a norm in today's business and the new methods of committing crimes many countries have to consider revisiting and amending their existing laws on personal data protection and relevant laws such as e-commerce laws and consumer laws. In Europe, the Council of Europe is also revising its Data Protection Convention (Convention 108) to meet and overcome challenges that arise every day. [40] In this respect Article 29 Data Protection Working Party is referred to and further discussed. While in the US a new bill on Consumer Privacy Protection 2011 was passed in April 2011 to protect and enhance the consumer's privacy.

In summary, the challenges and threats to consumer privacy are elaborated in the following:

i. New data collection technologies

Advancement in technology has resulted with more development of new tools and technologies to collect data. When cookies and web bugs are used to gather consumers' information, many consumers' data are collected through online profiling. Even the protected categories of data can also be accessed. However, since the act of online profiling is not regulated consumers affected by such act has proceeded under different legal theories. [41]

ii. Cyber attacks: Identity theft, unauthorized access, spamming and phishing

Fighting against cyber attacks such as unauthorised access or hacking offence, identity theft or theft of information, spamming, phishing and many others are very challenging in e-commerce environment. [42] The cyber attackers are always targeting the customers' personal data available at financial institutions and credit card agencies that keep personal data of their customers.

Since in e-commerce, payment can be made online by using a credit card or other methods of payment such as electronic cash, electronic wallets, digital checks or smartcards there is a possibility that the data provided to such institution will be accessed and stolen by others. In this regard, the financial institutions and credit card agencies must ensure that their financial system is secured and the personal information or data of their client is kept private and confidential.

Crimes such as phishing and spamming may cause businesses money in the form of lost worker productivity and their ability to market their products. It also harms Internet Service Providers (ISPs) and large corporate networks, because it uses up large amounts of bandwidth capacity and adds to technical support costs. [43] This is a form of data breaches and a violation of consumer's privacy. According to a 2010 Ponemon benchmark study, the cost of data breaches to businesses – in terms of preventing, detecting, and notifying individuals of breach, as well as legal defense and lost business opportunities – have risen considerably over the past several years. [44]

In addition, an Internet Protocol (IP) addresses can also be a subject of privacy since the addresses are belonged to certain individuals. It was argued that the use of such addresses in identifying the websurfers or infringers in cases of copyright infringement is a violation of individual privacy. The question is whether such addresses are personal data and whether there was a violation of privacy of such personal data? [45]

iii. Data recovery and the procedural law

It is also challenging to seek or recover data of an individual involved in commercial disputes. The particular individual may argue that such disclosure is a violation of his privacy right or he may say that the information is privileged information. However, in certain situations he still has to do so as to be fair to the opposite party. In the UK, for instance, disclosure of personal data is allowed if it was necessary for legal proceedings. This was held in *Totalise Plc v Motley Fool Ltd* [46]. In this case, the defendant failed to use s.35 of Data Protection Act 1998 in his defence against the Plaintiff (the Internet Service Provider) who requires disclosure of the identity of defendant's internet subscriber who has posted defamatory remarks about the plaintiff in the defendant's website.

Procedurally, the process of discovery of data or disclosure proceedings is governed by Order 24 of the Rules of Court 2012 (Malaysia), Part 31 of Civil Procedure Rules 1998 (UK) and Rules 16,26 and 34 of Federal Rules of Civil Procedure (F.R.C.P) (US). There are many discussions on this discovery issues but this issue will not be discussed in details here.

Despite the above challenges, there are still several effective methods to protect the privacy of online consumers and their personal data. Among the methods suggested are conducting comprehensive risk assessment; [47] establishing privacy and data protection policy that protects the rights of the consumers. This policy was adopted by many companies including Demandware that respects the privacy of its customers, partners, employees, Web site visitors, and job applicants. It also provides guidelines on how that information is used; [48] conducting comprehensive trainings; having good data privacy management and conducting privacy impact assessment (PIAs) as to know the effectiveness of data protection policies etc.

Legal Remedies on Invasion of Privacy in e-commerce

Generally, any person whose privacy has been violated may seek legal remedies under the available laws. The consumers or affected party may choose either to file their case in court or to settle the case out of court. Among the remedies available to them are injunction and damages. However, these remedies may differ from one country to another.

In Malaysia, claim for remedies for cases of breach of online privacy are forwarded to Financial Mediation Bureau (FMB) who will mediate the matter. This FMB is an alternative to courts or arbitration which in charge of settling disputes between individuals or corporations and the financial services providers who are under the supervision of Bank Negara Malaysia or 'National bank' and a member of the bureau. It was reported that the FMB is handling 3000 cases as in October 2011 since there are increasing number of disputes in online transactions. [49]

However, the protection on violation of personal privacy in Malaysia is limited to informational privacy only. [50] This violation is discussed under the PDPA 2010 and also CMA 1998. According to section 5(1) of the PDPA 2010 any personal data user who breaches the provision under this Act has committed an offence and faces a maximum jail term of two years, a RM200,000 fine or both. Further, when there is incident such as hacking or unauthorised access to the personal data the criminal may be charged under Computer Crimes Act 1997(CCA) or alternatively, the Penal Code.(PC).

Alternatively, the consumer may also forward their complaints to the Consumer Claim Tribunal. [51]

Other than the above laws, there are specific laws that protect the consumers namely the Consumer Protection Act 1999 (CPA) and the Competition Act 2010 which prohibits anti-competitive conduct and abuse of dominant position, thereby protecting the interests of consumers. [52] According to section 2 of the CPA, the Act shall applies in respect of 'all goods and services that are offered or supplied to one or more consumers in trade including any trade transaction conducted through electronic means'. In order to provide further protection to the consumers the CPA has been amended in 2010 [53] and there are ten regulations that act as subsidiary legislations to the CPA. This amendment also protects the consumers against unfair contract term (UCT) that only benefit those who prepared them. [54] Further, the claim for remedies may also be made under the Specific Relief Act 1950 and the Sale of Goods Act 1957.

In the US, privacy litigation involves cases on data security breaches of credit and debit cards. In *BJ's Wholesale Club* [55] Sovereign sued BJ's Wholesale and Fifth Third Bank ("Fifth Third"), the merchant acquiring bank for BJ's Wholesale, in state court, asserting claims for negligence, breach of contract, and equitable indemnification. Sovereign maintained that the security breach occurred because BJ's Wholesale improperly retained and stored cardholder information instead of deleting that data immediately after a transaction, as required by Visa's Operating Regulations. The defendants removed the case to federal court and moved to dismiss Sovereign's claims. Sovereign amended its complaint, adding breach of fiduciary duty and promissory estoppel claims against BJ's Wholesale. Ultimately, the district court dismissed all of Sovereign's claims as to BJ's Wholesale and all of Sovereigns claims *except* its breach of contract claim as to Fifth Third pursuant to Federal Rule of Civil Procedure 12(b)(6).

In summary, the future of privacy in e-commerce is unpredictable. One author submitted that despite the existence of the legislative framework and the efforts of national and international data protection authorities and bodies, privacy abuse continues on a vast and persistent scale. [56]

CONCLUSION

Personal information is very important to protect one's own privacy and dignity. Principally, the personal information or data must not be disclosed to others except under certain circumstances. However, the information is easily supplied by consumers (data subjects) to businesses (data users) when there is any online or off line transaction. As a result some information has been stolen, manipulated or tampered. Following these incidents several laws and Regulations have been passed by several countries to regulate issues pertaining to e-commerce, consumers' data protection and privacy as well as consumers'

rights. However, the existing laws seem to be inadequate in protecting the privacy of personal information. This can be seen through several exemptions for law enforcement and for taxation. (such as in the PDPA). In fact, in certain law there is no provision that limit the collection of personal data. Hence, what the people can do is to control the supply of their personal data to others, to ensure the companies comply with their privacy policy and to keep the personal data as if it is a trust property. They should not allow any violation of such information in any event.

REFERENCES

[1] WTO, 'Work Programme on Electronic Commerce', Adopted by the General Council, 25 September 1998. (1998). Retrieved from http://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm. See also Gillies, Lorna E. (2008) *Electronic Commerce and International Private Law*. England: Ashgate Publishing Limited, 25.

[2] OECD. Retrieved at http://stats.oecd.org/glossary/detail.asp?ID=4721 . See also Gillies, Lorna E. (2008). *Electronic Commerce and International Private Law: A study of Electronic consumer Contracts*, USA: Ashgate Publishing, 4-27 and Ding, Julian. (1999). *E-commerce law and Practice*, Asia: Sweet & Maxwell, 21-27.

[3] E-commerce Benefits. Retrieved from http://www.ecommerceeducation.com/benefits-of-ecommerce.asp

[4] Warren, A.D. and Brandeis, L.D., (1890, 15 December). The Right to Privacy, *Harvard Law Review* (4), 193-220.

[5] Advertising and Marketing on the Internet: Rules of the Road. Retrieved from Federal Trade Commission. http://www.ftc.gov/bcp/conline/pubs/buspubs/ruleroad.shtm.

[6] See Directive 95/46/EC of the European Parliament and of the Council. (1995, 24 October). 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. Retrieved from http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

[7] Electronic Transactions Amendment Bill 2011 (2011). Retrieved from http://www.comlaw.gov.au/Details/C2011B00001

[8] Electronic Transactions Act 2000 no 8 (2000). Retrieved from http://www.legislation.nsw.gov.au/viewtop/inforce/act+8+2000+FIRST+0+N/

[9] Electronic Transaction Act 2000 (2000). Retrieved from http://www.austlii.edu.au/au/legis/nsw/consol_act/eta2000256/ . Electronic Transaction Act 2003 (2003). Retrieved from http://www.austlii.edu.au/au/legis/wa/consol_act/eta2003256/s3.html

[10] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Retrieved from http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[11] OECD. Retrieved from http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html

[12] BEUC. Retrieved from http://www.beuc.org/BEUCNoFrame/Docs/1/PIMFKFDDJMLKGHOCLLHLLIKEPDWY9DB1AY9DW3571KM/BEUC/docs/DLS/2012-00531-01-E.pdf

[13] Ackerman, Mark S., & Davis, Jr, Donald T. Privacy and Security issues in E-commerce, Review Chapter for the New Economy Handbook (Jones, ed.) in press. Retrieved from http://www.eecs.umi.edu

[14] The Privacy Act 1974 Act limits what the federal government can do with the data it collects. Retrieved from Federal Trade Commission http://www.ftc.gov/foia/privacy_act.shtm

[15] H.R. 1528: Consumer Privacy Protection Act of 2011. Retrieved from http://www.govtrack.us/congress/bill.xpd?bill=h112-1528

[16] T. Bilstad, Blake., & P. Enright, Keith. (2001, 30 April-9 May). Session 4: Consumer Privacy. Retrieved from http://cyber.law.harvard.edu/olds/ecommerce/privacytext.html

[17] Protecting Consumer Privacy in an era of rapid change: A proposed framework for businesses and policy makers. (December, 2010). Retrieved from http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

[18] EU Data Protection Directive. Retrieved from http://www.dataprotection.ie/viewdoc.asp?DocID=92 .See also Sumner, Stuart. (2012, February). Analysis: Data Protection- Is the EU going too far?. Retrieved from http://www.computing.co.uk/ctg/analysis/2144279/analysis-protection-eu

[19] Collecting and Processing personal data: What is legal?. (2012). Retrieved from

http://ec.europa.eu/justice/data-protection/data-collection/legal/index_en.htm. See also Brinson, J. Dianne., Dara-Abrams, Benay., Dara-Abrams, Drew., & Others. (2001). *Analyzing E-Commerce & Internet Law*, New Jersey: Prentice Hall PTR

[20] Protection of personal data. (2012). Retrieved from http://ec.europa.eu/justice/data-protection/index_en.htm

[21] Viviane Reding Vice-President of the European Commission, EU Justice Commissioner Assuring data protection in the age of the internet BBA (British Bankers' Association) Data Protection and Privacy Conference London (2011, , 20 June). Retrieved from http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/452&format=HTML&aged=0&language=EN&guiLanguage=en

[22] UK Data Protection Act 1998. (1998). Retrieved from http://www.legislation.gov.uk/ukpga/1998/29/contents

[23] Section 2 of UK Data Protection Act 1998. (1998). Retrieved from http://www.legislation.gov.uk/ukpga/1998/29/section/2

[24] Personal data blaggers should go to jail, MPs say: People who 'blag' personal info or sell it on should face prison – committee. (2011, 31 October). *The Register*. Retrieved from http://www.theregister.co.uk/2011/10/31/personal_data_blaggers_should_go_to_to_jail_say_mps/

[25] Privacy and Electronic Communications (EC) Directive Regulations 2003, Retrieved from http://en.wikipedia.org/wiki/Privacy_and_Electronic_Communications_(EC_Directive)_Regulations_2003

[26] Business link. Retrieved from http://businesslink.gov.uk/bdotg/action/detail?itemId=1075385158&type=RESOURCES

[27] E-Privacy: New laws to force company website overhaul. (June 2011). Retrieved from http://www.hfw.com/publications/client

[28] Privacy Impact Assessment. Information Commissioner's Office (ico). Retrieved from http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.aspx

[29] Weedon, Emma., Robertson, Mccullough. (2010). Privacy Rules: The Increasing Need For Organisations To Comply With Privacy Laws. 1 LNS(A) Xxxix. See also 'What is privacy ?'. Retrieved from http://www.privacy.gov.au/aboutprivacy/what

[30] ibid.

[31] Case Notes. Retrieved from http://www.privacy.gov.au/law/apply/casenotes

[32] Office of the Australian Information Commissioner. New South Wales. Retrieved from http://www.privacy.gov.au/law/states/nsw

[33] Cheng Leong, Foong., and Abu Bakar, Halina Jael. (2010, July-September). Personal Data Protection Act 2010, *Legal Herald*, Lee Hishammuddin Allen & Gledhill.

[34] See Munir, Abu Bakar. (2010, 19 July). *The Malaysian Personal Data Protection Act: What it means for data users'*, MSC Malaysia, Personal Data Protection Conference, The Royale Chulan Hotel, Kuala Lumpur. Retrieved from http://cdp.mscmalaysia.my/downloads/PDPConference/Prof%20Abu%20Bakar%20-%20PDP%20Conference.pdf

[35] Munir, Abu Bakar., & Mohd Yasin, Siti Hajar. (2010). *Personal Data Protection*: *The Law and Practice in Malaysia.* Asia: Sweet & Maxwell.. See also Azmi, Ida Madieha. (2002, 5-6th April). E-Commerce and privacy issue: An analysis of the Personal Data Protection Bill, 17th Bileta Annual Conference, Free University, Amsterdam.

[36] Habib.Shahanaaz. (2011, 16 October,). Personal Data still open to abuse, *The Star*, p26

[37] Personal Data Protection Act to be enforced in June. (2012, 4 September). Retrieved from Malaysian Law http://malaysianlaw.my/news/personal-data-protection-act-to-be-enforced-in-june-21646.html

[38] [2007] 1 Current Law Journal 300

[39] Decision To Bar Agencies From Keeping Personal Data Welcomed, (2010, 30 June), *Bernama News* at http://bernama.com/bernama/v5/newsgeneral.php?id=510030. CTOS is governed by the Credit Reporting Agencies Act (CRAA) (Malaysia).

[40] Kierkegaard,,Sylvia., Waters, Nigel., Greenleaf, Graham., Bygrave, Lee A., Lloyd, Ian., & Saxby, Steve. (2011, June). 30 years on-The Review of the Council of Europe Data Protection Convention 108, *Computer Law & Security Review*, Volume27, Issue 3, 223-231

[41] T,Bilstad, Blake. & Enright, Keith P. (2001, 30 April-9 May). Session 4: Consumer Privacy. Retrieved from http://cyber.law.harvard.edu/olds/ecommerce/privacytext.html..'Cookies' is an online tracking system that attaches pieces of code to our internet browsers to track which sites we visit as we search the web. See Privacy Rights

Clearinghouse.(2011,1 November). Retrieved from http://www.privacyrights.org

[42] A.Winn, Peter. (2007, August). The Guilty Eye: Unauthorized Access, Trespass and Privacy. *The Business Lawyer*, 62, 1395

[43] K.Neogi, Prabir., & Cordell, Arthur J.(2005). Trust and Confidence and the Digital economy: Issues and Challenges. Retrieved from http://www.arraydev.com/commerce/JIBC/2005-08/Negi.ht

[44] Brookman, Justin.(2011, 4 May). The Threat of data theft to American consumers. Retrieved from http://cdt.org/data-theft-threat

[45] Moiny, Jean-Philippe.(2011, August). Are Internet Protocol addresses personal Data? The fight against online copyright infringement. *Computer Law & Security Review*, Volume 27, Issue 4, 348-361

[46] [2001] EMLR 29.

[47] According to Ron Ross, a Fellow at the National Institute of Standards and Technology (NIST),"Risk assessments can help federal agencies effectively evaluate the current threat, organizational and information system vulnerabilities, potential adverse impacts to core missions and business operations—using the results to determine appropriate risk responses." See Comprehensive Risk Assessment Guidance for Federal Information Systems Published, (2011, 20 September). NIST *Tech Beat* Retrieved from http://www.nist.gov/itl/csd/risk-092011.cfm

[48] Demandware Privacy Policy. (2012, 23 April). Retrieved from http://www.demandware.com/Privacy-Policy/privacy,default,pg.html

[49] Ahmad, Massita. (FMB handles increasing number of online transaction disputes. (2011, 13 October). Retrieved from http://www.bernama.com/finance/news.php?id=619799

[50] Habib, Shahanaz.,(2011,16 October). Personal Data still open to abuse. *The Star*, p. 26.

[51] See *Edris Subeli & Ors* v *City Mortgage Sdn Bhd* [2009] 9 CLJ 120

[52] Competition Act to promote competitive environment. (2010, 6 July). Retrieved from http://biz.thestar.com.my/news/story.asp?file=/2010/7/6/business/6612473&sec=business. This Act came into force on January 2012. It will govern all firms, including government-linked companies (GLCs).

[53] See Consumer Protection (Amendment) Act 2010 (2010). Retrieved from http://www.cljlaw.com/membersentry/legislationdisplayformat.asp?MY_FS_AME_2010_1381

[54] Amended Consumer Protection Act offers better protection to consumers. (2011, 24 February). Retrieved from http://www.theborneopost.com/2011/02/24/amended-consumer-protection-act-offers-better-protection-to-consumers/

[55] See *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 533 F.3d 162 (3d Cir. 2008).

[56] Riley, Thomas B. (2000). Privacy as a Human Right - The Wave of the Future. In Riley, Thomas B . Okot –Uma, Rogers W'O., *Electronic governance and electronic democracy: Living and working in the wired world*, (pp.87-98). United Kingdom: Commonwealth secretariat and SFI publishing. See also Ahmad, Nehaluddin. (2008). The Right To Privacy And Challenges: A Critical Review, [2008] 5 MLJ cxxi; Wong, Rebecca. (2011, February). Data Protection : The Future of privacy, *Computer Law & Security Review*, Volume 27, Issue 1, 53-57 and Abdul Ghani, Norjihan., & Mohamed Sidik, Zailani. (2009. March). Personal Information and privacy protection in e-commerce, *Wseas Transactions On Information Science And Applications*, Issue 3, Volume 6, 407-416

ABOUT THE AUTHOR

Name: Duryana binti Mohamed

She has been doing research in the area of cyberlaws, electronic evidence , civil procedures and electronic commerce.

Mailing address: Department of Legal Practice, Ahmad Ibrahim Kuliyyah of Laws, International Islamic University Malaysia (IIUM), P.O Box 10, Jalan Gombak, 50728 Kuala Lumpur.

Tel:+60361964206.

Fax:+60361964854

e-mail : mduryana@iium.edu.my