Business & Management Quarterly Review, 3(1), 46-52, 2012
ISSN 2180-2777

CYBER COMMUNICATION: THE LEGAL RISK OF THE EMPLOYER

Norazlina Abdul Aziz and Irini Ibrahim
Universiti Teknologi MARA, Malaysia

ABSTRACT

The direction of new communication technology has shaped a trend that requires every layers of the society to participate in its network activity. An exclusion of oneself in these linkages of activities may results in isolation from the society. In responding to this new culture, employers have provided facilities within their working environment for the employees to be able to access the network. Simultaneously, an overwhelming usage of the internet has contributed to uncontrollable activities which exposed harms to many private lives. This is a conceptual paper which outlined the potential legal risk of the employer relating to the illegal internet communication made by the employee. This emerging risk requires the diversion of management impose on the employer within their working space. The Malaysian legal framework in governing the rights and liabilities of the Employer on illegal communication through internet i.e. The Multimedia and Telecommunication Act 1998, Sedition Act 1948, Internal Security Act 1960, The Defamation Act 1957, and principles under the law of Tort will be highlighted. The study also requires the need to look into the advanced countries approach that could be of help to solve the inadequacy of the said laws. The objectives underlying this study is to examine the Malaysian legal standing on the rights and liabilities of the Employer in Malaysia under the illegal internet communication suits and looking into the approach taken by the advanced countries into solving the inadequacy of the said laws with the intention of recommending the most relevant amendment to the existing Malaysian legal framework on the liabilities and protection for the Employer.
Keywords: Internet, Communication, Employer, employee

INTRODUCTION

One of the fundamental rights granted to every citizen is to enjoy the freedom of speech. The penetration of Internet into becoming the medium of communication has indeed moving in parallel with the objective underlying this right. Common roles of the Internet are to disseminate information throughout the world. However it is this particular function that has also allowed the rising of a complicated issue of illegal communication via internet. One of the potential areas is the extent of employers' liability. Accordingly, the research is conducted to identify are the current Malaysian Legal Framework in governing the employer's liability for wrongful communication via internet adequate.

ELABORATION OF KEYWORDS

Internet/Cyber

The internet had its origins in 1969 as an experimental project of the Advanced Research Project Agency (ARPA) and was called ARPANET. It started with linking computers and computer networks owned by the military, defense contractors and universities laboratories. It was extended later allowing researches across the country to access directly and to use extremely powerful super computer (Roy, 2002). Besides being mentioned in many legislation frequently but none has defined clearly the word internet. Literature agrees that it is not advisable to attempt to define internet as it may be superseded more rapidly than law can be enacted and amended. While the owner of facilities such as satellite earth stations, broadcasting transmission towers and equipment, mobile communications base stations, telecommunication lines and exchange, radio communication transmissions equipment and broadband fiber optic cables are categorized as network facilities provider (Roy, 2002 at pg 7). Internet is usually intermediated by Internet Service Provider. Vakul Sharma (2006) in his book defines a network service provider as an interactive network service. Depending upon its functional attributes a network service provider may act as an 'information carrier' or 'information publisher'. In summary it can be said that the primary function of an internet or

network to provide medium for activities across border. This could be in the form of dial-up, broadband, satellite, microwave or any other communication media. Communication across the globe has spawned discussion group which have been organized into news group, electronic bulletin boards and electronic mailing lists for the exchange of views and experiences and the dissemination of information. Although the way in which they are set up and operated varies, they provide similar scope for the promulgation of defamatory material (Rowland and Macdonald, 1997 at pg 318).

Illegal Communication

Under the Communication and Multimedia Act 1998, a Code was formed by a content forum. The Content Code is a model of self regulation among industry and is drafted by members representing all the key industries. Although compliance is voluntary, as it is the industry's own regulation, there is no perceived problem of lack of bindingness as this Code is drafted by the industry players to bind them. The Code through section 233 of the Act defines the word as follows:

any sound, text, still picture, moving picture or other audio-visual representation, tactile representation or any combination of the preceding which is capable of being created, manipulated, stored, retrieved or communicated electronically.

With reference to the above definition it can be said that any dissemination of the above form of content which are obscene, indecent, false or offensive content which can lead to annoying, abusing, threatening or harassing another person are said to be illegal communication within the CMA. While other illegal communication are specifically stated in a specific act such as defamatory words in the Defamation Act 1957, seditious word in the Sedition Act 1948, communication prohibited under the Internal Security Act.

Employer

An employer is a person or entity who hires another to perform service under an express or implied agreement and has control, or the right to control, over the manner and means of performing the services. An employer has the right to control an employee (U.S Legal definition, 2011). Employer can also be define as a legal entity that controls and directs a servant or worker under an express or implied contract of employment and pays (or is obligated to pay) him or her salary or wages in compensation(Business Dictionary, 2011). Both of the above definition agree that employer has control over the person they invest money. To the other end, they also need to be responsible over the action of the employee if it is done within the scope of employment.

FORSEEABLE LEGAL RISKS FOR THE EMPLOYER

Defamation

To highlight a defamation case, the fundamental elements that would invoke a cause of action are the making of a defamatory statement, the defamatory words must refer to the claimant and the defamatory statement has been circulated to another third party. The frame that would suit the picture of employer is the third element, which is to proof that the defamatory statement has been circulated or distributed. The question is, under what circumstances, would an employer be held liable? Vakul Sharma (2006) in his book has listed the following circumstances to answer the question:

i) The employer knows, or has reason to believe, that the information content it is transmitting, is unlawful
ii) The employer fails to take reasonable steps to determine if the information content that it transmits is unlawful.

Literatures(Charlesworth and Reed, 2000) has stated that from the above statements, the potential of an employer to be challenged under a civil or criminal suit depends on the knowledge, the committed act was within the course of employment of the employee and exercising reasonable care in filtering all the information posted using its facilities. Smith(2007) raise up an opinion stating that the reason why employer

are at greater risk relates to the usage of the internet that create evidence of the wrongful communication made by the employee while sending, circulating emails and attachments. It involves a self recording process. The rights and liabilities of the employer under a defamation suit have been discussed (Smith, 2007) in many countries around the world. The possibility of being sued for unknowingly defaming the character of another person or company now makes the employer accountable for violating laws that previously applied only to journalist and music producers (Jan Samoriski, 2002).

The terms 'qualified immunity' has emerge from this EU directives where the ISP or employer is only entitle to used the immunity upon fulfillment of certain conditions as follows:

i) Has no actual knowledge of the defamatory words

The case of Bunt v Tilley [2006] 3 All ER 336, has been quoted by the literature to describe that ISP exercising passive role do not have actual knowledge. This is the first case that has utilized the provision under the EU Directives. It was also commented that this case has provide a better protection to the ISP as compared to the rulings under the Godfrey's case which upheld section 1 of the Defamation Act 1996.

ii) Removing the defamatory statement immediately upon receipt of notice to remove

Literature (Klett, 1997) has commented that EU law only contains'safe harbours' for the providers of strictly delineated 'mere conduit', 'caching', and 'hosting' services and the ISP generally do not profit from the provided legal certainty. For each of these categories it contains a conditional liability exemption. The result is a patchwork of degrees of liability across the EU. It was argues(Jan Samoriski, 2002) that currently EU law takes insufficiently into account the added value selection intermediaries provide to the online environment and their contribution to the free flow of information. Vakul Sharma (2006) again commented that it really makes sense for an ISP or employer to enjoy unqualified immunity from liability based on material created by third parties, and made available through its service. But this 'unqualified immunity' is lost if it either provides proprietary content or knowingly distributes the unlawful content.

In Malaysia, civil defamation is provided under the Defamation Act 1957. A defamatory statement against a private person is actionable. Applying the present libel laws to cyberspace or computer networks entails rewriting statutes that were written to manage physical, printed objects and no computer network or services. However, the said Act provide for publications in printed materials and broadcasting through radio or television (A. C Macdonald, 2004 at pg 16. It was further stated that since the law applies to published or broadcast materials, hence in principle it applies to materials such as blogs and websites published on the Internet.

Vicarious Liability

It's defined (A.C Macdonald, 2004) as a legal liability attached to the shoulder of the employer if the employee wrongful abuses the usage of the internet during course of their employment. In such case the knowledge of the employer is irrelevant. The principle underlying the case of *Imperial Chemical Industries Ltd v Shatwell[1965] 1 All ER 656* states that vicarious liability only arises where the employees commit torts. Further, in the case of *Credit Lyonnais Bank Nederland NV v Export Credits Guarantee Department [1999]1 All ER 929* it was decided that before the employer could be vicariously liable, all of the features necessary to make the employee liable in tort must have occurred in the course of his employment. If the individual in charge of editing or controlling content is an employer or agent of the service provider, the service provider, employer along with the individual can be held liable under the common law theories of vicarious liability. The important point raise up by literatures (R. Ferrera *et al.*, 2001) are the wrongful act was committed within the scope or terms of the employment. The main factor that must be considered while determining liability of the employer is the working hours. By the word of Lord Coleridge in the case of *Ruddiman v Smith (1889) 60 LT 708,* he stated that a master is liable if the act of negligence was done by the servant, either within the scope of his authority or as an incident to his employment. Grove J while deciding the case of *Stevens v Woodward* (1881) 16 QBD 318 had a consensus on the words of his colleague and he further add that the act must be something incident to the employment for which the servant is hired or which it is his duty to perform.

Contract

With the advance of technology and the creation of digital signature, employers are exposing to be bind by non foreseeable contract (Charlesworth and Reed, 2000). Upon fulfillment of elements of contract (offer and acceptance etc) the agreement will bind both parties to contract. Either party can be represented by an agent (employee) having acted within his actual authority or ostensible authority. In the case *of Generale bank Nederland NV v Export Credits Guarantee Department Times Law Report 4 August 1997* it was held that to bind an employer to a contract the agent must have acted within the implied and express authority.

Harassment

Cyber harassment is not new to Malaysia. It develops as fast as it does through all parts of the world. What may be far left behind is the traditional laws that failed to address this matter appropriately or unable to cop up with the fast growing technology (Norazlina and Irini, 2011). The nearest it could be is to look into the development of Malaysian laws on sexual harassment. Usually Complaints made on sexual harassment are classified under disciplinary issues. The victim only chances of getting a fair trial are by complaining to their employer or superior (Noraini and Norazlina, 2008). Sexual harassment is rarely recorded and sometimes it happens between the harasser and the victim in isolated situation. The only opportunity is if the harasser is practicing sexual harassment to more than one person in the workplace. In the case of *Lister & Ors v Hesley Hall Ltd, House of Lords, 3 May 2001* where a warden at school committed sexual assaults to the victim at school. The school was held to be liable as the incident happen within workplace by the school's employee. Nevertheless the victims of cyber harassment are spared with some lights of hope in succeeding the claims. The function of caching in the internet medium allows the inevitable act to remain in the memory of the computer. This can be tendered as evidence in court. Unfortunately having concrete evidence will not provide sufficient protection for the victims as the inadequacy of the existing laws does not permit justice to be carried out. For cases of cyber harassment, if it happens in workplace by the employee, the employers are exposed to the claims of vicarious liability. A disciplinary discourse would later await the employee. In a situation where both the harasser and victim works under the same roof and the act are conducted during office hour, then the harasser will potentially faced a trial on misconduct.

Disseminating obscene material

In the context of internet, it can be categorized that an act of 'publication' includes 'distribution'. The European Parliament Council has set an important precedent introducing the policy through a report of "Illegal and Harmful Content on The Internet Communication" by the Economic and Social Committee of the Regions which states that what is illegal offline must be illegal online (Ida Madieha, 2007). In response to the need to regulate the internet content that bears the possibility to impose liability to the innocent employer, certain laws were amended on suggestion of the Committee. Their recommendations were given effect in the Criminal Justice and Public Order Act 1994 which amended sections in Obscene Publications Act 1959(Rowland and Macdonald, 1997). In 1994, the UK Protection of Children Act has been amended to extend the definition of photograph as to include computer data. This has widened the usage of the statute to include internet communication. Section 1(1) of the Obscene Publications Act 1959 makes it a criminal offence to publish any obscene article. In the case of *Moonsar v Fiveways Express Transport Ltd, EAT September 27,2004* the employer were held liable for the failure to end the circulation of pornographic images which was downloaded by male employees in the presence of female employee.

Privacy Protection

Conflict between protection of the employee's privacy and profit making has been debated (Taras *et al.,2004)* when some of the employer opted to include monitoring system within the computer network at the workplace. Some of the employer was accused to have done it on profit making base. The less the employee accesses the computer the more productive they became and the more profit the employer would gain. This in a way has been challenge to encroach the Freedom of Speech right.

ISSUES ASSOCIATED WITH THE LIABILITY OF THE EMPLOYER

While anticipating the employer's risk, the employers in many countries are allowed to act against the spirit of promoting Freedom of Speech. They are allowed to monitor the electronic communication done by the employee in the workplace. This environment is well displayed within the U.K jurisdiction. The U.K Investigatory Powers Act 2000 gives power to the operators of private networks (inclusive of employer) to limit the usage of the employees blogs for the scope of employment only. Generally employees in United States are not allowed to use employer's email or internet systems for personal use. They used by the principle of 'business use only' policy. Today's culture of work very much contributed to a raising problem of absurd definition of workplace. Some are able to work from home. Controlling the employees' activities had become very challenging. There is a need to define a clear scope of workplace. Yet some decide that by giving interpretation will limit any new emerging culture in future nearby. Dealing with technologies we can never keep up with its rapid development. Some writers(Bidgoli, 2006) were of the opinion that employer should also address the scope issues in the context of wireless devices including whether to permit reasonable personal email or internet access on the job using wireless devices.

MALAYSIAN LEGAL STANDING

The Communication and Multimedia Act 1998(CMA)

The CMA is said to be based on the basic principles which focus more on the process and procedure rather that content. It promotes industry self regulation (Mazlina and Norazlina, 2010). In other word the employer are allowed to monitor the content disseminate by their employees via internet by self regulate. In cases involving technology an employer's restriction may varies to another depending on their nature of work, place of work and categories of employees. Therefore having one parent act would be insufficient to govern the whole lot. Nevertheless, the CMA does infer that a commission will be playing a role in regulating the content available on and accessible from the Internet and it is only within local jurisdiction. The Communications and Multimedia Content Forum of Malaysia recommended for the establishment of a Malaysian Complaints Bureau. The most important is that all complaints received from the public must be made in writing. If possible, the part of the Content Code that has been breached together with supporting documents or details of the alleged misconduct should be made clear to the Bureau. Among the matters that need a proper look into discussion would be the degree and standard to be applied when regulating (Juriah, 2002). In the parent Act, the main provisions prohibiting illegal content are provided under sections 211 and 233 of the CMA. Both sections prescribed the limit impose upon the service provider, and the usage of any network facilities or services. This section does not specifically mention the word employer, nevertheless from the above discussion and court's decision, employer fit among the scope of definition. Any publication of obscene, indecent, false or offensive content which can lead to annoying, abusing, threatening or harassing another person are strictly prohibited. Compliance with the Code brings a number of benefits e.g. it will be a defense against any prosecution, action or proceeding of any nature, whether in court or otherwise. As the likelihood of employers of being sued or charged for hosting illegal or unlawful content is clear, taking note of their obligation under the Code will prove to be a wise choice.

Sedition Act 1948

The Sedition Act 1946 (SA) was introduced by the British in 1948, the same year that the autonomous Federation of Malaya came into being, with the intent of curbing opposition to colonial rule. The term "sedition" is not defined under the SA whereas "seditious" is prescribed as "when applied to or used in respect of any act, speech, words, publications or other thing qualifies the act, speech, words, publication or other things as one having a seditious tendency". To date there is no case filed suing the employer under the sedition act. Nevertheless the following provision might shed some possibilities. Section 4 of this act provides that it becomes a criminal offence when anyone who "does or attempts to do, or makes any preparation to do, or conspires with any person to do" an act with seditious tendency, such as uttering seditious words, or printing, publishing or importing seditious literature, is guilty of sedition. It is also a crime to possess a seditious publication without a "lawful excuse". The employer might be innocently guilty if he is found to

have conspired with his employee or he is caught having possession of the seditious material. This is irrelevant of the act was done within working hour or at the workplace.

DEVELOPMENT IN EUROPEAN UNION, UNITED KINGDOM AND UNITED STATES

Literature (Chelsea L.Y.Ng, 2004) has contended that the debate on this particular issue has started in UK since 1999 during the trial of the case of *Godfrey v Demon [1999] All ER 342*. In the context of internet, literature (Chris and John 2002) categorized an act of 'publication' includes 'distribution' (Juriah, 2002). However the development in UK states that intermediaries will not be categorized as author, editor or publisher if it only involved as the operator of or it has no effective control. UK was said(Endeshaw, 2001) to have been efficient in introducing the Defamation Act 1996 to clarify the extent of liability of various persons involved in electronic publication. Literature (Juriah, 2002) agrees that the UK law of Defamation is in line with the provision under the Electronic Commerce (EC Directive) Regulations 2002 which has laid down the principle that the intermediaries will not be held either strictly liable or for their negligence for transmissions provided they do not commence the transmission, do not select the receiver of the transmission or do not select or modify the contents of the transmission. The United Kingdom has swapped the Directive on Electronic Commerce into national law in 2002 with the Electronic Commerce Regulations 2002 and did not insert additional exemptions for providers of hyperlinks and information location tools. In the end of 2006, the U.K. government's Department of Trade and Industry (DTI) now called the Department of Business Enterprise and Regulatory Reform, conducted a review of the intermediary liability regime specifically addressing the question whether the existing safe harbours should be extended to providers of hyperlinks, location tools and content aggregation services. In United States the Communication Decency Act 1996(CDA) has answered the call to regulate speech through internet. It was stated by Jan Samoriski (2002)in his book that the U.S Supreme Court ruled that expression on the internet is entitled to a high level of constitutional protection. Several writers agreed that the U.S Constitution guaranteed right of privacy. The purpose of this Act specifically through Article 230 of the Act is to promote good conduct of the ISP or the employer.

CONCLUSION

To date many advanced countries such as United Kingdom and European Union has experienced progressive development to address this matter. These countries currently have advanced principles and statute of law. The litigation in these countries had determined legal responsibility for the online hosting, publishing and possession of unlawful and illegal content. The Malaysian Defamation Act 1957 attaches liability both to the author of a defamatory statement and the publisher thereof. However, the statute does not specifically address the employer's liability for wrongful publication and dissemination over the internet. Malaysian traditional law has not defined clearly on the extent of liabilities of the employer. Neither is there a clear distinction between an ordinary speech made through the old media and speech made through internet. Malaysian court has not been challenged to decide on these issues as there are not many claims being submitted to the Malaysian court. In a nutshell, there is lack of law authorities that could be of reference to settle legal issues that arise from employer's liability for employee's wrongful communication within the internet in Malaysia. There is a need to reform the current Malaysian legal framework to address the *lacunae's* stated above. Balancing the functions of the Internet in promoting freedom of speech and laying down the limitation to this right should be the main concern. Future study could try to address this concern by looking into the development in other advanced jurisdiction of United Kingdom and European Union with the objectives of recommending the appropriate reformation to the Malaysian legal framework.

REFERENCES

Alexander K. (1997). Cyberspace and Copyright in Washington and Kuala Lumpur: Should Service Providers be liable Under U.S and Malaysian Copyright Law?, Cyberspace-Law Seminar online available at http://www.file.PHD/ISP/klett.htm accessed on 26 May 2010.

Andrew C. and Chris R. (2000). The Liability of Internet Service Providers and Internet Intermediaries in Chris R and John A. (2000), Computer Law, Blackstone Press Limited, United Kingdom.

Assafa E. (2001) Internet and E-Commerce Law with Focus on Asia Pacific, Prentice Hall, Singapore.

Chelsea L.Y.Ng. (2008). Facing up to libel suits, The Sunday Star online available at http://mavrkylawofdefamation.blogspot.com/ accessed on 27 May 2010

Daphne G. T., James T. B. and Anthony M. T. (2004), Information Technology and the world of Work online available at http:// books.google.com accessed on 1 August 2011

Diane R. and Elizabeth M. (1997), Information Technology Law, Cavendish Publishing Ltd, London.

Gerald R. F., Stephen D L., Margo E.K.R., Ray A., and William T S. (2001). Cyber Law: Text and Cases, South Western College Publishing, Ohio

Graham J.H.S. (2007), Internet Law and Regulation, Sweet & Maxwell, London.

Hossein B. (2006), Handbook of Information Security, John Wiley & Sons Publication, London

Ida Madieha A. (2007). Content Regulation in Malaysia: Unleashing Missiles on Dangerous Web Sites, Journal of Information, Law and Technology pp. 4

Jan S. (2002), Issues in Cyberspace:Communication, Technology, Law and Society on The Internet Frontier, Pearson, Massachussets.

John X K. (2007). Hosting Liability-Overview, JISC Legal online at http:// www.jisclegal.ac.uk accessed on 31 May 2010

Juriah Abd J. (2002). Media in Digital Environment Legal Development of Television Broadcasting in Malaysia, International Conference on Law and Commerce, International Islamic University Malaysia, 25-26 June 2002

Lynda A.C.M. (2004). Tolley's Managing Email and Internet Use: a Practical Guide to Employers, John Wiley & Sons publishing, United States.

Mazlina M. and Norazlina A.A. Legal Challenges of the Blogging Activities, in Proceedings of International Conference on Communication & Media, 6 June 2010, Malacca

Norazlina A.A. and Irini I. (2010), Child's Right to Free Flow Information via Internet: Liability and Responsibility of The Internet Service Provider in Proceedings of Asean Institute Conference on Environment Behaviour (AiCebs), 7-9 December 2010, Sarawak

Norazlina A. A. and Irini I. (2011). Cyber Harassment: Study on the Behaviour of the Harasser and Protections of the Victims", Asean Conference on Social Science and Science Research(ACSSSR), 7-9 June 2011, Penang.

Noraini I. and Norazlina A.A. (2008), Defamation on Internet: Freedom of Speech v Protecting the Reputation in Proceedings of 5th Asian Law Institute (ASLI) Conference, 5th -6th May 2008, Singapore

Reed C. and Angel J. (2002), Computer Law, Universal Law Publishing, India.

Roy J. G. (2002), Cyberlaw National and International Perspectives, Prentice Hall, New Jersey.

Samtani A. The Limit of Liability of The Network Service Provider available online at www.ieid.org/congreso/ponencias/Anil Samtani.pdf accessed on 10 March 2010