Combating anonymous offenders in the cyberspace: An overview of the legal approach in Malaysia

Conference Paper · March 2017

DOI: 10.1109/Anti-Cybercrime.2017.7905255

1 author:

Nazli Ismail Nawang
Universiti Sultan Zainal Abidin | UniSZA
25 PUBLICATIONS **24** CITATIONS

SEE PROFILE

Combating Anonymous Offenders in the Cyberspace: An Overview of the Legal Approach in Malaysia

Dr Nazli Ismail Nawang
Faculty of Law and International Relations
Universiti Sultan Zainal Abidin (UniSZA)
21300 Kuala Nerus, Terengganu, Malaysia
inazli@unisza.edu.my

Abstract — **Among the most treasured characteristics of the Internet is arguably its default technical architecture that facilitates online anonymity. This feature is most commonly cherished by Internet users as they are empowered to publish online content anonymously; or in the alternative to conceal their true identities behind fictitious names (pseudonyms). Anonymity is believed to have bolstered freedom of speech as any speakers could freely express their ideas or personal views in the cyber world without the fear of being identified and retaliated. Unfortunately, anonymity poses new challenges to law enforcement agencies as well as victims of cyber-crimes as they would find it difficult to trace and identify the culprits. For that reason, the Malaysian legislature has in 2012 passed a new law, section 114A of the Evidence Act 1950 that has the effect of shifting the burden of proof on the alleged offenders to prove his innocence. The passing of this controversial provision has led to heated debates between the government and human right defenders on the ground that such law seems to be very oppressive and could be easily manipulated by prosecutors in criminal cases as well as claimants in civil suits. By referring to reported cases and judicial decisions, this paper attempts to scrutinize in details section 114A of the Evidence Act 1950 and its implications on the legal system in the country; and ultimately to lend some assistance in unravelling the dispute between the proponents and opponents of the new law.**

Keywords — anonymity; burden of proof; presumption of publication; cybercrime; Malaysia

I. INTRODUCTION

Malaysia's venture into the cyber world started with the setting up of the country's first Internet service provider (ISP), the Joint Advance Research Integrated Networking System (JARING), in 1992 by the Malaysian Institute of Microelectronic Systems (MIMOS), which was a unit under the Prime Minister's Department (Asia-Pacific Network Information Centre, 2004). The government then in December 1996, established the National IT Council (NITC) that was entrusted and responsible for the launch of the National IT Agenda (NITA), the national policy that provides the foundation and framework for the utilisation of information and communication technology (ICT) in the country (NITC Malaysia, 2014). Prior to that, Dr Mahathir Mohamad (the Malaysian forth Prime Minister) has on 1 August 1996 launched the gigantic project of the Multimedia Super Corridor (MSC) Malaysia, the Malaysia's version of Silicon Valley, in order to augment the people's participation in the Internet and to exploit the economic potential from ICT related industries (Reid, 1998). Since then, the usage of the Internet in Malaysia has ascended greatly with the latest report released by the Malaysian Statistics Department on 29 July 2016 shows that 71.1 percent out of the total population in 2015 aged 15 years and above had used the Internet compared to merely 28 subscribers when JARING was commercialised 25 years ago.

In order to oversee and regulate the development of the Internet and its related activities, the Malaysian Parliament has enacted a number of specific legislations including Digital Signature Act 1997, Computer Crimes Act 1997, Telemedicine Act 1997, Copyright (Amendment) Act 1997, Communications and Multimedia Act 1998, Malaysian Communications and Multimedia Commission Act 1998, Electronic Commerce Act 2006, Electronic Government Activities 2007 and Personal Data Protection Act 2010. Apart from that, the existing statutes of the Evidence Act 1950 and the Penal Code have also been amended to suit with the rapid changes of the Internet. Nonetheless, the efficacy of these laws in tackling cybercrimes and related offences in the cyber world has been in limbo partly due to the anonymous nature of the Internet that makes it difficult, although not impossible, to trace and identify the true identities of the offenders.

II. ANONYMITY

The word 'anonymity' has been defined as the condition of being anonymous, whilst 'anonymous' refers to (of a person) not identified by name; of unknown name (Oxford Dictionaries, 2016). Silva and Reed (2015) described an anonymous person as someone who is unnamed, unidentified, unknown, unspecified, undesignated, unseen or unacknowledged. In short, anonymity renders a person not to be identified or recognised by the public.

Social sciences have submitted that anonymous speakers tend to act differently when they cannot be identified (Burkell, 2006). Zimmerman (2012) argued that online anonymity empowers a sense of self-government and a greater range of self-expression. This is arguably true in a developing country like Malaysia where the traditional print and broadcast media are strictly controlled by the ruling government since they are perceived as 'vital agents of social change' in promoting unity among the people of different races and ethnics (Anuar, 2004). Consequently, it should not be a surprise when Kim (2001)

978-1-5090-5814-3/17/$31.00 ©2017 IEEE

observed that certain quarters in the society were no longer influenced or dependable on the news or coverage by the mainstream media when more often than not their reports or stories are glaringly biased and favourable towards the ruling government. On the contrary, political criticisms and critical dissent towards the government and its policies were completely blocked from entering the public domain (Mohd Sani, 2009).

Nonetheless, the rapid development of the Internet and a vast array of web-based communications such as blogs, online news portals, social networking sites like Facebook and Twitter and many others have resulted in the previous rigid control over the traditional media to be futile and pointless. This is apparent since the government are no longer capable to dictate or exert total control over the dissemination and publication of huge amount of information in the cyberspace. In relation to this, Surin (2010) argued that the Internet has altered the media landscape in the country by shifting the power to publish from the domain of the traditional print and broadcast media to the new media.

Apart from the technical architecture of the Internet that makes it difficult (though not impossible) to be controlled and regulated in the same manner like the traditional print and broadcast media, the existence of the no censorship of the Internet policy in Malaysia has further caused the new media to be subjected to a very minimal regulation. The no censorship policy was firstly announced by Dr Mahathir Mohamad during his promotion of the MSC Malaysia to foreign investors overseas in 1997 (Steel, 2007). The policy has then been incorporated into both the MSC Malaysia Bill of Guarantees and the Communications and Multimedia Act 1998. George (2006) highlighted that the no censorship policy was primarily framed to attract foreign investors to the MSC Malaysia. In addition, Davidson (1998) observed that the policy is also aimed at handling the incredulity of potential investors and close rivalry from Singapore and other countries in the Southeast Asia (Davidson, 1998). In relation to this, Ismail Nawang (2015) argued that the Internet's perceived economic value has resulted in the government to disregard the strict regulatory regime that have been applied to the traditional print and broadcast media.

Due to the 'soft' approach that has been adopted by the government to regulate the Internet as well as online based publications, the Internet users seem to enjoy 'greater' right to freedom of speech in the cyber world. Suparmaniam (2012) asserted that such approach has arguably improved the ranking of press freedom in Malaysia as the people are now permitted to express and publish their personal opinions and views on any issues or topics of public interests. On the same note, Wu (2005) argued that online publications, particularly blogs, have not only revitalised freedom of speech, but also have reshaped and redefined the landscape of the media in the country.

Despite the fact that the Internet has been effectively used to promote free speech, the new media has unfortunately been misused or exploited to disseminate illegal and harmful content including defamatory statements, hate speech, indecent and obscene materials and many other illicit online contents. This scenario is further worsened when the online offenders resorted to anonymity in order to conceal their true identities from being traced and identified by enforcement agencies. The increase of these unlawful publications has prompted the then Minister in the Prime Minister's Department, Dr Rais Yatim, to announce that the government will unleash 'set of missiles' on Internet publications that threaten the security of the country (Azmi, 2004). Regardless of the announcement, the provision and publication of illegal content and improper use of the Internet have already been regarded and declared as criminal offences and upon conviction, such offenders are liable to imprisonment and/or fine under the Communications and Multimedia Act 1998. Apart from that, a specific piece of legislation, namely the Computer Crimes Act 1997, has also been enacted to tackle cyber-crimes. In addition, the existing statutes such as the Defamation Act 1957, the Sedition Act 1948 and the Penal Code could also be extended and applied to the new electronic environment.

Unfortunately, the enforcement agencies were facing with an uphill task, though technically still possible, in tracing and identifying anonymous cyber offenders. And even if the alleged offenders could be attributed and apprehended, the prosecutors then confronted another difficult hurdle to hold them guilty or liable for the commission of these offences due to the existence of certain weaknesses or loopholes in the existing statutes.

The difficulty of proving such a case could be best illustrated with the case of *PP v Muslim Ahmad* (2013). The respondent (accused) was charged under section 233(1)(a) of the Communications and Multimedia Act 1998 for posting offensive comments against the state government's official portal. The court of the first instance acquitted and discharged the respondent as the appellant (prosecutor) failed to prove the case beyond reasonable doubt even though the comments were traced to his Internet protocol (IP) address since there was a slight possibility that someone else could have used the same IP address. However, the case was reversed on appeal as the High Court found that the trial judge had erred in her findings as she did not consider the failure of the respondent to state his whereabouts during the commission of the alleged offence was a bare denial and hence did not raise any reasonable suspicion in the case.

Similarly, in the subsequent case of *PP v Rutinin Suhaimin* (2013), which involved the posting of offensive remark on the same state's portal, the respondent (accused) was also acquitted by the trial judge. It was decided that there was no *prima facie* case against the respondent as the appellant (prosecutor) failed to prove the offensive remark was posted by the respondent and that the Internet could have been accessed by anyone from the same computer. On appeal, the previous acquittal was quashed and the respondent was ordered to enter his defence. It was decided by the High Court that the trial judge had failed to consider the strength of circumstantial evidence by forensic expert indicating that the disputed Internet account belonged to the respondent and that there was no evidence that any other person used the computer at the time of the offence.

The aforesaid decisions have clearly shown the hardship and difficulty faced by the prosecution in proving such cases against the alleged offenders. As such, it is not a surprise that

only these two cases, though on appeal, have been ruled in favour of the prosecution. For that reason, the government has inserted a new section of 114A to the Evidence Act 1950 in order to tackle and resolve the predicament faced by the prosecution.

III. Section 114A Of The Evidence Act 1950

Section 114A, entitled 'Presumption of Fact in Publication' was inserted as a new amendment to the Evidence Act 1950 vide the Evidence (Amendment) (No 2) Act 2012. The amendment was tabled in the Parliament on 18 April 2012 by the Minister in the Prime Minister's Department, Mohamed Nazri Aziz, with the principal aim of resolving the burgeoning issue of online anonymity. During the Second and Third Readings of the Amendment Bill, the Minister has highlighted the ever-increasing challenges of the enforcement authorities in handling cybercrimes and that such amendment was necessary and indeed timely to facilitate the identification and proving of the true identity of anonymous offenders. The amendment was then passed without substantial debate on 9 May 2012 and it came into force on 31 July 2012.

The passing of the amendment has nevertheless received mixed reactions from the public as it has introduced a rebuttable presumption of fact in both civil and criminal cases for publication and ownership of publishing of such content on the Internet. The Centre for Independent Journalism (2012) has strongly objected to the new amendment on the perception that the presumption could lead to arbitrary arrest and prosecution of innocent persons and this is clearly against the basic principles of a fair legal system which presume a person is innocent until proven guilty by the prosecution. It was further alleged that since section 114A will impose the burden on the accused or defendant to prove his innocence, it will have a serious chilling effect on the exercise of the fundamental right to freedom of speech and expression as any ordinary people may simply resort to self-censorship to avoid any unwarranted consequences in the future.

On the contrary, the proponent of this new amendment asserted that the enforcement agencies are still required to conduct comprehensive investigation to trace and identify the real suspects before making charges (The Sun Daily, 2012). This is in parallel with the explanation by the Minister during the Parliamentary debate which provides that the prosecution must prove the existence of certain specific facts before the rebuttable presumption of fact under section 114A may be invoked (*Hansard*, 18 April 2012).

In relation to this, since these two conflicting views were made prior to the coming into force of the new amendment, it is now imperative to critically analyse the provisions of section 114A and to see how they have been interpreted and applied by local courts. Subsection (1) of section 114A states that:

A person whose name, photograph or pseudonym appears on any publication depicting himself as the owner, host, administrator, editor or sub-editor, or who in any manner facilitates to publish or republish the publication is presumed to have published or re-published the contents of the publication unless the contrary is proved.

Plain reading of the subsection seems to presuppose any person as the publisher simply if his name, photograph or pseudonym is portrayed as the owner, host, administrator, editor or sub-editor of the online content. Peters (2012) argued that the provision may implicate Internet intermediaries or any persons who administer, operate or provide online forums or discussion groups. It was further argued that they may possibly be held accountable for the content even if they have no knowledge about it once it is proved that they facilitate its publication. Apart from that, Radhakrishna (2013) alleged that the presumption may affect victims of hacking and identity theft and they would have to bear the evidential burden of proving otherwise.

The application of section 114A (1) has first been invoked in the case of *YB Dato' Hj Husam Hj Musa v Mohd Faisal Rohban Ahmad* (2015). The appellant (plaintiff) sued the respondent (defendant) for publishing articles defamatory of him on a blog '*ruangbicarafaisal.blogspot.com'*. The trial judge found the articles were defamatory of the appellant, but ruled in favour of the respondent on the ground that the appellant failed to establish the respondent as the writer or owner of the blog in question without considering section 114A of the Evidence Act 1950. On appeal, it was ruled that the trial judge had failed to consider the application of the new amendment in cybercrimes as it will assist the appellant to force the respondent to exonerate himself from liability. Since the appellant had successfully linked the respondent to the defamatory posts via the latter's photographs and his letter to other bloggers, the first presumption under section 114A was accordingly invoked. Consequently, the appeal was allowed as the respondent had failed to rebut the presumption and the defence of mere denial was not acceptable as his identity has been established on the balance of probabilities.

Subsection 1 of section 114A has also been referred to in the case of *Ahmad Abd Jalil lwn PP* (2015). The appellant (accused) was convicted for posting offensive comments in Facebook using a pseudonym account of Zul Yahya. The appellant then appealed against his conviction on a number of grounds including that the disputed computer from which the offensive remarks were published on the pseudonym Facebook account of Zul Yahya, though was under his control, could have been accessed by anyone in his office and thus the presumption of publication invoked by the prosecution under section 114A should have failed. Nevertheless, the appeal was dismissed as the High Court found that based on relevant circumstantial evidence and forensic experts presented by the prosecution, the appellant had failed to rebut the presumption on a balance of probabilities.

Based on the aforesaid judgments, it is apparent that the court would only permit the application of presumption of publication by the prosecutor (in criminal cases) or plaintiff (in civil suits) after the existence of relevant facts has been clearly established. Only then, the burden will be shifted to the offender to prove his innocence on a balance of probabilities.

With regard to subsection (2) of section 114A which reads:

A person who is registered with a network service provider as a subscriber of a network service on which any publication

originates from is presumed to be the person who published or re-published the publication unless the contrary is proved.

A scrutiny of subsection (2) demonstrates that a registered subscriber may be regarded as publisher of any content if such content is proved to originate from his registered account. This could affect owners or operators of public places that offer free Wi-Fi services to their customers such as restaurants, cafes and many others. Further, Peters (2012) claimed that registered subscribers with unsecured Wi-Fi services could face problems if their Wi-Fi accounts are used by piggy-back riders to publish illegal content on the Internet.

The presumption of publication in subsection (2) has been discussed in *Tong Seak Kan & Anor v Loke Ah Kin & Anor* (2014). In this case, the plaintiffs sued the first defendant for online defamation and as a result of a judgment in default, damages for the sum of RM 600,000 were awarded to the plaintiffs. The first defendant then applied to set aside the judgment by claiming *inter alia* that he was neither the owner nor the publisher of the two blogs allegedly containing defamatory statements of the plaintiffs. The court found that confirmation by Google Inc. and two local network service providers offered conclusive evidence that the first defendant was the registered subscriber of the two blogs in question. By virtue of section 114A (2) of the Evidence Act 1950, the first defendant as the registered subscriber was presumed to be the publisher of the defamatory publication and consequently, was statutorily required to rebut the presumption by proof to the contrary on the balance of probability. Since the first defendant merely denied ownership of the two blogs without producing any evidence to rebut the presumption of publication under subsection (2) of section 114A, his application to set aside the earlier judgment in default was dismissed by the court.

In the subsequent case of *Dato' Abdul Manaf Abdul Hamid v. Muhammad Sanusi Md Nor and Zulkifli Yahya* (2014), the application of section 114A (2) of the Evidence Act 1950 has again been invoked. The plaintiff sued the defendants for defamatory statements published in a Facebook account bearing the first defendant's name and defamatory articles in a blog *KedahLa.blogspot.com* that were allegedly written by the two defendants. Nonetheless, the civil suit failed as the court observed that the plaintiff did not take any measures to identify the true owner of the disputed Facebook account as well as the actual authors or administrators of the defamatory entries in the blog. As such, it was decided that plaintiff could not rely on the presumption of publication in section 114A (2) as he failed to prove the defendants as the registered subscribers of the social network services.

Apart from the two presumptions in subsections (1) and (2), a further presumption of publication is stipulated in subsection (3) that states:

Any person who has in his custody or control any computer on which any publication originates from is presumed to have published or re-published the contents of the publication unless the contrary is proved.

The potential implication of subsection (3) has been argued by Dazuki (2016) to render parents accountable for illicit content posted on the Internet by their children for the mere fact that the IP address is traced back to their computers. On the same note, it was further submitted that employers might get into trouble for illegal content posted by their employees using the office's Internet and computers. The merit of the argument can be seen in the above-mentioned case of *Ahmad Abd Jalil lwn PP* (2015) whereby the offensive comment was traced to have originated from one of the computers and the Internet facility in the appellant's office. Nonetheless, instead of prosecuting the employer, the prosecution had based on technical experts and forensic evidence successfully identified and then brought criminal action only against the appellant. Finally, the court ruled that it was the computer under the appellant's custody which was used to access the pseudonym Facebook account that posted the offensive remark. Thus, the presumption of publication under subsection (3) of has been successfully invoked by the prosecution against the appellant.

With regard to the presumption in subsection (3) of section 114A, there are a few key words that need to be clearly explained. Firstly, the word 'computer', which has been given the same interpretation in both section 3 of the Evidence Act 1950 and section 2 of the Computer Crimes Act 1997, reads:

An electronic, magnetic, optical, electrochemical, or other data processing device, or a group such interconnected or related devices, performing logical, arithmetic, storage and display functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an automated typewriter or typesetter, or a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility.

It is apparent that the word 'computer' has been statutorily defined in a comprehensive and all-embracing manner so as to include any electronic devices that are capable of performing the four required functions namely logical, arithmetic, storage and display. This would undoubtedly cover smartphones as well since they are able to perform the four stated functions and are currently being widely used to access the Internet and other web-based communication platforms such as Facebook, Twitter, Instagram and many others.

Another important key word is the phrase 'custody or control' which does not synonymously amount to ownership. This can be best illustrated in the case of *Ahmad Abd Jalil lwn PP* (2015) as the disputed computer belonged to the appellant's employer but was put under his control or custody. As a result, the subsection (3) has been successfully invoked against him as it was evidently proved that the offensive comment originated from the computer that was under his control and thus, he was presumed to have published the content since he was unable to prove to the contrary.

IV. Conclusion

To sum up, section 114A of the Evidence Act 1950 has introduced a new presumption of publication that empowers the prosecution or plaintiff in civil proceedings to rely on it in order to prove and attribute the identity of anonymous offender in the cyber world. Regardless of the coming into force of the new provision, it is pertinent to highlight that any person who

wishes to rely on such a presumption must first establish the existence of certain basic facts before the presumption can be invoked. This general principle has been asserted by Abu Bakar Katar JC in the case of *Dato' Abdul Manaf Abdul Hamid* (2014) that only if the plaintiff has successfully proved that the social website was registered under the defendant's name, then the presumption of publication in section 114A of the Evidence Act 1950 may be prayed. On the contrary, the plaintiffs in the earlier case of *Tong Seak Kan* (2014) has established the true identity of the first defendant through a John Doe action against Google Inc. in the US and then obtained confirmation from two local network service providers. Consequently, Abdul Rahman Sebli J allowed the plaintiffs to rely on the presumption of publication and the burden was then shifted to the first defendant to prove his innocence. As such, these two cases have clearly indicated that the presumption of publication in section 114A is not automatic and its application will be determined by the court after considering the facts and circumstances of each case.

Apart from its application, it must be borne in mind that the presumption is rebuttable i.e. the person against whom the presumption is applied to may adduce evidence to rebut it on the balance of probabilities. Mere denials by the defendant as have been shown in *Tong Seak Kan* (2014) and *YB Dato' Hj Husam Hj Musa* (2015) are not acceptable to rebut the statutory presumption on a balance of probability.

Finally, it is submitted that comprehensive analysis of the provision of section 114A of the Evidence Act 1950 and its application by judges in the aforesaid reported cases may be a good basis to concur with Peters (2015) that the new amendment is not oppressive as it sounds. Though some critics are worried and concerned about its implication on freedom of speech and expression, it must always be remembered that the cyberspace does not guarantee absolute freedom as what is illegal offline will also be illegal online. For that reason, Internet users in Malaysia must always be warry of various laws that have been enacted to govern publication of illegal content and they are no longer could hide their identities behind the cloak of anonymity.

ACKNOWLEDGMENT

This research is funded by Universiti Sultan Zainal Abidin through Special Research Grant Scheme (SRGS).

REFERENCES

[1] *Ahmad Abd Jalil lwn. PP* [2015] 5 CLJ 480

[2] Anuar, M. K. (2004). *A historical overview of media development in Malaysia*. Kuala Lumpur, Malaysia : MKini Dotcom Sdn Bhd

[3] Asia-Pacific Network Information Centre. (2004). *The internet in Malaysia*. Retrieved from https://www.apnic.net/__data/assets/pdf_file/0020/27920/apster9-200402.pdf

[4] Azmi, I. M. (2004) Content regulation in Malaysia : unleasing missiles on dangerous web sites. *Journal of Information Law and* Technology, 3, 1-20. Retrieved from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_3/azmi/

[5] Burkell, J. (2006). Anonymity in behavioural research : not being unnamed, but being unknown. *University of Ottawa Law & Technology Journal,* 3:1, 189-203

[6] Centre for Independent Journalism. (2012). *Frequently asked questions on section 114A of the Evidence Act 1950, "presumption of fact in publication"*. Retrieved from https://stop114a.files.wordpress.com/2012/08/stop114a-faq-english.pdf

[7] *Communications and Multimedia Act 1998 (Malaysia)*

[8] *Dato' Abdul Manaf Abdul Hamid v. Muhammad Sanusi Md Nor & Zulkifli Yahya* [2014] 1 LNS 895

[9] Davidson, A. D. (1998). I want my censored MTV : Malaysia's censorship regime collides with the economic realities of the twenty-first century. *Vanderbilt Journal of Transnational Law,* 31, 97-152

[10] Dazuki, A. (2016). No, it wasn't me! *Firasat Newsletter.* Retrieved from http://www.ridzalaw.com.my/downloads/firasat06_NO_IT_WASNT_ME.pdf

[11] *Defamation Act 1957 (Malaysia)*

[12] Department of Statistics Malaysia. (2016). *ICT services and equipment use by individuals, Malaysia.* Retrieved from https://www.dosm.gov.my/v1/index.php?r=column/cthemeByCat&cat=395&bul_id=Q3l3WXJFbG1PNjRwcHZQTVlSR1UrQT09&menu_id=amVoWU54UTl0a21NWmdhMjFMMWcyZz09

[13] *Evidence Act 1950 (Malaysia)*

[14] George, C. (2006). *Contentious journalism and the internet : towards democratic disclosure in Malaysia and Singapore.* Singapore : Singapore Univesity Press

[15] Ismail Nawang, N. (2015). *Political blogs and freedom of expression : a comparative study of Malaysia and the United Kingdom.* (PhD thesis). Retrieved from University of Edinburgh Law Thesis and Dissertation Collection. (1842/10658)

[16] Kim, W. L. (1998). Malaysia : ownership as control. *Development Dialogue,* 2:61, 65-74

[17] Malaysia. *Hansard* House of Representatives. Parliamentary Debates (2012, April 18) (Mohamed Nazri Aziz) Retrieved from http://www.parlimen.gov.my/files/hindex/pdf/DR-18042012.pdf

[18] Mohd Sani, M. A. (2009). *The public sphere and media politics in Malaysia.* Newcastle upon Tyne, UK : Cambridge Scholars Publishing

[19] National IT Council. (2014). *National IT agenda – NITA*. Retrieved from http://nitc.kkmm.gov.my/index.php/national-ict-policies/national-it-agenda-nita

[20] Oxford Dictionaries. (2016). Retrieved from https://en.oxforddictionaries.com/definition/anonymity

[21] Peters, M. (2012). Section 114A … a presumption of guilt?. *Malayan Law Journal,* 6 MLJ ciii, 1-12

[22] Peters, M. (2015). Section 114A … guilty until proved innocent? *LawyerIssue.* Retrieved from http://www.lawyerissue.com/communications-multimedia/

[23] *PP v. Muslim Ahmad* [2013] 5 CLJ 822

[24] *PP v. Rutinin Suhaimin* [2013] 2 CLJ 427

[25] Radhakrishna, G. (2013). Legal presumptions and the burden of proof : s. 114A Evidence (Amendment)(No. 2) Act 2012. *Current Law Journal,* 1 LNS(A) lxxxv, 1-39

[26] Reid, E. (1998). *Malaysia's Multimedia super corridor and roles of information professionals.* Paper presented at the IATUL Conferences, Purdue University, Indiana

[27] Silva, S. G., & Reed, C. (2015). You can't always get what you want : relative anonymity in cyberspace. *SCIPTed,* 12(1), 35-50. Doi:10.2966/scrip.120115.35

[28] Steel, J. (2007). Malaysia's untethered net. *Foreign Policy,* July/August (161), 86-89

[29] Suparmaniam, S. (2012, February 22). Malaysia moves up 19 notches in press freedom. *New Straits Times*, p. 13

[30] Surin, J. A. (2010). Occupying the internet : responding to the shifting power balance. *The Round Table,* 99(407), 195-209. Doi:10.1080/00358531003656388

[31] *The Sun Daily*. (2012, September 18). Section 114A : thorough investigation still required says AG, p. 8

[32] *Tong Seak Kan & Anor v. Loke Ah Kin & Anor* [2014] 6 CLJ 904

[33] Wu, T. H. (2005). *Let a hundred flowers bloom : a Malaysian case study on blogging towards a democratic culture*. Paper presented at the 20th BILETA Conference, Queen's University of Belfast. Retrieved from http://www.bileta.ac.uk/content/files/conference%20papers/2005/Let%20a%20Hundred%20Flowers%20Bloom%20-%20A%20Malaysian%20Case%20Study%20on%20Blogging%20Towards%20a%20Democractic%20Culture.pdf

[34] *YB Dato' Hj Husam Hj Musa v. Mohd Faisal Rohban Ahmad* [2015] 1 CLJ 787

[35] Zimmerman, A. G. (2012). *Online aggression : the influences of anonymity and social modeling* (Masters thesis). Retrieved from University of North Florida Theses and Dissertations. (403)