Cyberlaw on Pornography*

Dr. Sonny Zulhuda
Ahmad Ibrahim Kulliyyah of Laws
International Islamic University Malaysia
sonny@iium.edu.my

=== *Introduction – "pr0n"* ===

Internet is the enabling infrastructure of today's digital society, which sees blurring borders between countries, thus creates an ever dynamic and diverse global community. Just as we start to enjoy this innovative realm called cyberspace, we are confronted by a myriad of questions that challenge the more established values that we have had adopted in "real" space defined by conventional social borders of politics, cultures and religions. One of those challenges lingers around the question of how much we would compromise the cyberspace – our cyberspace– to be the place for harvesting porn and obscenity.

"Pornography" may not be "obscene", at least according to the United States legal lexicon. The Black's Law Dictionary (10th Edition, Bryan A. Garner, 2014) defines *pornography* as material (such as writing, photography, or movies) depicting sexual activity or erotic behaviour in a way that is designed to arouse sexual excitement. In the U.S., pornography is protected speech under the First Amendment unless it is determined to be legally *obscene*. Meanwhile *obscenity* the quality, state, or condition of being morally abhorrent or socially taboo, esp. as a result of referring to or depicting sexual or excretory functions. So something is *obscene* if it is "extremely offensive under contemporary community standards of morality and decency; grossly repugnant to the generally accepted notions of what is appropriate." However it is to be noted that *indecency* – the quality, state or condition of being outrageously offensive, esp. in a vulgar or sexual way – is not illegal in the U.S. and it is protected under the First Amendment. By virtue of the Supreme Court's decision in *Miller v California* 413 U.S. 15, 93 S.Ct. 2607 (1973), courts will revert to a three-part test to find out if a material is legally obscene – and therefore not protected under the First Amendment. The test is to see if, taken as a whole, the material (1) Appeals to the prurient interest in sex, as determined by the average person applying contemporary community standards; (2) Portrays sexual conduct, as specifically defined by the applicable state law, in a patently offensive way; and (3) Lacks serious literary, artistic, political, or scientific value.

* Presented at the National Law Students Conference 2015 (PEMUDA IV) at the Universiti Utara Malaysia, Sintok, Kedah, 2nd of October 2015.

This American constitutional protection and "contemporary community standard" is what the law in the U.S. has been shaped in relation to pornography and obscenity. Thus, only when it is obscene, a material will be illegal. Porn itself is legal and constitutionally protected. This is certainly not always the case in other countries. In the U.K., porn may fall under certain categories, including child porn, indecent photograph of children, obscene material and extreme pornography. According to the U.K. Obscene Publications Act 1959, an article "shall be deemed to be obscene if its effect… if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it." This includes any description of article containing or embodying matter to be read or looked at or both, any sound record, and any film or other record of a picture or pictures.

In the Malaysian law, the law is supposedly less complicated because any types of obscene materials (not specifically child materials) are outlawed. As Juriah Abdul Jalil (2015) elucidates in her latest work concerning online child pornography, "Malaysia regards all pornography as illegal and thus does not have any specific law criminalising child pornography." On the legal landscape of obscenity law, she had this to say:

> "The laws are scattered and govern all types of pornography under the category of obscene, indecent and offensive materials. The Printing Presses and Publications Act 1998 (PPPA), the Film Censorship Act 2002 (FCA) and Penal Code clearly prohibit obscene and offensive materials in relation to print medium and film, whereas indecent, obscene and offensive online contents are governed by the Communication and Multimedia Act 1998 (CMA) and Content Code (CC)."

Of all the above laws, Content Code is the only one which is not an Act of Parliament. It is a form of industry's self regulatory instruments institution of which is mandated by the Communications and Multimedia Act 1998. While adopting it is voluntary, such adoption may work as an evidence for the industry player that they reach certain level of compliance. Interestingly, the Content Code is the only one instrument that comes with a relatively clear definition of obscenity. Thus *obscene content* has been described in Item 3.0 Part 2 of the Content Code as "content that gives rise to a feeling of disgust because of its lewd portrayal and is essentially offensive to one's prevailing notion of decency and modesty." The test of obscenity is whether the content has the tendency to deprave and corrupt those whose minds are open to such communication. Among the classes of content that falls within this category are: (i) explicit sex acts/pornography, (ii) child pornography, and (iii) sexual degradation

(More on the commentary on the offensive content under the Code, read *Ida Madieha Abd. Ghani Azmi, 2004*).

Creation, possession or otherwise distribution of obscenity has often been dubbed as falling under "victimless crime". It is defined as "a crime that is considered to have no direct victim, usually because only consenting adults are involved, such as the possession of illicit drugs and deviant sexual intercourse between consenting adults" (Black's Law Dictionary, 2014).

In describing the uniqueness and complexity of a "victimless crime," Lon L. Fuller in his work "Anatomy of the Law" (1968) said that "when a man's house has been robbed or his brother murdered, he is likely to take this complaint vigorously to the police and demand action. His presence on the scene dramatizes the need for law enforcement and gives sense and purpose to the work of the police and district attorney. In contrast, the absence of a prosecuting witness surrounds 'crime without victims' with an entirely different atmosphere. Here it is the police who must assume the initiative. If the attempt to work without the aid of informers, they must resort to spying, and this spying is rendered all the more distasteful because what is spied upon is sordid and pitiable."

Is it accurate and safe to see pornography as a "victimless crime"? I doubt that. As we shall see in the passages to come, porn is clearly a social ill that has far-reaching implications not only to the person involved in the porn making and consuming, but more harmfully to the people living around him. In line with this notion, one can see that porn-related provision in the Malaysian Penal Code is placed under Chapter Nine which is titled "Offences affecting the public health, safety, convenience, decency and morals." Porn is indeed about a public ills to decency and morality which leads to the jeopardy of social structure such as family, friendship and community.

=== *The Cyberspace Today* ===

The question above, (how much we would compromise the cyberspace to be the place for harvesting porn and obscenity) is becoming relevant again today where the Internet has further developed as a powerful virtual space with over three billion global users actively using the Internet for personal and professional communications and publication (*Internet Society Global Internet Report 2015*). The Internet today is not only a space to consume

information, but has become a sharing platform for everyone to give and take, to read and write, and, using the jargons in Twitter, to follow and be followed.

Three inter-related powers that made the Internet it is today are: Connectivity, mobility, and abundance of data. People are having high-quality connectivity nowadays due to the growth of Internet broadband. There are 3 billion Internet users worldwide and counting. The possibility of being connected to the Internet from anywhere at anytime is now increasingly a common demand by many. Hotels, restaurants, cafes, gymnasium, buses or even laundry halls are now making the wireless connectivity as a competitive factor in their business. The ultimate idea is to ensure everyone is connected at all time.

The second element is mobility. Internet connectivity has now been further empowered by the rise of mobile devices in the form of smart phones and tablets. Even laptops are being increasingly outdated, and starting to become like a desktop. Suffice to say that the majority of new Internet users today are mobile users (*Internet Society Report 2015*). The high rise of mobile devices and mobile users is owing to the parallel development of mobile application software ("apps"). Innovations keep coming one after another: there is an app for a traveler, a student, a mathematician, a food lover, a lawyer, a gym-goer and so on. It is now quite hard to imagine doing an activity without thinking there is an app available to help people in it.

A high connectivity empowered by mobility and advanced mobile application innovations has led to "datafication" of everything. Datafication is, in the words of Meyer-Schonberger & Cukier (2013), the process of quantifying all information around us which will allow us to use such information in new ways, such as in predictive analysis. This will help us further to unlock the implicit, latent value of the information.

People's chat, daily activities, travels, meetings, preferences, friendships, even thoughts are now reduced to bits of data including texts, graphs and images. Mood is now stored, curiosity measured and fashion forecast using posts people upload on social networking sites. The multiplicity of devices people use is now solved with data synchronization tools. Sensors and cameras on mobile phones are kept busy to capture movement, events, "selfies" and emotion and store them on the devices. Not to worry with the overcrowded device storage, people now use external servers, a.k.a. *cloud*, readily available to "help" accommodate the storing of such data. In short, it is the Big Data, the data which is now over-abundant.

All the three features above: connectivity, mobility and abundance of data have reshaped the Internet today. After appreciating the exponential growth of the Internet today, the Internet Society's Global Report further summarizes the primary problems we encounter in this cyberspace today:

> "Smart devices enable services such as location awareness and include features such as cameras; the flip side of the coin is increased privacy issues. [Meanwhile] Usage of the mobile Internet depends on a number of wireless interfaces and access to apps; these lead to heightened security issues."

Indeed, threats to privacy and security remain the Internet major boogeyman. The revelations made by former U.S. National Service Agency's contractor Edward Snowden in mid-2013 has opened our eyes on how fragile our privacy is on the Internet. More so, this threat has come directly from one of the most powerful authority on earth in a country where the global Internet industry had initially and predominantly develops. As Prof Deibert (2013) puts it, it is from his revelation that we now know that "the U.S. government had required big Internet industries such as Google, Yahoo!, Facebook and Apple to facilitate direct access to customer data managed by the companies and compelled the companies to remain silent about these arrangements under penalty of law."

So now we start to see the less bright side of the Internet. As for the security issue, each of the connectivity, mobility and abundance of data has contributed to several (unintended) consequences surrounding the use of the Internet. For example, the more and the easier people are connected to the speedy Internet, the more they will tend to share data or documents, and the more they will be sharing materials including copyright-infringing materials including songs and films. Besides, the fact that our youth can take the Internet in their mobile devices to their solitude will unlock their curiosity and possible expose themselves to harmful materials. This is in line with the old notion framed by a social norm that porn corrupts people. Therefore it is better if watching or accessing porn is done in the solitude of the Internet user, hence the mobility effect.

Finally, the proliferation of big data means you can access almost any kinds of data at anytime and from anywhere. The data storage in the cloud is storing all those information without fail. The law may try to intervene that by restricting the period of time such data may be stored by data users. Nevertheless, that does not necessarily mean that such data will go away from the cyberspace. Often we feel shock and embarrassment if we find out that our old photos or CVs are still online somewhere in the Internet. What more if that data portrays an

image of you that you do not wish to be. Indeed, Mayer-Schonberger (2009) rightly pointed out about the virtue of deleting old memories. In this context, people feel the urge to have their old and unused data being deleted from the memory of the Internet. They want a right to be forgotten!

=== *The pr0n in Cyberspace* ===

The increasing connectivity and mobility empowered with big data and cloud technology has unsurprisingly made today's Internet a very efficient media to spread porn and obscene materials. Indeed, it is not all surprising. Because it is not the fact that porn will mushroom on the Internet – as it did through innovations in the past such as printing machines, camera technology, video as well as broadcasting technology – that really worries us, but the extent to which porn transforms and develops is truly shocking.

Let us do some reality check. Covenant Eyes, a U.S. Internet filtering company, in their 2015 Annual Pornography Statistics reported that, even though the size of the adult industry is difficult to determine because most of the industry is privately owned and there are no agreed-upon definitions for what consists of an "adult" service, some findings on the statistics related to pornography and online porn were at least staggering (See, http://www.covenanteyes.com/pornstats/). Here are some of the findings citing various sources:

- In 2006, the sex-related entertainment business' estimated revenues were just under $13 billion in the U.S. These estimates included video sales and rentals, Internet sales, cable, pay-per-view, phone sex, exotic dance clubs, magazines, and novelty stores. In 2007, global porn revenues were estimated at $20 billion, with $10 billion in the U.S.
- In 2005 pornography accounted for 69% of the total pay-per-view Internet content market, outpacing news, sports, and video games.
- From 2001 to 2007, Internet porn went from a $1-billion-a-year industry to $3-billion-a-year in the U.S.
- In 2006, revenue from online subscriptions and sales was $2.8 billion, up from $2.5 billion in 2005, according to estimates from Adult Video Network.

That is staggering. However, due to the connectivity, mobility and abundance of data, we are witnessing the decline of revenue of online porn industry because the porn goes *free of charge*. The Covenant Eyes has the following figures to describe that:

- Global porn revenues have declined 50% since 2007 due to the amount of free porn online. 9 out of 10 Internet porn users only access free material, whether it be samples of pay material, illegally copied versions of pay material, or amateur material.
- Today, one in eight online searches is for pornography. The number of searches for pornography since the start of 2015 until the eve of the present Conference (end of September) surpasses 1.6 billion searches.
- Meanwhile, 1 in 5 mobile searches are for pornography. 24% of smart-phone owners admit to having pornographic material on their mobile handset.
- In 2009, the Media Research Center (MRC) examined the most popular YouTube searches for the word "porn," yielding 330,000 results. The study reported on the top 157 videos, all with one million views or more.
- In 2010, out of the 1 million most trafficked websites in the world, 42,337 are sex-related sites.

Those are the global figures or those from other countries backyard. In Malaysia, we hear similar concerns too. Among the loudest came from none other than the architect of Malaysian modernity Tun Dr. Mahathir Mohammad when he said in his blog ("Censoring the Internet" at http://chedet.cc/?p=1431):

> "The internet has played a major role in undermining public morality. Our children are not safe from the kind of filth that the print and electronic media promote. Today any child can access pornography of the worse kind. Children are no longer safe from sexual assault. So are young girls and boys as the internet arouses the kind of base feelings that we curbed before…. Incest, child sex, sex with animals, sexual parties, sex in public and many other practices which we still feel are wrong will soon be a part of the expression of freedom and equality. All these will be promoted on the internet."

Perhaps, the only inaccuracy Tun Mahathir has had in his note was not that such social illnesses *will be* promoted on the Internet, as they are and they have been! Then it would be of our benefit to do some reality check at our own home yard.

Malaysia is few steps away from achieving its long-envisioned developed status by year 2020. The development of digital industry already shows that potential achievement. Based on the statistics issued by the Malaysian Communications and Multimedia Commission (MCMC) in its Communications and Multimedia Pocket Book of Statistics Q1 2015, one realizes that the Internet broadband penetration to more that 30 million population of Malaysia is truly high. One third of the whole population is now online with Internet broadband, while 70.4% of the household in Malaysia has also had the connection – an

impressive level of connectivity competed only by Singapore in this ASEAN region. In term of mobility, there is 146.2% mobile penetration rate in Malaysia, which means almost half of the population has two mobile subscriptions on average (They had sent 49,290,700,000 (49 billion) smses in 2014!). Supported by over 30,000 hotspot locations throughout all the states in Malaysia, Malaysian population has gone not only online, but also mobile.

In terms of the users, 15.5% of the Malaysian Internet users are under 20; while 56.6% are between 20-35 years old. A total of 72% of the users are categorically youth, and most of them may as well qualify as "digital natives." A term used by Harvard law professors to those new generations whose life has been predominantly "digitised" (See, John Palfrey and Urs Gasser, 2008).

On the related issues to Internet users in Malaysia can be derived from the following statistics:

- The report that came from the 2014 UNICEF's Digital Landscape in Malaysia (http://www.unicef.org/malaysia/UNICEF_Digital_Landscape_in_Malaysia) sthat Malaysia ranks top 15 countries with the highest Facebook penetration at 82.3% in 2013 behind Philippines (92%) and Thailand (89%). Over 90% visited social networking sites, while children and young people (13–24) make up half of Facebook users, who would use up to 1/3 of PC 'screen time' for social networking.
- Norton 2013 Online Family Report describes that 82% of children who breached Internet general rules experienced negative moments online; 6% of parents did not know of their children's activities online; 12% of children surfed porn website when parents not around.
- CyberSAFE Report (2014) showed that 83% of Malaysian Internet users do not take action to protect, while 40% do not know how to protect. Two thirds of the users (below 13 yrs) take low protection but 52% think they are safe. Furthermore, 64% Internet users feel that sending improper SMS-es, posting inappropriate photos, and pretending to be someone else is not cyber-bullying.
  Source: https://digi.cybersafe.my/CyberSAFE_Survey_Report_2014.

Much has been said about the impact of pornography which this paper does not intend to elaborate. Dolf Zillmann in his research published in the Journal of Adolescent Health in August 2000 ("Influence of unrestrained access to erotica on adolescents' and young adults'

dispositions toward sexuality," Journal of Adolescent Health 27 (Aug. 2000): 41-44.), explained that a prolonged exposure to pornography leads to:

- An exaggerated perception of sexual activity in society
- Diminished trust between intimate couples
- The abandonment of the hope of sexual monogamy
- Belief that promiscuity is the natural state
- Belief that abstinence and sexual inactivity are unhealthy
- Cynicism about love or the need for affection between sexual partners
- Belief that marriage is sexually confining
- Lack of attraction to family and child-raising

The impacts are certainly frightening. In order to avoid these problematic situations, governments must take action to prevent and address properly the issue of distribution and usage of pornography in our society. The recent incidents involving Malaysian students abroad who are implicated in the offence of obscenity should be a wake-up call for us (See: cases involving *Nur Fitri Azmeer Nordin* and *Jan Eave Jeremy Wan*, as examples).

Just because the pornography is everywhere in the cyberspace, does not mean we should condone it. This has even got a judicial notice when Datuk David Wong Dak Wah J. of the High Court (Kota Kinabalu) in the case of *Public Prosecutor v Zainuddin bin Adam* [2012] MLJU 684 commented that:

> "…in this day and age of internet where with free flow of information from cyber space, young people are exposed to things which the older generation could not have imagined. Such exposure had no doubt also made the art of parenthood that much more difficult in dealing with such social issues. In some cases, it had made it impossible. The value of society changes as each year passes by and because of such change, it of course has made the job of Court that much more difficult especially on such issues…"

=== *Cyberlaw on Pornography* ===

If this is the first time you hear about "cyberlaw," the chance is you may have some misconception on its nature. The dictionary says cyberlaw is **t**he field of law dealing with the Internet, encompassing cases, statutes, regulations, and disputes that affect people and businesses interacting through computers. Nevertheless, there two big misconceptions about cyberlaw – one is about *what it is* and the other is about *how it is*.

Cyberlaw is a new class of law. Wrong. Cyberlaw may not totally be a new law. Some statutes of cyberlaw may never use technical terminology as such, and may not even name computer network as its object of regulation. A cyberlaw may have been enacted decades before the proliferation of the ubiquitous Internet. In fact, cyberlaw covers the mix of laws dealing with both traditional non-technological law and laws which respond specifically to a technology or innovation. In Malaysia, the former includes Penal Code, Defamation Act, Seditions Act, Copyrights Act and Anti Money-Laundering Act. These are the "old-time" acts which are being extended to cover incidents using or taking place in the Internet. On the other hand, falling under the second category of cyberlaw is, among others, the Computer Crimes Act, Communications & Multimedia Act, Electronic Commerce Act as well as Personal Data Protection Act.

Jay Dratler Jr. (2001) neatly summarized that "much of the hoopla about cyberspace law relates more to climbing the steep learning curve of the Internet's technological complexities than to changes in fundamental legal principles. To the extent there was 'new' law, it was almost entirely case-by-case development, in accordance with the accepted and well-understood basic legal principles, albeit applied to new technology and new circumstances.

Secondly, cyberlaw alone can curb crime in the Internet. *Wrong*. At least, not on its own, and not in exclusivity from other components significantly important for regulating the Internet. This is the "shared responsibility" that needs contribution from each and everyone (Brenner, 2005). The discussion about this shared responsibility will be made at a later part of this paper. So, cyberlaw has limitations. But, as Lessig (2006) reckons, the law does not have to be perfect. It is sufficient that the law is generally effective and is further subject to improvement. So in regulating pornography, we would do a quick survey on the laws that deal with the use or involvement of computer or computer system for pornography.

In the short-span history of the modern Internet, question of cyberspace porn is not new. Back in 1997, the United States Supreme Court in the case of *Reno v. American Civil Liberties Union (ACLU)*, 521 U.S. 844 (1997) had to decide whether or not contested provisions in the newly-enacted Communications Decency Act (DCA) –meant to outlaw child pornography in the Internet– were unconstitutional for violating the First Amendment's guarantee of freedom of speech. The judgment, the first major ruling in the U.S. court on Internet obscenity issue, was given in favor of the applicant. The Court maintained that the

restriction imposed in the provision was effectively operating as a sweeping restrictions to materials which otherwise would be legal for adult Internet users (yes, pornography, instead of obscenity, is an expression protected under the U.S. fundamental liberties).

Interestingly, at the same time some fifteen thousands kilometers away, Malaysian legislatives and executives took up some task declaring the freedom of the Internet in Malaysia, quashing away the issue of censorship of the Internet. In the Bill of Guarantee in 1996, the Government pledged that there will be no censorship of the Internet. Meanwhile the Malaysian parliament had promulgated in the Communications and Multimedia Act 1997 that nothing in the newly-passed Act that would permit the censorship of the Internet.

The CMA 1998 went further to make it an offence under section 211 of the Act for anyone who provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person. Similarly, in section 233 it made an offence for anyone who by means of any network facilities or network service or applications service knowingly— (i) makes, creates or solicits; and (ii) initiates the transmission of, any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive, in character with intent to annoy, abuse, threaten or harass another person. Is this restriction (in sections 211 and 233 of CMA), constituting an Internet censorship? The answer depends on how one defines a censorship. If it is meant to be any method to curtail the access to the Internet, then the provisions are not censorship. But if a liberal view is considered, that censorship is any method to regulate the content, then the answer is positive.

Given the above, the CMA had been used by courts in several cases. In *Rutinin bin Suhaimin v Public Prosecutor* [2014] 5 MLJ 282, the prosecution's case was based on an entry of a comment ridiculing the Sultan of Perak via the internet protocol account (or 'the internet account') of the appellant on the stated date, time and place. The defence of the appellant was that he did not make and initiate the transmission of the impugned entry despite the fact that his internet account was used. The Court said that it appeared that the trial judge had shifted the onus of proof to the appellants while there was no presumption in s 233(1)(a) for the appellant to rebut. The onus remained with the prosecution to establish beyond reasonable doubt that it was the appellant who made and initiated the transmission of the impugned entry. In this case the court finally acquitted the appellant.

This case, though is not concerning a pornography, is yet beneficial to show the mechanism of section 233 of CMA 1998. The court held that:

> "this provision is worded widely. The initiation of network usage need not be continuous. Therefore, a single instance of network usage would suffice. Communication need not necessarily ensue in the process. This means that a solitary posting of remark on a website which did not elicit a reply is caught by this provision. It is also not relevant whether the accused had revealed his identity or otherwise during resession when the communication in question was made. The crucial ingredient of this offence is as follows: (a) That the accused person had made the communication in question through a network facility; and (b) The communication was made with "with intent to annoy, abuse, threaten or harass any person."

Still on the CMA 1998, one may have to read also section 263 of the Act, which is under the heading of "General duty of licensees". It provides that "a licensee shall, upon written request by the Commission or any other authority, assist the Commission or other authority as far as reasonably necessary in preventing the commission or attempted commission of an offence under any written law of Malaysia or otherwise in enforcing the laws of Malaysia, including, but not limited to, the protection of the public revenue and preservation of national security." What it simply means, the Internet service licensees in Malaysia such as the ISP's can take certain measures to ensure a crime is being prevented. That, in practice, has been interpreted by the Government as a license to block access to certain materials in the Internet on the ground of protecting public revenue or preserving national security.

Now let me turn my attention to the Penal Code, i.e. section 292 which prohibits the sale, etc of obscene materials. Section 292 makes it an offence for anyone who "sells, lets to hire, distributes, publicly exhibits or in any manner puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation makes, produces or has in his possession any obscene book, pamphlet, paper, drawing, painting, representation or figure or any other obscene object whatsoever."

This offence is not strict. It must be proven that such act of sale, hire etc. must be intended for the purposes mentioned above. This makes a mere possession of obscene materials a non offence. Juriah (2015) explained how this provision was put in court cases. In 2010, *Shahrom Mahdi* a security guard was charged under section 292 of the Penal Code for uploading pornographic pictures and disseminating them on six websites. He pleaded guilty to the charges and was convicted. In 2013, *Fila Syahida Zulkipli* was charged under the same provision by the Mukah Magistrates Court. She pleaded guilty to recording an obscene video

of a 15-year-old girl using her mobile phone and was fined for producing the obscene video. Indeed, an obscenity is rejected in Malaysian legal norm. At most, a distribution of obscene material will land a perpetrator guilty in crime. At the least, the action will be a fair and reasonable ground for taking disciplinary action at workplace including outright dismissal (See: *Low Tiam Seng v Panasonic Electronic Devices Malaysia Sdn Bhd & Anor* [2012] MLJU 452).

Has s.114A Evidence Act been helpful? A closer look is required to examine how much this amendment to the Evidence Act is helpful to curb online porn. My theory is it is vey helpful. Except that the court should always be cautious in shifting the presumption of guilt that is to the accused. The effectiveness of this amendment can be seen in the case of *YB Dato' Hj Husam bin Hj Musa v Mohd Faisal bin Rohban Ahmad* [2015] 3 MLJ 364, where the court upheld the intention of the Parliament in introducing section 114A of the Evidence Act 1950 as argued by the Appellant in this case (who was a victim of defamation by the respondent blogger):

> The appellant complains that the provision of s 114A of the EA 1950 was not considered by the learned judge. On this point, learned counsel for the appellant says: 'In passing the bill, Parliament acknowledged the parameters of proof being on a balance of probability but much lower than the criminal standard required in establishing identity calling in aid the following presumptions. They were as follows:
>
> (1) If the name, photograph or pseudonym appeared in a publication, depicting said person to have some connection with the publication, said person was presumed to have published or re-published the contents of the publication; (2) If a publication originates from a network service that a person has registered, said person is presumed to have published or re-published the contents of the publication; or (3) If a publication originates from a computer which a person has custody or control of, said person is presumed to have published or re-published the contents of the publication.' The defendant in this case has also failed to rebut the presumption under s 114A of the EA 1950 and the defence of mere denial is not acceptable on the facts of the case as identity has been established on the balance of probabilities; and in defamation suit it need not be on beyond reasonable doubt.

It is argued that this shifting of presumption of guilt for online information will be helpful in addressing the illicit distribution, publication or transfer of obscene material on the Internet. Yet, taken as a whole, we do need to contemplate on short-term and long-term strategies to achieve better objective of curbing social ills named pornography.

=== Way Forward ===

The preceding pages had showed us all the context and law that we currently have or see. What is next is to embrace the trend and get prepared with the challenges and improvement. There are few lessons we would like to bring forward here:

Firstly, law (i.e. cyberlaw) does not work in solitary mechanism. Indeed, law has never regulated our life without the support given by other factors. Lessig (2006) summarised four things that regulate the Internet, just the same way they regulate other object in real life: Law, Norm, Market and Architecture. Just as the porn in real life is regulated by those four modalities, online porn will be similarly regulated. Each of the law, norm, market and architecture surrounding the creation and distribution of porn online will have to be cautiously observed and studied so as to co-regulate the online porn. In other words, while we can maintain certain legislative or administrative laws prohibiting porn (because that is just what our social norm demands); we should make it more difficult or costly for users to access online porn. And this is, as Lessig reckons, where the difficulty lies (because porn is freely available online). We should be looking at certain mechanism which has to be supported not only by Government of the day, but also by industries surrounding the provision of Internet (ISP's, Internet companies – software and hardware). Among those alternative mechanisms would be "zoning regime" and "filtering regime".

Secondly, Malaysia must actively participate in the international sphere to forge international commitment to curb porn and other cybercrimes. There are some international intitiatives that Malaysia can consider either to accede or just to adopt the principles. On cybercrime initiative, one can look up at the Budapest Cybercrime Convention 2001 which provides for criminalization of online child pornography while forging international cooperation in addressing the cybercrimes. Meanwhile, it is noteworthy that Malaysia has signed for the United Nations Convention on Transnational Organized Crime (UNCTO) which potentially extend its scope to emerging crimes including cybercrime as part of the transnational organized crimes. More actions should be pursued at the regional level such ASEAN.

Susan Brenner and Clarke (2005) campaigned for a "distributed security" which also means shared responsibility on dealing with cybercrimes challenges. Not only the law enforcement will have the role to play, others in the society will need to play their role to ensure the enforcement of cybercrimes law is effective. In the context of Malaysia, we should not leave

everything to the Police, MCMC or Cybersecurity to deal with cybercrimes issues. More can be done in more preventive way by all members of society including:

- Internet Service Providers (ISPs) in helping users to identify harmful sites either for minors or otherwise; they can also help by strengthening the self-regulatory mechanism in the form of Content Forum and Consumer Forum under the supervision of the MCMC.
- Corporation administrators in workplaces and organizations by putting in place proper standard acceptable practices online (and monitoring its compliance) to be complied by all members of the organizations. This idea has been put forward by legislature in the introduction of the Personal Data Protection Act 2010 which places some duties to those who are responsible to persona data management in organisations.
- Schools by educating their users and introducing a safe Internet behaviour. We note that the Malaysian Ministry of Education has in the past four years introduced the innovative training program aimed at educating students and youths on the Internet literacy skills.
- Cybercafes (publicly accessible Internet stations) by ensuring that appropriate technical measures are taken to avoid unbecoming behaviour of their Internet users. It is noted here that some States government such as Selangor, Federal Territory and Sarawak have had in place some orders or by-laws requiring cyber centers to identify the users of their Internet accounts (See, for examples: *Cyber Centre and Cyber Café (Selayang Municipal Council) By-Laws 2007*; and *Cyber Centre and Cyber Café (Federal Territory of Kuala Lumpur) Rules 2012*) This is important to prevent anonymous users misuse the Internet for illicit activities.
- Parents and family by educating their children on positive use of the Internet. Parents should differentiate privacy from alienation. The former is a right while the other is a social illness leading to harmful and illicit use of the Internet. Parents need always to accompany the children and get in the know about their Children online activities, the same way as they get in the know about their offline friends, school activities and things they watch, read and chat about.
- Younger generation (a.k.a Digital Natives). They need to be more cautious and to understand few concepts that had naturally lapsed from their view: about the border between public and private space, about norms, about friendship, etc. They are soon becoming the majority of the Internet sphere. As they will hold offices, authority, professions, etc. they will be the one putting colours to the Internet in near future.

Indeed, we will never get enough with this scope of "distributed security" and "shared responsibility" because the list can go on and on. Nevertheless, we should carry on the spirit.

Last but not least, we can say that Internet is far from over. We will not know what it takes us in the future. Already the current trend of connectivity, mobility and big data amazed us with what the Internet has enabled us and empowered businesses (e.g. Uber and BitCoin). Therefore we can also say that the challenges to the society from the dark side of the Internet are far from over. What we are required to do is simple: stay focused and united as a society. Pornography is a socially-identified pathology, and we should never walk alone in addressing this.

Bibliography

Brenner, S.W. & Clarke, L.L. (2005). Distributed security: Preventing cybercrime. *The John Marshall Journal of Computer & Information Law*, 23 J. Marshall J. Computer & Info. L., 659.

Bryan A. Garner (2014). *Black's Law Dictionary*. 10th Edition, Thomson West, USA.

Ida Madieha Azmi (2004) Content Regulation in Malaysia: Unleashing Missiles on Dangerous Web Sites. *Journal of Information Law & Technology,* 2004 (3).

Internet Society (2015). *Global Internet Report 2015.*

Jay Dratler Jr. (2001). *Cyberlaw*, 2001: 1-3.

John Palfrey & Urs Gasser (2008). *Born Digital: Understanding the First Generation of Digital Natives*, Basic Books.

Juriah Abd. Jalil (2015). Combating Child Pornography in Digital Era: Is Malaysian Law Adequate to Meet the Digital Challenge? *Pertanika Journal of Social Sciences and Humanities.* 23 (S): 137-152.

Lawrence Lessig (2006). *Code and other laws of cyberspace — Version 2.0*. New York: Basic Books.

Mayer-Schonberger V. & Cukier K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work and Think*. London: John Murray.

Mayer-Schonberger V. (2009) *Delete – The Virtue of Forgetting in the Digital Age*, Princeton/Oxford: Princeton University Press.

Ronald J. Deibert (2013). *Black Code – Surveillance, Privacy and the Dark Side of the Internet*. Toronto: McClelland & Stewart.

Case Laws

Low Tiam Seng v Panasonic Electronic Devices Malaysia Sdn Bhd & Anor [2012] MLJU 452

Miller v California 413 U.S. 15, 93 S.Ct. 2607 (1973)

Public Prosecutor v Zainuddin bin Adam [2012] MLJU 684

Rutinin bin Suhaimin v Public Prosecutor [2014] 5 MLJ 282

YB Dato' Hj Husam bin Hj Musa v Mohd Faisal bin Rohban Ahmad [2015] 3 MLJ 364

Internet Reports

"Imperial College London Student Jailed For 30,000 Child Abuse Images." *The Huffington Post UK*, Posted: 09/05/2015. http://www.huffingtonpost.co.uk/2015/05/09/nur-fitri-azmeer-nordin_n_7247098.html

"Malaysian student sentenced in Perth for importing child pornography." *Department of Immigration and Border Protection*, 11-10-2012. http://newsroom.border.gov.au/releases/Malaysian-student-sentenced-in-Perth-for-importing-child-pornography-11-October

CyberSAFE (2014) Cybersafe Survey Report 2014. https://digi.cybersafe.my/CyberSAFE_Survey_Report_2014.

Internet Society (2015). *Global Internet Report 2015*

Malaysian Communications and Multimedia Commission (2015). *Communications and Multimedia Pocket Book of Statistics Q1 2015*

UNICEF (2014) Digital Landscape in Malaysia. http://www.unicef.org/malaysia/UNICEF_Digital_Landscape_in_Malaysia