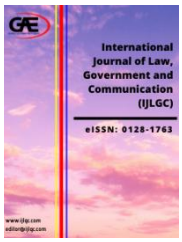
International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 5 Issue 20 (September 2020) PP. 80-86
DOI 10.35631/IJLGC.520005



INTERNATIONAL JOURNAL OF LAW, GOVERNMENT AND COMMUNICATION (IJLGC)
www.ijlgc.com

LEGAL CHALLENGES OF ADOPTING AGE-VERIFICATION TECHNIQUES FOR THE PROTECTION OF MINORS ON THE INTERNET IN MALAYSIA

Manique Cooray[1]

[1] Faculty of Law, Multimedia University, Melaka, Malaysia
Email: manique.cooray@mmu.edu.my
Tel: (606) 2523991
[*] Corresponding Author

Article Info:

Article history:
Received date: 01.08.2020
Revised date: 18.08.2020
Accepted date: 04.09.2020
Published date: 15.09.2020

To cite this document:

Cooray, M. (2020). Legal Challenges of Adopting Age-Verification Techniques for The Protection of Minors on The Internet in Malaysia. International Journal of Law, Government and Communication, 5 (20), 80-86.

DOI: 10.35631/IJLGC.520005.

Abstract:

Corporations in the form of Limited Liability Companies in Indonesia are regulated in Limited Liability Company Law No. 40 of 2007 concerning Limited Liability Companies, this Law regulates the liability of corporations and/or shareholders who commit acts against the law, but the liability that can be asked of shareholders does not exceed existing shares. This study uses normative legal research methods. The data used are secondary data consisting of primary legal materials, secondary legal materials, and tertiary legal materials. For data analysis, the qualitative jurisdictional analysis method was used. From this research, it can be found that law enforcement against shareholders who commit acts against the law can be upheld and the outcome is that the action against the law which was originally a civil action and then turned into a criminal act. By using the Piercing, the corporate veil doctrine, shareholders who commit acts against the law can be sentenced to criminal and all their assets to cover the financial losses of the state due to their actions. It is universally applied on the basis of fraudulent acts carried out to rake in personal profit and by implementing civil forfeiture or civil recovery, the proceeds of crimes committed by shareholders are likely to be returned.

Keywords:

Age- Verification; Internet Regulation; Online Harmful Material

Introduction

There is clearly an important difference between children particularly younger children inadvertently stumbling across pornographic and obscene content online, and young people who deliberately seek it out intensifying debate over sexualized content online and its

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 5 Issue 20 (September 2020) PP. 80-86
DOI 10.35631/IJLGC.520005

consumption by children and youth.[1] Whichever method it is, it is widely accepted that young children may not have the mental capacity to determine the appropriateness or the suitability of viewing pornographic and obscene material online.[2] It is quite clear that the landscape of online sexual content has changed and will continue to change with the development of technology.[3]

Since this paper is mainly focusing on pornographic and obscene matter it is necessary to look into definition and interpretations of these key terms. From the late twentieth century there has been a proliferation of sexual imagery in the media and children now move in a '"hyper-mediated" environment in which pictures and words have unprecedented cultural influence. Thousands of such sites exist on the Internet and can be accessed with very basic search criteria. While there are measures in place in countries such as Australia, to prevent under 18 year olds from viewing X-rated video content, no such measures exists in Malaysia for the simple reason that the Internet regulation in Malaysia is more or less in the form of self-regulation, where by individuals are required to take the necessary measures to prevent minors from accessing such content. Young people are more able to engage with pornography than ever before, both by choice and inadvertently. Many pop-ups, "mousetrapping" spam, manipulated web addresses and search engines give young people access to a profusion of images, many of them graphic and are part of an aggressive marketing approach by the industry. A child can type in sexual words into a search engine and literally millions of sites will appear. They then have free access to pornography which is not limited through age-related barriers and at times access to live web chatting. Three quarters of commercial pornographic websites display explicit content on their first page. Most allow viewers a "free preview" with graphic images and film material. This has given rise to large-scale studies in the United States, Holland and other European countries, Australia, Taiwan and elsewhere to look into the problem. Studies from Australia, Cambodia, Canada, Denmark and Norway, Italy, Iceland, Sweden and Taiwan to show that large numbers of young children, particularly boys, are exposed to sexually explicit media.

Difficulties In Regulating Content

Unsuitable and harmful content on the Internet can be easily accessed. The reality is that a child is only click of a mouse away from pornographic, obscene, indecent, and unsuitable content on the Internet. Trying to prevent this situation by legislating against the material itself misses the concern as technically it is not possible to prevent material circulating on the Internet.[4] For

[1] * Acknowledgment: The funding for this research paper is from a research grant - Fundamental Research Grant Scheme (FRGS-2017) supported by the Malaysian Ministry of Higher Education, Malaysia in which the author is the Project Leader.

(Star-Online-A Growing Addiction, 2016. Available at: https://www.thestar.com.my/news/nation/2016/12/18/a-growing-addiction-as-internet-addiction-tightens-its-grip-on-asia-sunday-star-speaks-to-experts-ab/
Hentai popular Amongst Malaysian Porn buffs, 2017.
Available at: https://www.thestar.com.my/news/nation/2017/01/09/hentai-popular-among-malaysian-porn-buffs/)

[2] Yaman, Akdeniz, "Controlling illegal and harmful content on the Internet", Crime and the Internet, Ed., David S. Wall, (London: Routledge, 2001) pp. 113 -117.

[3] Zittrain, Jonathan, The Future of the Internet-And How to Stop It, (New Haven [Conn]: Yale University Press, 2008) pp. 36-62. For a discussion on the social impact of cyberspace upon the individual see the following: Nicholas, Negroponte, Being Digital, (New York: Knopf, 1995) pp. 163-231.

[4] Reported in "Disturbing Views: Left alone with their own devices small children have been secretly viewing pornography and some have even been mimicking what they see online"
The Star Malaysia, 19 Aug 2018;

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 5 Issue 20 (September 2020) PP. 80-86
DOI 10.35631/IJLGC.520005

instance, in terms of regulating content on the Internet, section 211 of the Communication and Multimedia Act 1998 provides for the following:

> "(1) No content applications service provider, or other person using a content applications service, shall provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person.
> (2) A person who contravenes subsection (1) commits and offence and shall, on conviction, be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding one year or to both and shall be liable to a further fine of one thousand ringgit for everyday or part of a day during which the offence is continued after conviction."

With regard to the above provision if the content originates within Malaysia the access to the website and the content could be prevented. However, more often than not such material emanates from overseas Internet Service Providers. In such an instance, the above provision might not be too effective. Hence, a method by which content unsuitable for children could be reduced by adopting age-verification controls could have some positive impact for the Internet. Alternatively, the better choice would be to implement mechanism to prevent access to such material.

Methodology

The methodology used for this research includes traditional legal doctrine analysis of various legislative framework enacted particularly, in the United Kingdom on age-verification and briefly on Estonia. This is carried out through firstly through a proposal to construct a legal framework with a requirement for age verification with possible sanctions for failure to comply and secondly to formulate a personal digital identity management service system for verification of age. In order to achieve the first objective the methodology that has been used is legal analysis or what is known as the doctrinal analysis of legal material. This method has been used to examine the current legislative frameworks with age verification controls in existence in various other jurisdictions and legal frameworks. Mainly, the United Kingdom and the system which is in place in Estonian legislative provisions will be examined for the second proposal.

Age Verification Controls

Age verification is a mechanism whereby access to content is restricted by putting in place technical measures based upon a user's specified age. Such a mechanism could control or perhaps reduce the chances of minors accessing the content online and strengthen the existing regulatory framework. Recent advances in identity authentication and assurance mean that public authorities bear a renewed interest in the possibility of improving protection for children through the use of technological measures to verify age which is not the same as children are to be monitored every step they click a mouse.[5]

Authentication as a fundamental goal in security and can be achieved in many ways. It is achieved by asking the users for their credentials which are formed by one or more of the following categories. Firstly, through knowledge which may consists of passwords, pass

[5]Effective age verification techniques: Lessons to be learnt from the online gambling industry, Final Report December 2012-December 2013.

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 5 Issue 20 (September 2020) PP. 80-86
DOI 10.35631/IJLGC.520005

phrases, secret questions, cryptographic key etc. Biometrics. Is another form of authenticating which uses fingerprints, face recognition, signatures, and thumbprints? Finally, authentication could also be achieved by the used of tokens mainly consisting through the usage of security dongles, tokens, smart cards, smart phone and the like.

The above could also be explained through behavioral patterns such as Behaviour Biometric software using key-stroke dynamic software to record typing patterns. The typing pattern would recognise whether the users are children or adults as the pattern of typing for children differs from that of adults. Other known software on gait biometric recognition and face recognition technology are also used to determine the age of a user.

Implementing age verification control mechanism into the law nevertheless has some disadvantages and challenges. A district court in the United States[6] identified three problems with age-verification measures. First, age verification "deters lawful users from accessing speech they are entitled to receive" by potentially compromising the user's anonymity. Second, age verification is problematic because it requires the use of a credit card, which not all adults have. Third, age verification would pose significant costs for Internet speakers who have to segregate harmful and non-harmful material, and update and maintain [the] system.

An example of a country adopting age-verification using users' national identity card is Estonia. Whereas United Kingdom, with the passing of the Digital Economy Act 2017 is using users' credit card also as a measure to prevent access to pornographic sites. However, in order for the verification to be effective both the authentication systems need the knowledge of a secret pin which resulted in a dual-factor authentication that covers knowledge and token categories. In 2015, the government of South Korea required minors to have content filtering applications installed in their mobile devises. The mandate required all telecommunications operators to provide means to block content deemed harmful to children below the age of 19 years on their mobile phones and to ensure notification to parents whenever the blocking mechanism becomes inappropriate.

However, as highlighted in the above case in the United States there are many security vulnerabilities associated with the collection of sensitive information as users test sample is collected during the identification process and is matched with all the templates stored in databases. An audit carried out in the Canada identified some of these risks as unauthorized access to stored messages and search history of the user, sensitive leakage of data such as children's date of birth to be misused. And basic web security issues.

Position In The United Kingdom

The UK has been promoting the use of age verification since 2015. The commitment by the Government to impose regulations that required age verification for access to all sites containing pornographic material in order to reduce the access of children to harmful sexual content online. The main highlight of this commitment is to impose liability on those Internet Service Provides who provide pornography for a commercial gain have been required to implement such verification procedures. As such with the enactment of the Digital Economy Act 2017 is seen as a significant step to make the service providers responsible and to make

[6] See. Booksellers Ass'n v. McMaster, 371 F. Supp. 2d 773, 782 (D.S.C. 2005) (citing Reno v. ACLU, 521 U.S. 844, 881 (1967); PSINet, Inc. v. Chapman, 362 F.3d 227, 236-37 (4th Cir. 2004)

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 5 Issue 20 (September 2020) PP. 80-86
DOI 10.35631/IJLGC.520005

the Internet safe for children. Now, all commercial pornography service provides are required to carry Age Verification tools to stop children from accessing these contents online. In order to carry out the above individuals must prove that they are 18 years and above but without having to show their personal identification. Section 14, Part 3 of the Act sets out the requirement that commercial pornographic material cannot be make available online to users without sufficient age verification controls. The said section also provides for the State Secretary to make regulations specifying what is regarded as commercial pornography. Section 21 of the Act enables the regulator to notify payment-service providers and ancillary service providers who has breached Section 14(1) or who are making extreme pornographic material under Section 22 in the United Kingdom. It was observed that the current legislation only applies to commercial pornographic websites and will not be able to restrict viewing on social media sites, such as Facebook, Twitter, and YouTube. The regulator can only give notice to the social media but has no power to compel these ancillary service providers to close down accounts with pornography or hardcore pornography.[7]

Aside from this all content hosted outside of the United Kingdom will be required to carry verification mechanism as well. Regulators are required to collaborate with each other to ensure that online providers comply with this legal requirement. It has to be noted the position in Malaysia is somewhat different from that in Malaysia as commercial pornography is not allowed in Malaysia. Thus, age verification controls would be useful to access content originating out of Malaysia.

Digital Identity Verification In Estonia

Estonia's electronic ID card program was launched after the Estonian Parliament passed the Identity Documents Act 1999, which became effective on 1 January 2000. The country's national guidelines were established to create a mandatory national identity card where it has a function of both a physical ID and an electronic ID. Chapter 3, s 9(5) of the Act states that the identity card shall have the digital data of a person, a certificate enabling digital identification and digital signing. Estonia's electronic signature functionality is mandatory, where the authentication certificate will contain the cardholder's name, personal ID number and an official e-mail address unique to each cardholder. Verification of a user is made easy where the particular service queries a central database, named identity documents database to check that the card and relevant code match. This allows its citizens to perform electronic transaction easily. The usage of electronic authentication transaction has reached 2.7 million in the month of September 2018. This is easily done as Estonia offers over 900 e-services to citizens and 2400 to businesses. With the advancement of wireless and mobile technology, the use of this government verified identification naturally evolved from e-ID to mobile-ID, where the citizens' identity is tied to their mobile sim card. Mobile-ID was introduced in 2007, but the law regulating it came into force in 2011. Most of the issued SIM cards now are Mobile-ID ready by default. Estonia also has Digital-ID system, regulated under Section 201 of the Act, which is another identification solution for those that do not have a SIM card in their smart device but needs to verify their online identity. It is basically a chip card for digital use only. All IDs (ID card, Digi-ID, and Mobile-ID) have public key infrastructure (PKI) certificates for digital signatures and secure authentication.[8]

[7] Explanatory Notes to the Digital Economy Act 2017, para 21.
[8] Estonia takes the plunge (The Economist, 28 June 2014) https://www.economist.com/news/international/21605923-national-identity-scheme-goes-global-estonia-takes-plunge

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 5 Issue 20 (September 2020) PP. 80-86
DOI 10.35631/IJLGC.520005

Legal Challenges In The Implementation Of Age Verification

In Malaysia, freedom of expression is practically restricted on grounds of morality. Internet is regulated by practicing self-censorship. Pursuant to Article 10(2) of the Malaysian Federal Constitution, freedom of expression is restricted on any matter in the interest of the security of the federation or any part thereof, friendly relations with other countries, public order or morality. In terms of sexual materials and pornographic materials, Malaysian laws are piecemeal. Printing Presses and Publications Act 1984, and the Film Censorship Act 2002. Communication and Multimedia Act 1998 regulates content which is not only obscene, but also indecent and offensive. The Penal Code too applies to obscene material either in print or in online form. Matters pertaining to children also found in the Sexual Offences against the Children Act 2017 which includes provision on online pornography.

For example, section 211 of CMA 1998 provides for a fine not exceeding RM50,000 or imprisonment not more than 1 year or both upon conviction. The said section deals with prohibits content including obscene materials. Section 233 of the same Act deals with an improper use of a network or facilities in relation to obscene materials, provides for the same punishment upon conviction. It states that:

> "(1) A person who— (a) 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; or (b) initiates a communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address, commits an offence.
> (2) A person who knowingly— (a) by means of a network service or applications service provides any obscene communication for commercial purposes to any person; or (b) permits a network service or applications service under the person's control to be used for an activity described in paragraph (a) commits an offence.
> (3) A person who commits an offence under this section shall, on conviction, be liable to a fine not exceeding RM50,000 or to imprisonment for a term not exceeding one year or to both and shall also be liable to a further fine of RM1,000 for every day during which the offence is continued after conviction."

It is put forwarded that none of these existing legislative provisions have a method of preventing exposure to content which may originate out of Malaysia. The legislative measures put in place are to regulate content which originates from or within Malaysia which is an offence under the CMA. Hence, circulation, distribution and making available harmful sexual content are prohibited. However, as stated early in this paper sexual harmful content can be available on the Internet as it could originate outside the jurisdiction of Malaysia. The statistics on Internet usage by children and the younger age that children are exposed to verifies this problem. It is therefore timely legislative provisions to be enacted which require Internet Service Providers to employ some form of a verification method to prevent such exposure of children while they are surfing the websites.

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 5 Issue 20 (September 2020) PP. 80-86
DOI 10.35631/IJLGC.520005

The first challenge relates to remediation in the adoption of biometric technology either in the form of using thumb print or face recognition to confirm the age of the child which would be kept in a data bank. Such a collection of data could lead to identity fraud by altering or concealing traits. Thus, it will be important for policy and law to both address the perpetrator of identity fraud and introduce system owners to create an environment that minimizes the opportunity for misuse of biometric samples.

The second issue concerns the lack of consent in which case the child's parents/ guardians consent is needed for the processing of information as one's face; photograph or a picture of an individual falls within the ambit of personal data. Also, the lack of digital consent does not only invade one's privacy and may lead to cases on harassment if the data is misused. Thirdly, age verification technology is not absolutely accurate. This leads to the issue of reliability in the data gathered.

Concluding Remarks

Malaysia's journey towards the realisation of Vision 2020 of becoming a developed nation and choosing information and communication technology as a tool for achieving this goal has resulted in the increase use of technology, by society at large, including children. This is also reverberated in the 11th Malaysia Plan (2016-2020): Anchoring Growth on People. The enactment of cyberlaws, in particular, the Communications and Multimedia Act 1998 also echoes the Government's objective in regulating converging communication technology. Moreover, this research is also in line and has a relevance to National Cyber Security Policy (NCSP) in which this research falls within one of the ten critical factors including Information Infrastructure in existence.