Pertanika J. Soc. Sci. & Hum. 29 (S2): 185 - 203 (2021)

PERTANIKA JOURNALS

SOCIAL SCIENCES & HUMANITIES

Journal homepage: http://www.pertanika.upm.edu.my/

Monitoring Internet Child Pornography (ICP) in Malaysia

Nabilah Hani Ahmad Zubaidi

Department of Law, Faculty of Law & International Relations, Universiti Sultan Zainal Abidin (UniSZA), 21300, Kuala Terengganu, Malaysia

ABSTRACT

Malaysian law enforcement authorities were previously at a disadvantage in monitoring and investigating ICP cases. They lacked online tools to detect ICP and other cases of child sexual exploitation and relied on information from their international counterparts. The discovery of Richard Huckle and Blake Johnston, two child sex offenders who abused Malaysian children, was only possible with information shared by Australia's Argos Task Force and the US Homeland Security Investigations. While Malaysia currently practises information and intelligence exchange and collaboration in digital forensics, more action is needed to detect and monitor ICP activities. It is imperative for Malaysia to take all necessary steps to prevent, detect, investigate, punish, as well as address the root causes of ICP. This paper addresses this issue; it focuses on the dilemmas faced by Malaysian authorities in reducing the availability of ICP images and in deciding to prosecute offenders. It conducts an initial exploration of the ways in which authorities can protect children by proactively seeking out ICP images via a victim-identification database and blocking ICP images. The paper seeks to demonstrate that traditional policing methods, such as responding to citizen reports and image discovery through arrest and seizure, while still necessary, can be out-dated. Through semi-structured interviews with key-stakeholders from the Malaysian government and agencies, this study seeks to gain some insight into Malaysia's implementation and enforcement experience in relation to ICP. The study suggests how the present-day policing response of ICP images can be realigned to other key intermediaries on the internet.

Keywords: Child pornography, detecting and monitoring ICP material, enforcement of the law, *Sexual Offences Against Children Act 2017*

ARTICLE INFO

Article history:
Received: 05 May 2020
Accepted: 12 March 2021
Published: 17 May 2021

DOI: https://doi.org/10.47836/pjssh.29.S2.13

E-mail address:
nabilahhaniaz@unisza.edu.my

ISSN: 0128-7702
e-ISSN 2231-8534

INTRODUCTION

The *Sexual Offences Against Children Act 2017* (SOAC) represents a significant landmark in protecting children from ICP offenders. It marks a departure from criminalising child sexual abuse images through the more general obscenity-based approach in the *Penal Code*, the *Communications and Multimedia Act 1998* and the *Child Act 2001*. SOAC now covers an unlimited representation of ICP in various technologically-mediated forms. This include pseudo pornographic imagery and virtual images of child sexual abuse, as well as other forms of non-physical sexual crimes such as child sexual grooming. Sections 5 - 10 under Part II of SOAC are the main provisions governing ICP. Another significance of SOAC is the provision of a specific working definition of ICP, which was previously absent in other legislation. To ensure harmonisation between SOAC and other applicable provisions, cross-referencing clauses are explicitly provided in Schedule 1 to 5.

Although Malaysia is not short of good legislation such as SOAC, the main problem is reported to lie in its implementation and enforcement. Criminal sanctions alone are insufficient to deal with the problem and will be ineffective if enforcement is weak. This is especially important because ICP crimes are clearly complex and time-consuming and often involve multiple jurisdictions. RMP officers report some challenges faced and dilemmas encountered in detecting and investigating ICP images on the internet. These include a general lack of coordination and control in the administrative structure of regulatory agencies, limited funding, limited digital forensic investigation experts, a lack of coordination between governmental law enforcement agencies and telecommunication companies, and limitations in detecting and monitoring ICP crimes. These problems are highlighted when, in 2018, Malaysia was revealed to be one of the locations favoured by pornographers to download, transmit, and distribute ICP.[1]

The paper focuses in examining issues in the detection and monitoring of ICP crimes in Malaysia. Law enforcers especially find it difficult to detect ICP images in mobile applications with temporary recording features such as media streaming and private-browsing sessions. Furthermore, the possession of ICP material in an individual's portable software is almost impossible for the authorities to detect, and identifying offenders is not clear-cut if ICP is found on a computer used by multiple individuals. The case of R v. Richard Huckle (2016)[2] demonstrated how the dark web was used for illegal activities such as the transaction of child pornography imagery; an opportunity for offenders to evade police detection. According to a Sessions Court Judge: [3]

[1] As reported in Malaysia's mainstream media and confirmed by the police, The Straits Times Asia. (2018, January 30). Malaysia Tops in South-east Asia for Online Child Pornography. Retrieved from https://www.straitstimes.com/asia/se-asia/malaysia-tops-in-south-east-asia-for-online-child-pornography. See also interview: Police Officer 1.

[2] R. v. Richard Huckle London Central Criminal Court, Old Bailey (Unreported) 2016.

[3] Interview: Judge 1.

> The dark web needs specialised and aggressive undercover agents who are equipped with thousands of ICP images as a 'ticket' to enter the group. Our law enforcement can only scratch the surface. Our expertise is not at the level to dig into the deep web. This is why there has yet to be any charges against dark web ICP activities.

From 2006-2014, Huckle worked as an English teacher and church volunteer in the Malaysian capital of Kuala Lumpur. It was later discovered that Huckle had systematically abused the children under his care. Huckle would photograph and film his sexual exploits of these children, which he then edited, and posted on the hidden 'dark web'[4] network. During his trial in London in June 2016, the Crown revealed that Huckle was an active member of a heavily encrypted deep website, 'The Love Zone', which is now inoperative. The shift away from the public domain of the web to password-encrypted networks has facilitated offenders to evade filtering and other detection software from law enforcement bodies, reducing the risks of getting captured.[5] This would explain why Huckle had managed to conduct his illegal activities for nine years without being detected. He only came to the attention of the British authorities in 2014, after a tip-off from Australian's Argos Task Force investigators who had arrested another man running a paedophile site. By using the dark web to upload, distribute, advertise, and sell images of child abuse, the Crown emphasised the intensity and extremity of Huckle's crime.

Another case highlighted by RMP is R v. Blake Robert Johnston (2017). This involved an American child sex offender arrested by the US authorities in 2014 for ICP and child sexual grooming offences.[6] In 2017, US' Homeland Security Investigations agency had identified 94 minor victims who were enticed online by the Johnston to engage in sexual activity, ranging in age from as young as 12 years and coming from 32 US states and six different countries. On his personal electronic devices the police found explicit images of his own genitals and those of more than 300 child victims, many of whom were Malaysian. His *modus operandi* was to befriend children through the social media applications *OoVoo*, *Kik*, and *Omegle*.[7] He would "entice young

[4] The term 'dark web' refers to the 'hard to access' part of the internet, as opposed to the public domain of the internet accessible via search engines such as Google, Internet Explorer, or Mozilla Firefox. Accessing the dark web requires the use of an anonymising browser called The Onion Router, or commonly knowns as TOR. The TOR browser routes a web page request through a series of proxy servers operated by thousands of servers around the globe, and each of these levels may be encrypted. This process renders an internet protocol (IP) address unidentifiable and untraceable, and is often used by individuals to hide their physical location. See Wall (2017). *Crime and deviance in cyberspace*. Abingdon, UK: Routledge.

[5] Ibid.

[6] US v. Blake Robert Johnston, 2017, Northern District of California (Unreported).

[7] *OoVoo* is described as being similar to *Skype*. *Kik* is a secure messenger application that protects user's anonymity. *Omegle* is a website designed to allow strangers to talk to other strangers anonymously. See Ireland's Raidió Teilifís Éireann (RTE) (2017, September 3). *US Sex Offender Groomed Children*

girls" and exchange pornographic images with them.[8] Even though the images in Huckle and Johnston's case were initially distributed in a closed network, the images are ultimately subjected to uncontrolled worldwide distribution.

It is useful to chart some concerns about the Malaysian law enforcement framework to identify further steps that that should be taken by law enforcement agencies in enhancing the detection and monitoring of ICP material transmitted online.

METHOD

This research adopts a doctrinal approach. A library research was conducted to examine the legal literatures from the primary and secondary sources which included, but not limited to, international human rights treaties, statutes, case-laws, extra-legal materials, books, articles, seminar papers and newspapers. The study was supplemented by an empirical study through semi-structured interviews conducted over a period of three months from 2017 to 2018[9].

RESULT AND DISCUSSION

The Detection and Monitoring of Crime

One accepted practice for enhancing legal compliance is to increase rates of detection and prosecution. This concept is widely accepted and is used in various contexts. For example, threats of a fine for speeding or illegal dumping are preventive measures to improve road safety and protect the environment. Compliance increases in proportion to the degree to which the general public believes that failure to comply is likely to be detected and penalised. The WePROTECT Global Alliance addresses this issue, and demonstrates a commitment undertaken by state parties to, among others, investigate cases of ICP exploitation and prosecute offenders, reduce the availability of ICP material, and increase public awareness of the risks posed by children's activities online.[10] For example, SOAC criminalising the possession of ICP is based on the fact that the image would not have been produced in the first place but for the demand for such material on the part of those who have an interest in ICP. When the authorities intervene to block the supply of images, this may deny users access to the images. When image producers are aware of the online presence of regulators, they are more likely to desist. This, therefore, contributes to deterrence.

Every image viewed represents a real child who has been groomed and abused to meet the demand for ICP. As long as the material is still circulating, the child is continuously harmed. This is particularly significant when ICP activities are difficult to detect and blocking the infringing website is the only practical immediate recourse in preventing further re-distribution. The authorities, therefore, play an important

in Ireland. Retrieved from https://www.rte.ie/news/2017/0910/903600-johnston-abuse/.

[8] Interview: Police Officer 1.

[9] Ethical approval to conduct the interviews was granted on May 2017.

[10] WePROTECT Global Alliance (End Child Sexual Exploitation Online). (2015). *Our Commitments: 15-16 November 2015.* Retrieved from https://www.weprotect.org/our-commitments.

role in monitoring ICP websites to reduce public access to them. WePROTECT Global Alliance demonstrates that the identification and blocking of ICP images is practiced by most national regulatory agencies. While restrained by a number of enforcement challenges and thus unable to nip ICP images in the bud, this strategy remains key in reducing dissemination and possession of ICP and serves to dissuade ICP offenders in the long run.

The Role of Relevant Law Enforcement Agencies in Malaysia

Figure 1 illustrates the main agencies involved in regulating ICP in Malaysia:

The discussion of this paper confines itself to mainly the role of RMP, and to a certain extent, of MCMC and the Royal Malaysia Customs Department (Customs Department).

The Policing Regime

> *Money and resources are always a chicken and egg problem, but like it or not, we just have to manage accordingly. It ought to motivate us to be more innovative, and at the same time active and proactive, rather than responsive.*[11]

[11] Interview: MCMC Officer 2.

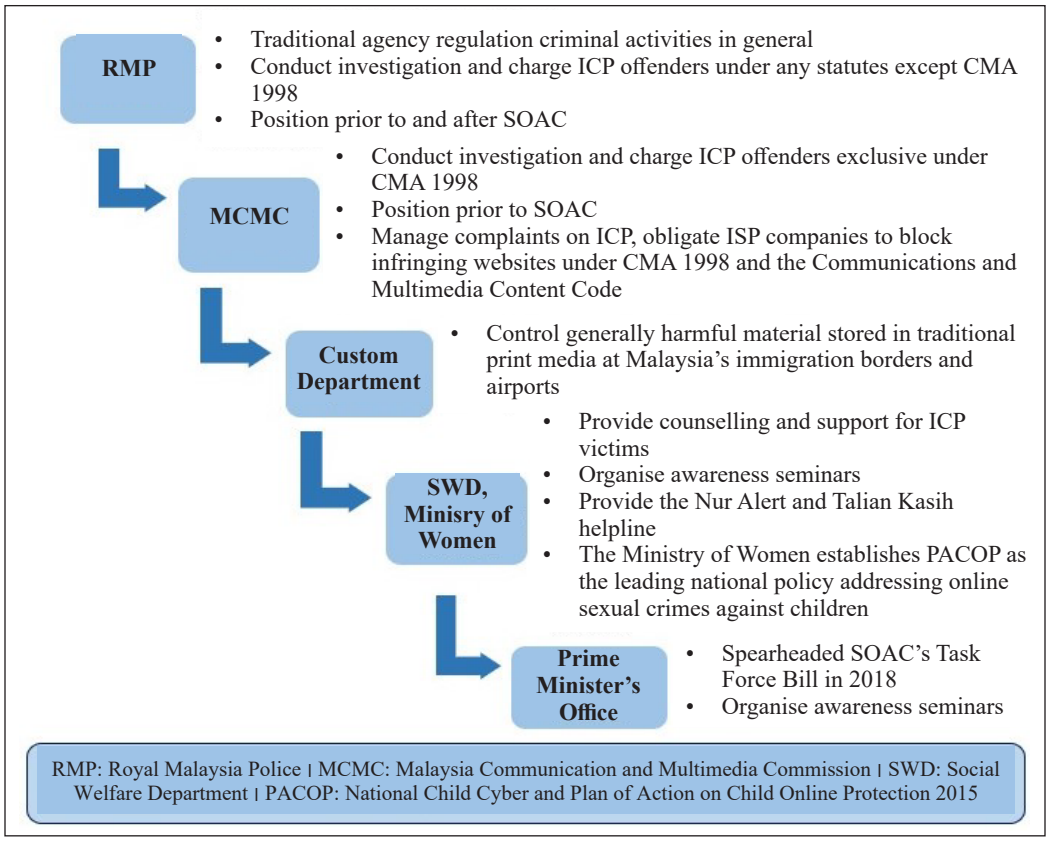

Figure 1. The role of law enforcement and regulatory agencies

Traditional methods of conducting investigations, such as responding to reports and image discovery through arrest and seizures, will not be sufficient, as the investigation and prosecution of ICP crimes must be swift.[12] The internet medium in which ICP offences are committed demands technological competence and sophistication on the part of law enforcement agencies. Earlier police operations used impersonation techniques where investigators adopted a number of guises: ICP consumer; child pornography collector interested in trading images; or user of a private P2P media application such as *bit-Torrent*, *Ares* or *Freenet*.[13] For example, Operation Starburst was first conducted in England in 1995, yielding many prosecutions[14] The operation resulted in the arrest of 15 offenders in Britain, and a number of others in Hong Kong, Germany, South Africa, Singapore, Canada and the United States.

Other international police operations have since resorted to a new, technology-based form of policing using undercover techniques. One example is the Sweetie Operation of 2013 which was considered "a policing success".[15] This Dutch-led police operation identified 999 men of 71 nationalities who tried to make sexual contact with a life-like computer-generated 10-year-old Filipina girl called *Sweetie*. *Sweetie* was used as bait to lure child predators: when adults contacted Sweetie in public chat rooms, the police operated her from an Amsterdam warehouse through a software application. The police identified suspects by cross-referencing their e-mail or *Skype* addresses, social media profiles and other public information. The highest three groups of child sex offenders arrested in this operation were from the US, the UK, and India,[16] and this is linked to webcam cybersex as a 'flourishing' ICP phenomenon of the 21st century. Such investigations are, however, very resource intensive, complex and time-consuming. ICP investigations are ultimately a race against time as the technology possessed by the Malaysian Government is reported to "often be a few steps behind that of the industry".[17] Special

[12] Interview: Police Officer 1. For a commentary on international police operations against ICP, see Krone, T. (2005). *International police operations against online child pornography*. Canberra: Australian Institute of Criminology.

[13] Adilah & Dzulkifly (2018). Experts laud new police system tracking child porn users. *Malay Mail*. Retrived from https://www.malaymail.com/news/malaysia/2018/07/10/experts-laud-new-police-system-tracking-child-porn-users/1650523.

[14] Subsequent police operations include Operation Cathedral in 1998, and Operation Ore in 2002, both led by Britain's National Crime Agency. Operation Cathedral seized pornographic material from an international ring called *The Wonderland Club* which traded child abuse images over the internet. The operation discovered one of the largest collections of ICP images, over 750,000 images and over 1,800 hours of digitised videos. Operation Ore led to the investigation of more than 7000 people, with almost 1,500 convictions. See Metcalf (2008). Policing operation ore. *Criminal Justice Matters*, 68, 8-9. doi: 10.1080/0962725070855327, BBC News. (2001, February 13). *Wickedness of Wonderland.* Retrieved from http://news.bbc.co.uk/1/hi/uk/1167879.stm.

[15] Crawfurd (2014). Child abuse image database containing millions of images to launch. *BBC News UK*. Retrieved from https://www.bbc.co.uk/news/technology-30175102.

[16] DW News. (2013, November 7). *Dutch Activists Uncover Webcam Child Sex Tourists*. Retrieved from https://www.dw.com/en/dutch-activists-uncover-webcam-child-sex-tourists/a-17213042.

[17] Interview: Police Officer 1.

units managing online investigation needs to be sufficiently agile to respond to the rapid pace of on-going technological change.

Despite these challenges, there are technological initiatives which provide potentially viable means to help address the problems of ICP. This is the approach taken by RMP, one which is underpinned by a dose of realism regarding the institution's available funding, facilities and human resources at this point in time. RMP recently launched the Internet Crime Against Children: Child Online Protective Services (ICACCOPS) monitoring software. ICACCOPS represents a significant investment by the government in the development of police services to assist ICP investigations. The government recognises that direct harm to children depicted in images will continue for as long as the image is distributed and displayed[18], hence the need for authorities to monitor and subsequently block access to the images. A similar tool was deployed by Australia's Argos Task Force and this was responsible for detecting *Huckle's* activities.[19] This software is a welcome addition to RMP's suite of investigative tools to detect ICP offences.

RMP had been under heavy public scrutiny for their failure to detect Huckle's activities and the complete lack of trained police forensic hackers in Malaysia.[20]. In 2017, RMP's Assistant Principal Director Jenny Ong revealed in a press statement that the Malaysian police could not properly monitor encrypted paedophile networks as it did not have the expertise to access and navigate the dark web.[21] It should be noted that, at that time, there was a distinct lack of urgency on the part of the government and the RMP hierarchy regarding the problem of ICP. RMP's regime underwent significant change in July 2018, a year after SOAC was enacted. The newly-launched Malaysia Internet Crime Against Children Investigation Unit (MICAC) has now replaced RMP's former D11 Women and Children Investigation Division (D11) and operates under D11's supervision. MICAC monitors traffic at pornographic websites, and are tasked with using software to monitor, locate and pin-point viewers and disseminators of CSA material in order to obtain evidence for prosecution.[22] MICAC's objective is to enhance ICACCOPS and expand its coverage to monitor anyone who accesses ICP websites.

[18] Dewan Rakyat (House of Representatives). (2017). April 3 Debate (Thirteenth Parliament, Fifth Session). Retrieved from https://www.parlimen.gov.my/hansard-dewan-rakyat.html?uweb=dr&lang=en, per YB Azalina Othman Said, pp. 14-16.

[19] 'Team Argos, the Australian detective unit…made a startling discovery from the team's scouring of online paedophile networks…the unusual number of internet addresses in the Kuala Lumpur area transmitting CSA material from the dark web", in Ananthalakshmi (2016). Child sex abuse crimes 'going unpunished' in Malaysia. *Independent*. Retrieved from https://www.reuters.com/article/us-malaysia-sexcrimes-insight-idUSKBN1390AT?il=0.

[20] Interview: Police Officer 1.

[21] Ibid.

[22] Vijaindren & Sazili (2018) Communications and Multimedia Ministry to combat child pornography. *News Straits Times*. Retrieved from https://www.nst.com.my/news/nation/2018/07/389324/communications-and-multimedia-ministry-combat-child-pornography.

ICACCOPS represents the use of innovative technology as part of a package of measures designed to monitor the activities ICP offenders and provide evidence with which the authorities can prosecute them .[23] It works 24 hours a day and locates and pin-points in real time internet users surfing ICP sites. It builds a data library of these individuals and the Internet Protocol (IP) addresses they visit. The individuals are profiled for three data points: which portals they frequent, how long they spend on the sites, and the files they upload and download. ICACCOPS tracks in real time the IP addresses of individuals accessing ICP and the websites they visit.[24]. The key capacity of this software is its ability to remotely monitor an offender's use of known mobile phones and computers. Ong explains that MICAC is now authorised to call suspects in for questioning or even arrest them in their homes. MICAC also has the power to seize smart phones, computers or laptops to check for both adult and child pornographic material.[25] Sections 4 - 10 of SOAC and section 292 of the Penal Code provide the legal underpinnings of ICACCOPS investigations.

Some Issues with Malaysia's ICACCOPS

The first issue is whether ICACCOPS is monitoring ICP activities in general internet traffic or is focused only on activities on the dark web. In 2017, when the fieldwork was conducted, RMP reported that they were still beta-testing ICACCOPS. The reporting officer mentioned that, if successful, ICACCOPS would be able to monitor the uploading and downloading of child abuse images to and from the dark web. The officer was, however, aware of several drawbacks of the software and spoke about them candidly: [26]

> With ICACCOPS, we can detect the traffic of IP addresses, leading to whoever is downloading or uploading any pornographic image. But we do not know what he does with the material, and we cannot ascertain if it is a video or an image. We cannot access that because of our Data Protection Act 2010. We are trying to get full access to this [ICP images in the dark web], however, for now, this remains a concern.

This software is reported to have the ability to monitor the dark web and P2P networks, provided that investigation teams can decipher encrypted pages. However, it is unlikely that the software will monitor regular internet usage through public sites such as *Google*, *Youtube*, as well as social media sites including *Facebook* and

[23] Ibid. For transparency in investigation, officers handling the system were required to log in their registered credentials, in interview: Police Officer 1.

[24] Today Online. (2018, July 9) *New Malaysian Police Unit to Monitor Citizens Who Watch Pornography Online.* Retrieved from https://www.todayonline.com/world/new-malaysian-police-unit-monitor-citizens-who-watch-pornography-online

[25] Ananthalakshmi, 'Child sex abuse crimes 'going unpunished' in Malaysia'.

[26] Ibid. See also interview: Police Officer 1.

Twitter.[27] This is because private activities carried out within the public internet domain are protected under the *Data Protection Act 2010*. The RMP officer was concerned that the protection of individual personal data provided under the *Data Protection Act 2010* might limit the success of ICACCOPS.[28]

The second issue is that ICACCOPS identifies websites based on IP address. However, this is problematic in the case of public computers. IP addresses in a family home or a cybercafé, for example, are generally shared. It should not be automatically assumed, therefore, that all traffic to and from an IP address corresponds to a single account holder. The government has, nonetheless, undertaken to regulate cyber cafes and introduce liability on online publishers in an attempt to solve this quandary. It has partially ordered internet cafe operators to take measures against obscene, indecent or pornographic materials in some territories.[29] For instance, the Federal Territory of Kuala Lumpur enacted the *Cyber Centre and Cyber Cafe Rules 2012*. Its main role is to supervise the granting of professional licenses, and to require licensees to keep records of computer usage for each computer deployed, including the personal identity of users. The rules are not federal law and, therefore, only apply in Kuala Lumpur. This creates gaps and discrepancies among the laws applicable in different Malaysian states.

The third issue is that MCMC's role in detecting and monitoring ICP is further enlarged by ICACCOPS. In 2019, MCMC's Network Security, New Media Monitoring, Compliance and Advocacy Sector Chief reported that the agency was starting to collaborate with RMP in monitoring pornographic websites through an Artificial Intelligence (AI) system[30] known as the Algorithm.[31] Algorithms is practiced by Microsoft's *PhotoDNA*, *Google Photo*, *Google Cloud*, and is commonly deployed by the US and Australian police.[32] This is uncharted territory for MCMC, and the agency needs more time to explore this AI in order to ensure that it does not block or

[27] Ibid.

[28] Under Section 40 (1) of the Data Protection Act 2010, a data user shall not process "any sensitive personal data". Sensitive personal data includes information on physical health or any other information the relevant Minister deems to be personal, including an individual's private communications data.

[29] United Nations Human Rights Council. (2018). ECPAT Universal Periodic Review of the Human Rights Situation in Malaysia Submission. In End CSEC Network Malaysia & ECPAT International, *Sexual Exploitation of Children in Malaysia*. Geneva: OCHCR Publications. Retrieved from https://www.ecpat.org/wp-content/uploads/2018/07/Universal-Periodical-Review-Sexual-Exploitation-of-Children-Malaysia.pdf.

[30] According to Fadhlullah Abdul Malek, in Adilah & Dzulkifly, 'Experts laud new police system tracking child porn users'.

[31] Algorithms are calculations, instructions and rules that computers and other technologies use to make decisions about what people see online. Algorithms allows for the interlinking of websites based on similarity content and other criteria. See UK Department for Digital, Culture, Media & Sport and Home Office. (2019). Closed consultation. In Wright, J. & Javid, S., *Online Harms White Paper*. UK: APS Group. Retrieved from https://www.gov.uk/government/consultations/online-harms-white-paper.

[32] See Interview: MCMC Officer 2.

bypass restrictions to free expression under the Federal Constitution. The Algorithm system functions in a similar to *Google Photos*: it categorises pictures according to user, photographic subject, and other traits, and these images are continuously fed to the algorithm by users. The Algorithm can also translate images into text which could make possible narrower searches that are beyond the capabilities of visual tools; one could search an archive of images with the search string "children and beds", for example.[33]

While ICACCOPS builds a database of user profiles, RMP has to work with MCMC in order to obtain internet users' details.[34] This raises another issue with regard to the "fair procedure requirement": affected users are not afforded the opportunity to respond or appeal before a blocking decision is made.[35] It is worth noting that a number of European countries rely on the police to analyse internet content and decide its potential illegality, and this is based on the EU-funded COSPOL Internet Related Child Sexual Abuse Material Project (CIRCAMP)[36]. The CIRCAMP project manages investigation activities in the field of child abuse material and the internet. CIRCAMP is initiated by the European Police Chief Task Force under the Comprehensive Operational Strategic Planning for the Police (COSPOL) mandate. For example, Ireland, Denmark, France (Gendarmerie), Norway, Sweden and Spain are tasked to monitor the different peer to peer networks and collect evidence and data on computers and IP addresses. These countries disseminate evidence packages to enable national police services to start investigations, ands such information will lead to the identification of high-profile targets. This practice demonstrates how ICACCOPS, alongside MCMC, can represent a workable and proactive model of policing to determine the legality of a material, and whether or not it should be blocked.

The final issue is that, despite having recourse to the ICACCOPS system, RMP still suffers from a lack of technology specialists and computer forensic experts and from inadequate staffing levels in general. To detect ICP images, RMP needs a highly-skilled investigation team to monitor and infiltrate heavily-encrypted websites and P2P groups. The absence of a dedicated specialist unit makes the penetration of password-encrypted webpages a challenging task and makes it inherently difficult to read large hard drives in the course of collecting evidence. RMP have to work with limited staffing resources, a crucial factor hindering a comprehensive enforcement of the law.

[33] Ibid.

[34] The Straits Times. (2018, July 12). *MCMC Does Not Act on its Own in Combating Online Pornography - Gobind.* Retrieved from https://www.nst.com.my/news/nation/2018/07/390127/mcmc-does-not-act-its-owncombating-online-pornography-gobind.

[35] McIntyre (2013). Child abuse images and cleanfeeds: assessing internet blocking systems. In Brown, I. (Ed.). *Research handbook on governance of the Internet*. University of Oxford, UK: Edward Elgar Publishing.

[36] Other member states of the CIRCAMP project include Belgium, Finland, Germany, Ireland, Italy, Malta, and the Netherlands. See European Commission Migration and Home Affairs. (n.d.). *Project Description: COSPOL Internet Related Child Abuse Material Project.* Retrieved from https://ec.europa.eu/homeaffairs/financing/fundings/projects/HOME _2010_ISEC_AG_INT-004_en.

RMP's Assistant Principal Director confirms this:[37]

> We [the division] do not only handle child abuse cases, but also rape and domestic violence ones. In some districts, we don't even have enough investigating officers and priority has to be given to murder cases. In other countries, they have teams visiting the crime scene, recording statements and holding meetings, but that is rarely the case here because everyone is bogged down…We should have a case-by-case team to allow us to run through each case effectively. Some cases had to be dropped due to inexperienced police investigators.

All stakeholders agree that Malaysia is held back by manpower and budget constraints in addressing crimes against children, including ICP. A police officer explains that it costs a lot to keep up with rapidly-changing technology and, at the moment, there is a lack of funding to purchase state-of-the-art investigation technology.[38] While RMP admits that investigation of the dark web can be particularly expensive; to tackle the ICP issue seriously would require significant institutional will to invest in sending staff overseas to train as digital forensic investigators.[39] Meanwhile, exchanging tip-offs with counterpart police forces is considered one of the best strategies to enhance ICACCOPS.

Definitional Dilemmas and Forensic Software

Law enforcement agencies may be more willing to pursue cases if clear digital evidence of the crime confirms its severity, and this increases the likelihood of a successful prosecution.[40] In determining the severity of an image, the authorities are required to determine: whether actual children are depicted; the identity of the children; and their location in anticipation of future testimony. Each defendant enjoys a "built-in defence of reasonable doubt as to the actual existence of the depicted child at each step in that process".[41] These prosecutorial burdens are onerous and the obvious difficulties in meeting them render the enforcement of existing ICP laws practically impossible. From a practical standpoint, law enforcement and prosecuting authorities may not always be able to determine whether or not children in images fit statutory definitions. Some prosecutors may be hesitant to move ahead with cases in which the only images available depict older

[37] New Straits Times (2018, October 6). *Child Abuse: We are Not Doing Enough About It*. Retrieved from https://www.nst.com.my/news/exclusive/2018/10/418676/child-abuse-we-are-not-doing-enough-about-it.

[38] Ibid.

[39] Interview: Police Officer 1.

[40] United Nations Office on Drugs and Crime (UNODC). (2015). *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*. Vienna, Austria: United Nations Office on Drugs and Crime. Retrieved from https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf.

[41] Armagh (2001). Virtual child pornography: Criminal conduct or protected speech. *Cardozo Law Review*, 1993, 23(6), p. 2.

children, while others may give priority to these cases.[42] In many instances, prosecutors are hesitant to arrest an offender if the image depicts adolescent children and they anticipate problems proving that the image depicts a minor.[43]

RMP and MCMC officers argue that it was thought a better use of police resources to tackle crimes involving images depicting grave acts with obviously underage children as they were the most vulnerable group. This is due to the assumption that harm to younger children is greater. There also exists the risk of wasting resources in investigating images which may turn out to be individuals who are aged 18 or over but may appear younger.[44] Moreover, if the images do not depict actual children, it is important to consider the "civil liability" for law enforcement agencies who conduct search-and-seize operations in violation of protected speech rights.[45] An RMP officer reports that RMP has thus far only responded to reports of ICP involving actual children.[46] It relies on forensic resources to determine the age of the child before deciding to proceed with a legal action against an offender and to assist with the investigation of ICP cases.

It is pertinent that discussion now turn to forensic software that examines material suspected to contain videos or images of child abuse. MCMC and Cybersecurity Malaysia (CSM)[47] have developed *Prototype A* to identify suspects from surveillance videos, and this prototype could be used to identify a child depicted in an image.[48] Regulators from MCMC and CSM report that RMP have been requesting assistance in digital forensics from them.[49] While RMP has an in-house forensic lab, it is insufficient, and to a certain extent, outdated from the point of view of MCMC and CSM. A prosecutor reports that RMP is often delayed because they have an extremely large number of images to extract: "For cases charged today, we may not even get a forensic report within three-months' time".[50] This is why forensic analysis is often outsourced to MCMC and CSM. Representatives of both agencies are currently unaware if their product has been used in ICP investigations since SOAC is fairly recent.

The main drawback of *Prototype A* is that RMP can only use it to analyse images already detected and the authorities also need to secure copies before the software can be used. A CSM officer confirms that, while this software can render a clearer image of a person in a photograph or video, it is not yet sufficiently sophisticated to distinguish older

[42] Wells et al. (2007). Defining Child Pornography: Law Enforcement Dilemmas in Investigations of Internet Child Pornography Possession. *Police Practice and Research*, 8(3), 278.

[43] Ibid.

[44] Interview: MCMC Officer 2.

[45] Armagh, 'Virtual child pornography: Criminal conduct or protected speech'.

[46] Interview: Police Officer 1.

[47] Cyber Security Malaysia (CSM) is an advisory and consultative arm of the government. It provides support for the government's cyber-security policy and cyber-forensics support to law enforcement agencies and is not involved in regulating ICP in Malaysia.

[48] Interview: MCMC Officer 2.

[49] Interviews: MCMC Officer 1 and MCMC Officer 2.

[50] Interview: Police Officer 1.

children from adults.[51] This is particularly problematic when it cannot determine the age of post-pubescent teenagers depicted in an image, for example those aged 14 and above. A sexually explicit image of a 15-year-old victim may be overlooked as grounds for a police investigation because the child appears to be an adult. In a lot of instances, much also depends on the quality of CCTV recording.[52] Given the cost of mobile devices with high-end cameras, most amateur ICP images are of low quality and, therefore, it is beyond the capacity of *Prototype A* to make forensic use of them. *Prototype A*, nonetheless, is a useful tool to detect young children in pornographic images or video provided that the recorded image is clear. These are some of the main limitations of *Prototype A*, and its exact reliability remains to be seen.

Exploring the Victim Identification Technology

Having a software such as ICACCOPS is a positive development, but it is only the first step in detecting and identifying offenders. It is equally important for law enforcement to use detected ICP images as evidence to identify, rescue, and protect child victims who may remain at risk of ongoing sexual abuse. International instruments such as the Lanzarote Convention[53] and the EU Directive 2011[54] emphasise victim protection and support as key elements of ICP. One of the recognised issues in supporting victims of ICP is the difficulty of identifying them.[55]. Once identified, the authorities can take steps to search for, rescue, and safeguard the child. They could also provide medical or psychological support to help victims overcome trauma. The images acquired essentially provide evidential leads contributing to successful prosecution in court.

The general lack of formal complaints made to RMP and MCMC are among the pressing issues which makes the detection and investigation of ICP cases difficult. Without some form of ICP monitoring or a victim identification system, there is maximum reliance on public reporting, and interview respondents unanimously argue that this has not always been dependable. Agencies in charge of coordinating the take downs of ICP websites such as the UK's Internet Watch Foundation (IWF) report that the overall volume of global ICP is increasing.[56] While this could mean that more children are abused and exploited for

[51] Interview: MCMC Officer 2.

52 Ibid.

53 Lanzarote Convention Article 5: Recruitment, training and awareness raising of persons working in contact with children (1) Each Party shall take the necessary legislative or other measures to encourage awareness of the protection and rights of children among persons who have regular contacts with children in the education, health, social protection, judicial and law-enforcement sectors and in areas relating to sport, culture and leisure activities.

54 EU Directive 2011 Article 23(3): Member States shall promote regular training for officials likely to come into contact with child victims of sexual abuse or exploitation, including front-line police officers, aimed at enabling them to identify and deal with child victims and potential child victims of sexual abuse or exploitation.

[55] Interviews: Police Officer 1 and 2.

[56] UK Internet Watch Foundation (IWF). (2018). Annual Report. Retrieved from https://www.iwf.org.uk/report/2018-annual-report.

the purposes of producing these images, it could also be true that the increase in images may reflect higher rates of duplication of an already existing image stock.[57] Although duplicates may seem to be less worrying in the sense that no child is subject to a new instance of abuse when duplication takes place, it is nevertheless a serious issue. This is because the existence of the image on the internet entails continuing harm to the victim, and further proliferation of the image needs to be stopped where possible. It would be useful, therefore, to explore victim identification as a method of policing where the authorities identify duplicate images and prevent their redistribution, effectively responding to and preventing the crime.

Through its National Crime Agency, England and Wales have launched a similar system known as the Child Abuse Image Database (CAID)[58] as part of its commitment to identify and protect victims. By November 2015, all forces in the UK were connected to CAID and the system is fully compatible with INTERPOL's ICSE.[59] The US National Centre for Missing & Exploited Children (NCMEC) developed a similar system, the Child Victim Identification Program (CVIP). CVIP allows analysts to perform a review of copies of seized images and videos and determines which images contain previously identified child victims.[60] Since 2002, NCMEC has reviewed more than 160 million images and videos. CAID and CVIP are examples of national ICP image databases that represents a national law enforcement effort to locate and rescue child victims depicted in ICP images. They are especially useful in stopping any ongoing abuse and exploitation of children.

There are some practical concerns relating to data protection and data retention in implementing any victim identification software in Malaysia. In commenting on the success of CVIP in the US, an RMP officer observes:[61]

> Their software is of course much more sophisticated. Unfortunately, we do not have it yet. Even if we do, I doubt we can use it with our present *Data Protection Act 2010.* Because of this 2010 Act, we do not have image datasets suitable for the necessary training and testing of this kind of software.

The officer is sceptical about the effectiveness of such a system in the

[57] Nair (2018). *The Regulation of Internet Pornography: Issues and Challenges*. Abingdon, UK: Routledge.

[58] INTERPOL. (n.d.). *International Child Sexual Exploitation Database*. Retrieved from https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database, UK Prime Minister's Office. (2013). News story: Internet safety summit at Downing Street: communique. Retrieved from https://www.gov.uk/government/news/pm-hosts-internet-safety-summit.

[59] Brown (2017). *Online risk to children: Impact, protection and prevention*. UK: John Wiley & Sons.

[60] US Department of Justice. (n.d.) National Strategy for Child Exploitation Prevention and Interdiction. Retrieved from https://www.justice.gov/psc/national-strategy-child-exploitation-prevention-and-interdiction.

[61] FBI Services. (2003). *Privacy Impact Assessment (PIA) Child Victim Identification Program (CVIP) Innocent Images National Initiative (IINI)*. Retrieved from https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/cvip.

Malaysian context due to data protection laws under the Data Protection Act 2010[62] and this echoes her earlier concerns about the implementation of ICACCOPS. In light of this, there is an urgent need to provide law enforcement agencies with the legislative mechanisms they require to investigate ICP offending. For example, legislation that forces ISPs to retain data would increase law enforcement agencies' investigative capabilities. While provisions on mandatory data retention is not provided under the Malaysian law[63], it can be justified up to a limit that respects rights to privacy; this would constitute a solution that addresses the officer's concerns. Due to constraints of space and time, this issue is beyond the scope of the paper, but it should be the subject of future research exploring possible avenues to increase the effectiveness of applying ICP offender detection and victim identification technology in Malaysia.

A Collaborative Recommendation: Extending the Responsibility to Internet Intermediaries

This paper discusses how law enforcement has been extended from traditional police work to identification and blocking strategies implemented by ISPs as internet intermediaries. ISPs, because of their technical capacities, are better placed than the police to act as regulatory agents and content assessors in the detection and blocking of ICP material. It is prudent to consider how identification and blocking strategies by ISPs are fundamental to effectively regulate the flow and dissemination of ICP.

ISP traffic is monitored by dedicated agencies such as IWF and NCMEC. These agencies dispatch ICP reports to ISPs who, in response, issue take-down orders to ICP websites where possible and block public access. While this approach is intended to prevent the cross-border flow of ICP content, Malaysia's current implementation of the identification and blocking strategy can only censor ICP content within local network servers. The strategy is regulated under the Content Code which currently regulates local ISPs as its licensees.[64] In theory, the Content Code should limit ISP immunity by placing on such companies extra liability for the distribution of and access to all forms of pornographic content. However, uncoordinated efforts by MCMC in the broader enforcement scheme has largely protected ISPs' legal immunity in terms of content.

MCMC is also not required to work with other international bodies, such as IWF and NCMEC, in the taking down

[62] Under Section 40 (1) of the Data Protection Act 2010, a data user shall not process "any sensitive personal data". Sensitive personal data includes information on matters such as health or any other personal data as determined by the relevant Minister. This would include an individual's private communications held on his personal devices. In interview: Police Officer 1.

63 "I was there in AGC when they wanted to make a law on data retention. It was extremely difficult as there were a lot of interests to consider. Until now, we cannot decide what data should and can be retained by the ISPs", in interview: MCMC Officer 2.

[64] See section 213 (1) of the *Communications and Multimedia Act 1998*: "A content code prepared by the content forum or the Commission shall include model procedures for dealing with offensive or indecent content".

of ICP content. As a consequence, the identification and blocking strategy is not being used to its maximum potential. To address this, the paper proposes the drafting and passing of a clearly-defined substantive law on the duty of care of ISPs to regulate the consumption and dissemination of ICP images on its platforms. Furthermore, it argues for the reinforcement of MCMC's role as an independent regulator to oversee and enforce ISPs' duty of care to their users in relation to ICP material. As per section 23 of SOAC, MCMC can act as an independent regulator with the power to issue substantial fines and impose liabilities on senior members of ISP companies should take-down notices be disregarded. This would undoubtedly be a financial challenge, nevertheless it should be introduced as a standard feature of MCMC's regulatory practice. According to this arrangement, MCMC would evolve in its role as the main regulator, as per CMA 1998, into a body which provides monitoring, support and enforcement. This would permit ISPs to take a leading role in regulating and censoring ICP content. ISPs would actively develop and maintain software for the acquisition, storage, and dissemination of monitoring, control, and surveillance data, taking into account the public's rights to data protection. Coordinating its monitoring efforts with INTERPOL's ICSE victim database should also facilitate the discovery of ICP victims. Law enforcers could exploit this information to block public access to websites with potential matches, integrating an extensive detection and monitoring approach to curb the crime of ICP.

CONCLUSION

England, Wales, and the US may have dedicated police units with specially trained officers and private specialists dealing with ICP such as CAID, IWF, and NCMEC. However, other countries such as Malaysia lack specialist units within their police forces. This inevitably means that the law cannot be effectively and efficiently enforced at the global level. It is commendable that RMP has now adopted ICACCOPS as an ICP online monitoring system. RMP and MCMC can now monitor the traffic of internet users by IP address on Malaysian internet servers, as well as identify duplicate images of child abuse and prevent their redistribution. These systems should be sufficiently agile to respond to the rapid pace of technological development. A continuous evaluation of Malaysia's regulatory responses should boost the capacity of MCMC and RMP to keep pace with developments on the internet and effectively detect, identify, and block ICP images. These initiatives demonstrate the government's paradigm shift in their perception of the severity of the ICP problem as well as a strengthened political will to ensure that children remain safe from the harms of ICP.

In reality, current levels of police resourcing and traditional policing techniques of arrest and seizure are inadequate to the task of combatting ICP crime. There is so much ICP content available that the police, despite these initiatives, cannot entirely stem its flow. In the complex, risky, and rapidly changing world of crime and technology, placing

total reliance on the traditional policing system is an inadequate policy approach. This is because it assumes that police and others in the criminal justice system have the competence to tackle the problems posed by ICP crime; the immediate causes of this inadequacy lie well beyond their resources or traditionally defined roles. The main challenges are posed by content distributed via the dark web, media streaming devices and encrypted email services. The increasing use of mobile devices to exchange ICP and the development of advanced and default encryption makes it more difficult to detect content and identify offenders. It is prudent to consider realigning the policing response of ICP images to other key intermediaries on the internet. This, it is envisaged, will alleviate some of the concerns surrounding the policing and institutional challenges in enforcing ICP law in Malaysia.

ACKNOWLEDGEMENT

The author thanks her PhD supervisors, Ms. Ann Sherlock and Dr. Brendan Coyle for their comments on the earlier draft of this manuscript. The author would also like to express her appreciation to Prof. Dr. Zuhairah Ariff Abd Ghadas for her invitation to submit this article.

REFERENCES

Adilah, A., & Dzulkifly, D. (2018, July 10). Experts laud new police system tracking child porn users. *Malay Mail*. Retrieved December 31, 2019, from https://www.malaymail.com/news/malaysia/2018/07/10/experts-laud-new-police-system-tracking-child-porn-users/1650523

Ananthalakshmi, A. (2016, November 14). Child sex abuse crimes 'going unpunished' in Malaysia. *Independent*. Retrieved December 31, 2019, from https://www.reuters.com/article/us-malaysia-sexcrimes-insight-idUSKBN1390AT?il=0

Armagh, D. S. (2001). Virtual child pornography: Criminal conduct or protected speech. *Cardozo Law Review*, *23*(6), 1993.

BBC News. (2001, February 13). *Wickedness of Wonderland.* Retrieved December 31, 2019, from http://news.bbc.co.uk/1/hi/uk/1167879.stm

Brown, J. (2017). *Online risk to children: Impact, protection and prevention*. Oxford, UK: John Wiley & Sons.

Child Act, 2001.

Communications and Multimedia Act, 1998.

Crawfurd, A. (2014, December 2). Child abuse image database containing millions of images to launch. *BBC News UK*. Retrieved December 31, 2019, from https://www.bbc.co.uk/news/technology-30175102

Data Protection Act, 2010.

Dewan Rakyat (House of Representatives). (2017). *April 3 Debate (Thirteenth Parliament, Fifth Session).* Retrieved December 31, 2019, from https://www.parlimen.gov.my/hansard-dewan-rakyat.html?uweb=dr&lang=en

DW News. (2013, November 7). *Dutch Activists Uncover Webcam Child Sex Tourists*. Retrieved December 31, 2019, from https://www.dw.com/en/dutch-activists-uncover-webcam-child-sex-tourists/a-17213042

European Commission Migration and Home Affairs. (n.d.). *Project Description: COSPOL Internet Related Child Abuse Material Project*. Retrieved December 31, 2019, from https://ec.europa.eu/homeaffairs/financing/fundings/projects/HOME_2010_ISEC_AG_INT-004_en

FBI Services. (2003). *Privacy Impact Assessment (PIA) Child Victim Identification Program (CVIP) Innocent Images National Initiative (IINI)*. Retrieved December 31, 2019, from https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/cvip

INTERPOL. (n.d.). *International Child Sexual Exploitation Database*. Retrieved December 31, 2019, from https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

Ireland's Raidió Teilifís Éireann (RTE). (2017, September 3). *US Sex Offender Groomed Children in Ireland.* Retrieved December 31, 2019, from https://www.rte.ie/news/2017/0910/903600-johnston-abuse

McIntyre, T. J. (2013). Child abuse images and cleanfeeds: assessing internet blocking systems. In Brown, I. (Ed.), *Research Handbook on Governance of the Internet*. Oxford, UK: Edward Elgar Publishing

Metcalf, C. (2008, March 13). Policing operation ore. *Criminal Justice Matters*, 68, 8-9. doi: 10.1080/09627250708553272

Nair, A. (2018). *The Regulation of Internet Pornography: Issues and Challenges*. Abingdon, UK: Routledge

New Straits Times. (2018, October 6). *Child Abuse: We are Not Doing Enough About It.* Retrieved December 31, 2019, from https://www.nst.com.my/news/exclusive/2018/10/418676/child-abuse-we-are-not-doing-enough-about-it

Penal Code, 1976.

R. v. Richard Huckle, 2016, London Central Criminal Court, Old Bailey (Unreported).

Sexual Offences Against Children Act, 2017.

The Straits Times Asia. (2018, January 30). *Malaysia Tops in South-east Asia for Online Child Pornography.* Retrieved December 31, 2019, from https://www.straitstimes.com/asia/se-asia/malaysia-tops-in-south-east-asia-for-online-child-pornography

The Straits Times. (2018, July 12). *MCMC Does Not Act on its Own in Combating Online Pornography - Gobind.* Retrieved December 31, 2019, from https://www.nst.com.my/news/nation/2018/07/390127/mcmc-does-not-act-its-own combating-online-pornography-gobind

Today Online. (2018, July 8). *New Malaysian Police Unit to Monitor Citizens Who Watch Pornography Online.* Retrieved December 31, 2019, from https://www.todayonline.com/world/new-malaysian-police-unit-monitor-citizens-who-watch-pornography-online

UK Department for Digital, Culture, Media & Sport and Home Office. (2019). Closed consultation. In J. Wright, & S. Javid, *Online Harms White Paper*. UK: APS Group. Retrieved December 31, 2019, from https://www.gov.uk/government/consultations/online-harms-white-paper

UK Internet Watch Foundation (IWF). (2018). *Annual Report*. Retrieved December 31, 2019, from https://www.iwf.org.uk/report/2018-annual-report

UK Prime Minister's Office. (2013). *News Story: Internet Safety Summit at Downing Street*: *Communique*. Retrieved December 31, 2019, from https://www.gov.uk/government/news/pm-hosts-internet-safety-summit

United Nations Human Rights Council. (2018). ECPAT Universal Periodic Review of the Human Rights Situation in Malaysia Submission. In End CSEC Network Malaysia & ECPAT International, *Sexual Exploitation of Children in Malaysia*. Geneva: OCHCR Publications. Retrieved December 31, 2019, from https://www.ecpat.org/wp-content/uploads/2018/07/Universal-Periodical-Review-Sexual-Exploitation-of-Children-Malaysia.pdf

United Nations Office on Drugs and Crime (UNODC). (2015). *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children*. Vienna, Austria: United Nations Office on Drugs and Crime. Retrieved December 31, 2019, from https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf

US Department of Justice. (n.d.). *National Strategy for Child Exploitation Prevention and Interdiction.* Retrieved December 31, 2019, from https://www.justice.gov/psc/national-strategy-child-exploitation-prevention-and-interdiction

US v. Blake Robert Johnston, 2017, Northern District of California (Unreported).

Vijaindren, A. & Sazili, S. (2018, July 10) Communications and Multimedia Ministry to combat child pornography. *News Straits Times*. Retrieved December 31, 2019, from https://www.nst.com.my/news/nation/2018/07/389324/communications-and-multimedia-ministry-combat-child-pornography

Wall, D. (2017). *Crime and deviance in cyberspace*. Abingdon, UK: Routledge

Wells, M., Finkelhor, D., Wolak, J., & Mitchell, K. J. (2007). Defining child pornography: Law enforcement dilemmas in investigations of Internet child pornography possession. *Police Practice and Research*, *8*(3), 269-282. https://doi.org/10.1080/15614260701450765

WePROTECT Global Alliance (End Child Sexual Exploitation Online). (2015). *Our Commitments: 15-16 November 2015.* Retrieved December 31, 2019, from https://www.weprotect.org/our-commitments