Online Sexual Grooming: A Critical Analysis on Section 4 of The Computer Misuse Act 2007 and Section 377g of The Brunei Penal Code 1957

Azilla Liyana binti Mohd Azam Zaki*

Abstract

The Brunei Computer Misuse Act 2007, Chapter 194 is a vital instrument in tackling cybercrime in the country. Section 4 of the respective Act allows punishment on any misusers of technology who access with intent to commit or facilitate commission of offence. This particular provision has been reiterated in a number of Bruneian computer related cases, usually associated with the Brunei Penal Code 1957, Chapter 22. In 2015, the provision on sexual grooming was imposed in reflection of the growing trend of this nature of offence, especially its commission through technology. Section 377G of the Brunei Penal Code was introduced to protect minors from adult sex predators. Although the purpose of this provision was to combat sexual grooming offences committed through technology, it does not specifically state on the technology aspect of the crime. Does this mean, like other conventional crimes, such as theft and fraud, the Brunei Computer Misuse Act will take place when a technology is involved in the commission of crime? This paper uses the doctrinal approach and has chosen Singapore for its comparative study. It seeks to examine the Brunei Computer Misuse Act 2007, Chapter 194 and the Singapore

* Masters of Laws (LL.M) student, Faculty of Shariah and Law, Universiti Islam Sultan Sharif Ali, Negara Brunei Darussalam. Email: liyana107@gmail.com

Computer Misuse Act 1993, Chapter 50A, the Brunei Penal Code 1957, Chapter 22 and the Singapore Penal Code 1871, Chapter 224, commentary judgments and principles, and whether Section 4 of the Brunei Computer Misuse Act can be imposed in a sexual grooming offence.

Keywords: Brunei Computer Misuse Act, computer, criminal law, cybercrime, Singapore Computer Misuse Act

Abstrak

Bab 194 di dalam Akta Penyalahgunaan Komputer Brunei 2007 merupakan perkara penting dalam menangani jenayah siber di negara ini. Bahagian 4 di dalam akta perundangan yang sama turut menyatakan tentang hukuman ke atas setiap perbuatan penyalahgunaan teknologi untuk akses dengan niat melakukan kesalahan. Peruntukan ini telah kerapkali digunapakai di dalam sejumlah kes yang berkaitan dengan perbuatan penyalahgunaan komputer Brunei, yang biasanya berkaitan dengan Kanun Hukuman Jenayah Brunei 1957, Bab 22. Pada tahun 2012, perbuatan seksual telah menunjukan peningkatan melalui teknologi. Manakala seksyen 377G dalam Kanun Keseksaan Brunei turut diperkenalkan akta khusus bagi melindungi kanak-kanak di bawah umur dari menjadi mangsa seksual. Walaupun tujuan peruntukan ini adalah untuk memerangi kesalahan perbuatan seksual yang dilakukan melalui teknologi, namun ianya tidak dinyatakan secara spesifik dari aspek teknologi tentang kesalahan tersebut. Adakah ini bermaksud, seperti jenayah konvensional yang lain sebagai contoh kecurian dan penipuan, Akta Penyalahgunaan Komputer Brunei akan

digunapakai apabila berlakunya kesalahan jenayah yang melibatkan teknologi? Dengan ini, saya menggunakan satu pendekatan doktrin / terperinci di dalam kajian saya dengan membuat perbandingan dengan negara luar iaitu Singapura. Tujuan perbandingan ini adalah untuk meneliti kesemua bab-bab yang digunapakai oleh kedua buah negara iaitu Bab 194 di dalam akta Penyalahgunaan Komputer Brunei 2007 dengan Bab 50A di dalam Akta Penyalahgunaan Komputer Singapura 1993 dan juga Bab 22 di dalam Kanun Hukuman Jenayah Brunei 1957 dengan Bab 224 di dalam Kanun Keseksaan Singapura 1871. Penelitian ini juga termasuk prinsip dan ulasan untuk menilai keberkesanan Seksyen 4 di dalam Akta Penyalahgunaan Komputer Brunei adakah ianya boleh disabitkan di dalam kesalahan serangan seksual.

Introduction

The Attorney General of Brunei, Dato Hairol Arni[138] indicated there will be measures taken to monitor the amendments to the cyberlaws as well as cybersecurity. This does not profess a new oath; a Cybersecurity Working Group established in 2015 has been running for almost five years. With the exponent advance of information communications technology (ICT) comes a rapid increase of the cybercrime.

[138] Yang Berhormat Dato Hj Hairol Arni Hj Abdul Majid, Attorney General of Brunei.

In 2017, at least 207 cybercrime cases were reported to the Royal Brunei Police Force.[139]

The Brunei Computer Misuse Act 2007, Chapter 194 ("BCMA") criminalizes the following offenses: unauthorized access to, and modification of computer material, access with intent to commit or facilitate commission of offence, unauthorized used or interception of computer service, unauthorized obstruction of use of computer, unauthorized disclosure of access code and refers to protected computers and law enforcement powers. Section 4 of the BCMA in particular has caught the researcher's attention as it is the provision that is most often used in Bruneian computer related cases. When a BCMA offence is committed, the offender is usually charged with another offence under the Brunei Penal Code 1957, Chapter 22 ("BPC"). With that said, does this mean that Section 4 of the BCMA is sufficient to be embedded in all types of criminal law?

In 2015, an amendment was made to the BPC to include an offence for sexual grooming under Section 377G. This particular clause was imposed in reflection of the ongrowing crime rate for child abuse, especially sexual grooming through the use of technology. Though the implementation of this provision was in view of the growing crime of sexual grooming, the technology aspect in commission of this particular crime was never cited in the provision. Thus, one

[139] Othman, A. (2017, November 29). Cybercrime of the rise, *Borneo Bulletin*, Retrieved from https://borneobulletin.com.bn/cybercrime-on-the-rise/

wonders whether Section 4 of the BCMA can be applied here. The aim of this paper is to discuss whether Section 4 of the BCMA is applicable in an offence of sexual grooming committed through technology. Bear in mind, that this paper only focuses on Section 4 of the BCMA and the Section 377G (sexual grooming) of the BPC.

In order to examine cybercrime legislation, doctrinal research has been used. Cybercrime legislations and literatures are examined to answer the above question. Here, the application of the legislations, the issues addressed, and the opinions from both the academia and the legislature can be explored. The materials accumulated from the previous research can contribute to identifying and analyzing the similarities and divergences among the approaches taken by the selected legal regimes. However, it must be noted that Brunei Magistrates cases are not accessible as they are not published. Thus, for the purpose of this paper, the researcher has referred to news articles as its main source for Brunei Magistrates cases. For a better understanding of cybercrime legislation, and to better contribute to the regulation of cybercrime, this paper has chosen two jurisdictions for its comparative study – Brunei and Singapore.

Singapore had made numerous and major significant changes to their cyber legislations in response to the growing and changing cybercrimes in the country. It is due to advanced technology that they have implemented and the exponent growing cybercrime rate that has pushed Singapore to consistently amend their laws. In making

legislative and judicial decisions, Brunei has always referred to Singapore legislations and law cases as guidance. Taking into account of the similarities in traditions, history, culture and society, the Singapore Computer Misuse Act 1993, Chapter 50A ("SCMA"), Singapore Penal Code 1871, Chapter 224 ("SPC"), cases, commentary judgments and principles will be referred to as a comparative study in this paper.

The paper is structured as follows: following the introduction, this paper explains the definition of cybercrime and computer. Part 3 has discussed the offence of using technology in a criminal offence, whilst part 4 dealt with the offence of sexual grooming under the BPC. Part 5 discussed on the application of section 4 of the BCMA into a sexual grooming offence and the proper sentence to impose on the technology aspect committed in a criminal offence. Finally, part 6 looked into its conclusion.

Definition of cybercrime and computer

Cybercrime is synonymous with the term "computer crime", "computer-related crime", "crime by computer", "high-technology crime", "technologically enabled crime", "virtual crime", "network crime" and "digital crime."[140] As the Internet began to play an increasing crucial role in the conducting of criminal activity, computer crime transformed into a cyber-version. Thus, the term 'cybercrime' was

[140] Wang, Q.Y. (2016). A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe, *Wolf Legal Publishers*.

developed to emphasise the role of the network in computer.[141] The definition of "computer" has been cited in the BCMA:

> an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include –
> *(a)* a similar device which is non-programmable or which does not contain any data storage facility; or
> *(b)* such other device as the Minister may, by notification in the Gazette, prescribe

The SCMA amended this clause to include "an automated typewriter or typesetter" and "a portable hand-held calculator" as devices which are not defined as "computer". Interestingly, Lee (1994) opined that "portable hand held

[141] Ibid.

calculator" is not clear. This is because this term could encompass "from the simplest of numerical calculators with only basic arithmetic functions to the most sophisticated scientific calculator with considerable memory capacity."[142] An 'express provision' rather than a statutory definition would have been preferable to determine a 'computer'.[143] Wang (2016) conjectured that judges can take some responsibility on interpreting and applying the existing provisions, provided that necessary guidance is present.[144]

In Brunei, this term has been broadly worded so as not to become obsolete with rapid technological change without fully adopting the definition of computer from the SCMA. The term that has been widely used in referring to the tool in the commission of the offence of cybercrime has been "computer", "information communications technology (ICT)"[145] and "social media".[146] Therefore, this paper has adopted 'computer' and 'technology (referring to information communications technology)' to describe the technology aspect in the commission of a criminal offence.

1. The offence of using technology in a criminal offence

Introduced in 2000 as an Order and enacted as an Act in 2007, the BCMA is significant in the prosecution of offences committed through computers. It is Brunei's principal

[142] Lee, G.M.C. (1994). Offences Created by the Computer Misuse Act 1993. *Singapore Journal of Legal Studies*. p 265
[143] Ibid.
[144] Wang. *A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe.*
[145] Othman. *Cybercrime on the rise.*
[146] Ibid.

legislative response to cybercrime. Its offence provisions are based primarily on the SCMA (before its amendments). Section 4 of the BCMA states as follows:

> "**4.** (1) Any person who causes a computer to perform any function for the purpose of securing access to any program or data held in a computer with intent to commit an offence to which this section applies is guilty of an offence."
>
> (2) This section applies to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years.
>
> (3) Any person guilty of an offence under this section is liable on conviction to a fine not exceeding $50,000, imprisonment for a term not exceeding 10 years or both.
>
> (4) For the purposes of this section, it is immaterial whether –
>
> *(a)* the access referred to in subsection (1) was authorised or unauthorised;
>
> *(b)* the offence to which this section applies was committed at the same time when the access was secure or at any other time."

This computer misuse provision that best applies to the use of counterfeit or forged cards in order to obtain unauthorized access to funds is section 4 of the BCMA.[147] Where the attempt to obtain funds succeeds, offenders may also face charges under the Penal Code for theft or other offences.[148] Thus, the BCMA is usually associated with the BPC.

The following cases illustrate the approach of Brunei and Singapore takes in relation to the punishment of misusing technology.

1.1. Brunei cases

a) Public Prosecutor vs Norhayati binti Hj Zaini (Criminal Trial No.9 of 2017)

The defendant was employed as an Assistant Manager at the Baiduri Bank Berhad Mall Branch and had been working in the respective place for 15 years. Thus, this renders her a senior role and pure trust amongst her colleagues. The defendant instructed several bank tellers to withdraw monies for her by logging into the bank tellers' computer in order to access the program held in the computer server of Baiduri Bank Berhad. The defendant also logged into the bank's computer server with a bank teller's ID and password, and input a debit of respective amount in order to effect a withdrawal of the monies from the said account. In total, the defendant misappropriated $84,928.90. The defendant, who was 'entrusted with the cash' as an Assistant Manager to the

[147] Urbas, G. (2008), An Overview of Cybercrime Legislation and Cases in Singapore, Working Paper Series No. 001*, Asian Law Institute.*
[148] Ibid.

bank, was charged for unauthorized access, abetting and breach of trust. The defendant was sentenced to 1 year and 6 months for breach of trust and 2 years for the charges under Section 4[149] and 10[150] of the BCMA with consideration of mitigations put forth; inordinate delay, absence of previous convictions and admittance to her wrongdoing. The court in *Norhayati* prefers to impose on custodial sentences rather than fine for the offence of the BCMA:

> For starters, in considering the appropriate sentence, the court as evidenced in numerous case authorities referred to by the prosecution views the offence of criminal breach of trust and offences committed under the Computer Misuse Act seriously. The sentences imposed should reflect the gravity of the offence committed. Except in very exceptional circumstances, the court's approach is to impose an immediate sentence of imprisonment.

b) Public Prosecutor vs Pathmanathan Jegan (Criminal Trial No. 7 of 2013)

The defendant, a 33 year old Sri Lankan National whom before his arrest resided in Indonesia, had used a counterfeit

[149] Section 4 of the BCMA Cap 194 states the access with intent to commit or facilitate commission of offence.
[150] Section 10 of the BCMA Cap 194 states the abetments and attempts punishable as offences.

Hong Kong Shanghai Bank (HSBC) card encoded to gain access to the program held within the Automated Teller Machines ("ATM") machine. Once securing access to the program, the defendant committed the theft of money. Further investigations also discovered that the defendant had used the counterfeit card to commit theft of money from both Standard Chartered and HSBC ATM machines. The defendant was charged with Section 4 of the BCMA and Section 379 of the BPC. The defendant admitted to committing the theft of money in total of $450. He further admitted that he knew that the card which he had used was counterfeit and had received the card and PIN number for ATM card criminal syndicate when he was in Indonesia. The court noted in particular of the greater number of charges taken into consideration as well as the larger amount involved, the nature of the offences and the role of the offender. The defendant was also part of a big syndicate ring operating in the region and against this backdrop, this constitutes, a relevant factor in sentencing.

1.2. Singapore cases

a) Public Prosecutor vs Law Aik Meng [2007] SGHC 33

The respondent is a male Malaysian national who was a member of an organized syndicate which is based in West Malaysia. The respondent's role was to plant the skimming devices at certain ATM in Singapore and then lie in wait in the vicinity. After the data from a sufficient number of ATM cards was captured, the respondent and his accomplices would remove the skimming devices and transport them to the syndicate in West Malaysia for the manufacture of cloned cards. The respondent and his accomplices were also

responsible for returning to Singapore to withdraw cash from various ATMs in Singapore with the cloned cards. The syndicate successfully withdrew a total of $18,590. For the charges of SCMA, the defendant was sentenced to 42 months' imprisonment. The judge in that case commented:

> "The damage cause here is decidedly widespread and multi-faceted: the prevalence of such offences will irreparably undermine public confidence in the security of ATM networks and compromise the integrity of the affected financial institution, tainting its reputation for security and secrecy. It will also translate to increased costs and efforts necessary to implement improved security measures. One only appreciates the full extent and impact of the harm in this case when it is viewed and measured in the context of Singapore's milieu as a secure and efficient financial and commercial hub. With regards to the second prong of seriousness, the respondent's culpability was by all accounts substantial. His participation in the scheme was hardly peripheral. His involvement with a criminal syndicate, his central role in the criminal scheme, the premeditation and planning that preceded the

> operation all constitute relevant factors exacerbating his culpability."[151]

b) Navaseelan Balasingham vs Public Prosecutor [2006] SGHC 228

The appellant, a 29-year-old male British national, arrived in Singapore on 28th February 2006 on a 14-day social visit pass. A bank officer working at the United Overseas Bank ("UOB") branch in Novena Square was alerted by his colleagues from the UOB Card Centre that the bank's ATM was being operated fraudulently. He detained the appellant and called the police. When the police arrived, they searched the appellant and found 22 ATM cards, believed to be counterfeit ones, on him. The appellant was arrested and charged under Section 4 of the SCMA for causing ATMs to access data held in the central computer systems of the UOB with the intention to commit theft of money, and five charges under Section 379 of the SPC for theft of money from UOB through the above unauthorized transactions. In total, the defendant was sentenced to 5.5 years imprisonment. The severity of the offence is that it is committed fast paced whilst being undetected, thus resulting in a huge loss to the victim and the institution. The court in *Navaseelan* commented:

> "… there can be little doubt that the sinister tentacles of a syndicate are involved. Consider the rapidity of commencement of operations upon the appellant's touchdown in

[151] [2007] SGHC 33, para 33.

> Singapore, the seeming speed and ease with which he moved from ATM to ATM from the east to the central to the west of Singapore – and this coming from a first-time visitor to this country – and the urgency of withdrawals, some occurring even between 2 and 4am. It was as if the appellant has an ATM tour itinerary which he had to complete within his short stay here.
>
> Considering the speed and the persistence of the transactions, if he had no been apprehended through the quick action of the bank's officials, I think he was most likely to have gone on to hit other ATMs and then quietly disappear from our shores together with the cash pile. The appellant was definitely not an innocent, lonely tourist suddenly tempted by the mystery man "Kumar". He was here in Singapore on a mission – the mission was to raid as many ATMs as he could before any alarm was raised. Even if his face was captured by the ATMs' security cameras, and indeed, he had to put on a cap to try to conceal his face, it would take the investigators some time to track him down as he is a foreigner here, by which time he would already have a made a clean and easy exit and returned home, or

perhaps, moved on to his next ATM "El Dorado"."[152]

2. The offence of sexual grooming under the Brunei Penal Code

The BPC and the SPC set out the general principles of the criminal law in their respective countries. In a cybercrime case, the Penal Code takes place in the act of a cybercrime when it violates criminal law. Jiow (2015) described this as an "old crime (for example, theft)" committed through a "new crime (for example, hacking)."[153] Thus, the commission of an offence under the BCMA usually comes with a commission of an offence under the BPC. For the purpose of this paper, the researcher focuses on the offence of sexual grooming in the BPC.

2.1. Definition of sexual grooming

Sexual grooming has been described as a "process by which a person prepares a child, significant adults and the environment for the abused of this child".[154] Grooming, therefore, involves a careful process of seduction and manipulation, often through a non-sexual approach, aimed at

[152] [2006] SGHC 228, para 37.
[153] Jiow, H.J. (2013). Singapore's Cybercrime Regulation based on Lessig's Modalities of Constraint, Working Paper No. 179.
[154] Craven, S., Brown, S. & Gilchrist, E. (2006). Sexual Grooming of Children: Review of Literature and Theoretical Considerations, *Journal of Sexual Aggression,* p 297.

enticing a child into a sexual encounter.[155] Mohan and Lee (2020) opined that the ultimate objective of the groomer is to create a bond with the victim who is then more likely to comply with his or her wishes.[156]

O'Connell (2013) has identified seven stages in this process.[157] These are the friendship-forming stage, the relationship forming-stage, risk assessment stage, exclusivity stage, sexual stage, fantasy re-enactment stage and the damage limitation stage.[158] Until the sexual stage is reached, there might be insufficient evidence to warrant an arrest and conviction for a sexual offence.[159] O'Connell (2013) also suggests that by the time sexual stage is reached, there is rapid progression towards the commission of the offence and the child needs immediate protection.[160]

[155] Berson, I. (2008). Grooming Cybervictims: The Psychosocial Effects of Online Exploitation for Youth, *Journal of School Violence,* p 11
[156] Mohan, S.C., Lee, Y. (2020) Sexual grooming as an offence in Singapore, *Singapore Academy of Law (e-First)*, para 1
[157] O'Connell, R. (2013, July). A Typology of Child Cyberexploitation and Online Grooming Practices. Retrieved from http://image.guardian.co.uk/sys-files/Society/documents/2003/07/17/Groomingreport.pdf
[158] Ibid.
[159] Ibid.
[160] Ibid.

2.2. Statutory provisions

As mentioned, in reflecting the growing trend of cybercrime in Brunei, an offence of sexual grooming was imposed in 2015 under Section 377G of the BPC as follows:

> **Sexual grooming of minor under 16**
> (1) Whoever is of or above the age of 21 years (A) if having met or communicated with another person (B) on 2 or more previous occasions -
> (a) An intentionally meets B or travels with the intention of meeting B; and
> (b) At the time of the acts referred to in paragraph (a) -
> (i) A intends to do anything to or in respect of B, during or after the meeting, which if done will involve the commission by A of a relevant offence;
> (ii) B is under 16 years of age; and
> (iii) A does not reasonably believe that B is of or above the age of 16 years,
> Shall be punished with imprisonment for a term not exceeding 3 years, fine or both.

In 2007, the SPC has been amended to include an offence of child grooming[161] as well. In May 2019, the SPC provision has been amended again as follows:

[161] See Section 376E of the Singapore Penal Code, Chapter 50A.

> **376E. –** (1) Any person of or above the age of 18 years (A) shall be guilty of an offence if having met or communicated with another person (B) on at least one previous occasion –
>
> (a) A intentionally meets B or travels with the intention of meeting B or B travels to attend a meeting with A which A has either initiated or agreed to whether expressly or by implication; and
>
> (b) At the time of the acts referred to in paragraph (*a*) –
>
> (i) A intends to do anything to or in respect of B, during or after the meeting, which if done will involve the commission by A of a relevant offence;
>
> (ii) B is under 16 years of age; and
>
> (iii) A does not reasonably believe that B is of or above the age of 16 years.

Based on the section 15 of the UK's Sexual Offences Act 2003,[162] the provision applies to all persons in Singapore who is over 18 years. Prior to the amendments, the SPC provision stated that the offender should be 21 years old and have met up with the victim twice. However, this was then reduced from two to one as this "will also allow the Police to intervene at an even earlier stage to protect minors from

[162] The UK Sexual Offences Act 2003's threshold is 18 years.

predatory offenders"[163] and that the *content* of the communication matters more than the *frequency*[164]. In *R v Mansfield,*[165] the court stated that the provision served to protect young girls "against their own immature sexual experimentation and to punish much older men who take advantage of them."

In order for the law enforcement authorities to intervene before a child is physically assaulted, the Second Reading Speech of this clause noted:

> In practice, what this offence does is to allow law enforcement authorities to step in when for example, a child receives sexually suggestive communications over the Internet, or a child is seen being met by a stranger in suspicious circumstances. That law enforcement authorities can now intervene at an earlier stage would be sufficient to send a chilling effect on would-be sex predators. Besides being a deterrent, those who persist will be apprehended more easily.

The 2019 amendments also included exploitative sexual grooming of minor of or above 16 but below 18 years of age (Section 376EA), sexual communication with minor below 16 years of age (376EB) and exploitative sexual

[163] Ministry of Home Affairs and Ministry of Law, Penal Code Review Committee, Report (August 2018), p 120.
[164] Mohan. *Sexual grooming as an offence in Singapore*, para 43.
[165] [2005] All ER (D) 195.

communication with minor of or above 16 but below 18 years of age (376EC).

2.3. Brunei cases

a) Public Prosecutor vs Mohammad Shahdon Mohammad Ramlee (2015)[166]

The defendant, a 28-year-old man, was charged under this clause where defendant pleaded guilty to two counts of sexually grooming on two young boys aged 15 years old. The man posed as a teenage girl and pretended to make friends with the two boys. These boys were persuaded to send nude photographs of themselves to this 'girl'. The defendant then posed himself as the elder brother of this 'girl' and threatened the male victims to spread their nude photos on social media. The court sentenced the defendant to nine-year imprisonment and six strokes.

b) Public Prosecutor vs Alias bin Rosli (2010)[167]

The defendant asked for kisses from the victim and sent the victim 'emoticons' which contained sexual connotations.

---

[166] Anonymous. (2015, July 2). *Man pleads guilty 18 counts sex offences minors*. Borneo Bulletin. Retrieved from: https://btarchive.org/news/national/2015/07/02/man-pleads-guilty-18-counts-sex-offences-minors

[167] Faisal, F. (2017, October 19). *Local man jailed for sexual grooming autistic boy*. Borneo Bulletin. Retrieved from: https://borneobulletin.com.bn/local-man-jailed-for-sexually-grooming-autistic-boy/page/9197/

Further, the defendant suggested to meet up with the victim to perform the lewd act. A custodial sentence of four months was imposed on the defendant for his lewd text messages to an autistic child for the offence of sexual grooming.

2.4. Singapore cases

a) Public Prosecutor vs Lee Seow Peng (2016) SGHC 2017

The defendant, a 36 year old man, became acquainted with the victim, a 13 year old girl, through a mobile phone application, Whatsapp. They exchanged numerous SMS and Whatsapp messages for three months, where they also exchange photographs of themselves and on sexual matters. The defendant was charged with sexual grooming and was sentenced to one year of imprisonment. It is interesting to note the judge's comments on corroborative evidence:

> "I had relied not only on the Complainant's evidence, but also on the strong corroborative evidence in the form of the numerous messages, especially those emanating from the Accused, the most significant of which were set out earlier."

3. Application of section 4 of the BCMA into a sexual grooming offence

Looking as a whole, Section 4 of the both BCMA is applicable in cases of theft and fraud (as demonstrated above). However, seeing that sexual grooming usually takes

place with the use of technology, one wonders whether Section 4 of the BCMA is applied here too. The amendments made in 2015 in the BPC included sexual grooming was in response to the exponent crimes related to the use of technology in Brunei and the growing trend of how sexual grooming is committed in the recent years. Although the BPC charges those who commit this offence under the respective Act, the element of utilising the computer or technology in the provision is missing.

Does this mean that this particular provision connotes to a sufficient, vigorous and resilient safeguard against the predators who commit such offence through the use of technology? The Criminal Justice Division from the Attorney General Chambers does not think so.[168] Ayswariya and Rajan (2018) opined that any conventional crime committed through the use of computer or electronic devices should render a higher penalty than a traditional crime.[169] The sexual grooming provision was made in order to keep up with the ongrowing conventional crime rates, which does not neccessarily mean committed through the use of computer or other technology. Hence, this means that its

[168] The researcher interviewed an officer of the Criminal Justice Division of the Attorney General's Chambers during the researcher's work attachment programme in February 2019. The officer opined that more should be done to accommodate the rising cases of cybercrime.

[169] Ayswariya, G. K. and Rajan, A. (2018). A Comparative Study on the Difference Between Conventional Crime and Cyber Crime, *International Journal of Pure and Applied Mathematics,* 119(17). Retrieved from https://acadpubl.eu/hub/2018-119-17/2/120.pdf

application is very generic. Here, the action of the stranger predator based 'online' is being evaluated and viewed as similar as 'offline'. A custodial sentence was imposed on *Alias Bin Rosli*[170] for his lewd text messages to an autistic child for the charge of sexual grooming. Thus, this same sentence may be imposed to a case where the offence was not perpetrated through the use of technology and that a commission of sexual grooming with or without technology aspect may render the same punishment. The wide and easy, yet insecured access of technology from the online predators to the innocent party is crucial and that it will bring more harm than the offline predators.

Further, in *PP vs Lee Seow Peng*, the court cites the five elements to sexual grooming (before the 2019 amendments) as follows:

1. The accused should be of or above 21 years old, and must have communicated with the victim on two or more previous occasions;
2. The accused must then have intentionally met the victim;
3. At the time of meeting the victim, the victim must be under 16 years of age;
4. The accused must have intended to do something to the victim, during or after the meeting, which if done would amount to the commission of

[170] Faisal. *Local man jailed for sexual grooming autistic boy.*

any of the relevant offences defined in s376E(2) of the Penal Code; and

5. The accused must not reasonably believe that the victim was of or above the age of 16 years.

It is clear that there are no references to the technology aspect when it comes to sexual grooming offence although the court considered it as an aggravating factor:

> [t]he accused used mobile technology to facilitate the commission of the offences. The prevalence of mobile technology in the present day and age provides fertile ground for exploitation and abuse. There is a need to protect the young from such exploitation and abuse.

The Singapore High Court in this case only viewed "the message trail on SMS and Whatsapp as evidence of communication and the sexually explicit communication as demonstrating the accused's clear intention of having sexual intercourse with the victim."[171] Hence, will the application of Section 4 be sufficient to warrant a sentence on the technology aspect in the commission of sexual grooming?

[171] Public Prosecutor vs Lee Seow Peng (2016) SGHC 2017.

Observing Section 4 of BCMA, this provision only allows any person who causes a computer to perform any function for the purpose of securing access to any program or data held in a computer with intent to commit an offence. This was further elaborated that this only applies to offence involving property, fraud, dishonesty or which causes bodily harm. On a deep introspection, this provision only focuses on the aspect of accessing a program or data for the purpose of commission of the Penal offences. Rather, this provision is leaning more towards of obtaining information to commit the mentioned offences. In hindsight, it would be difficult to impose this clause onto a sexual grooming charge. Observing the technics of a sexual groomer in utilising technology to commit the offence, often than not, the offender would communicate directly with his victim. With that said, Section 4 is inapplicable in sexual grooming offence.

However, this does not mean that the sexual grooming provision is redundant on its technology aspect. Interestingly, the court in *Norin bin Pungut/ Yussof vs Public Prosecutor* (Criminal Appeal No. 16 of 2016) viewed that this provision is more suitable in cases where the communication between the perpetrator and the victim were conducted through technology:

> It seems to us that it is extremely unlikely that the legislature ever contemplated a resort to that section whether the two people concerned live and constantly meet in the same dwelling. **It is more suitable to deal**

> **with circumstances where strangers communicate on social media** and one of them is a sexual predator who arranges a meeting with the underage victim with the intention of having sexual intercourse. [emphasis added]

This is to say, the legislative intent for the implementation of this provision was leaning more towards communications conducted through the use of technology, although it can be applied to both situations - "online" and "offline".

In the UK, before the amendment, the principal offences were those of *attempt*, and that offender had to go beyond acts of mere preparation to the substantive sexual offence to satisfy the elements of the offence.[172] In Mohan and Lee (2020), they noted that "the amendment hence covered situations where *an adult establish contact with a child, either through meetings, telephone conversations or internet communications, all with the intention of gaining the child's trust and confidence in order to meet the child to commit a sexual offence against him or her.*"[173] The meetings and communication need not necessarily have explicit sexual content although the intent to commit sexual offence must be proved. According to the Explanatory Notes to the UK Act:

---

[172] Mohan. *Sexual grooming as an offence in Singapore*. para 14-15.
[173] Ibid.

> The offence will be complete either when A meets the child or when he travels to the prearranged meeting with the intent to commit a relevant offence against the child. The planned offence does not have to take place. The evidence of the intent may be drawn from communications between A and the child before the meeting or may be drawn from other circumstances, for example A travels to the meeting with ropes, condoms and lubricants. [emphasis added]

Thus, it is clear that the technology aspect does not have to be necessarily stated in the provision as the intent of the legislature for this offence encompassed any kind of communications – whether online or offline.

3.1. Sentencing for technology aspect in a criminal offence

3.1.1. Relevant sentencing considerations

When it comes to the technology aspect of a sexual grooming offence, no cases have cited on the factors that the court need to consider to warrant a sentence for a sexual grooming offence committed through technology. However, under the computer misuse offences, there are cases where factors must be considered to warrant a proper sentence.

In *Navaseelan*, the judge fixed the benchmarks at six months' imprisonment for each charge under Section 379 of the SPC and 18 months imprisonment for each charge under

Section 4 of the SCMA. In his sentencing judgment, the judge referred to cases relating to the intrinsic nature and severity of the appellant's computer crimes warranting a deterrent sentence. The judge relied on *Public Prosecutor v Ooi Lye Guan,*[174] a case involving offences committed under subsection 4 and 5 of the SCMA. In that case, the court observed:

> In my opinion, the relevant factors that would determine the appropriate length of the custodial term would include (i) that nature and seriousness of the offences perpetrated whilst abusing the computer technology (ii) the level of pre-meditation and sophistication involved, namely, whether it is an one-off incident committed out of boredom or curiousity or whether it is a persistent course of conduct (iii) whether the offender had abused his position of trust in committing these offences as well as the quality and degree of trust reposed in the offender (iv) the extent of the harm or damage caused, the potential mischief occasioned or the amount of the inconvenience entailed in establishing the extent of the intrusion (v) his personal mitigating factors and (vi) whether the offending acts have a significant impact on

[174] [2005] SGDC 228: the offender was a support engineer who exploited a loop hole in the computer system and made $94,000. He was sentenced to a total of 42 months.

> public confidence in the use of the computer technology or computer system in that particular form or generally in our society.

These factors were reiterated in the case of *Law Aik Meng*, following the case of *Public Prosecutor vs Fernando Payagala Waduge Malitha Kumar.*[175] The court highlighted the important and relevant consideration is the 'international dimension' involved:

> The respondent has been part of a foreign syndicate which had systematically targeted financial institutions in Singapore to carry out its criminal activities. The audacity and daring of such a cross-border criminal scheme must be unequivocally deplored and denounced. There is a resounding and pressing need to take a firm stand against each and every cross-border crime, not least because the prospect of apprehending such foreign criminals presents an uphill and, in some cases, near impossible task.

3.1.2. Custodial or non-custodial

In some cases, the offences against vulnerable victims create deep judicial disquiet and general deterrence. These must necessarily constitute an important consideration in the sentencing of perpetrators. In *PP v NF,*[176] the court stated:

[175] [2007] SGHC 23.
[176] [2006] 4 SLR 849.

> …[O]ur courts would be grievously remiss if they did not send an unequivocal and uncompromising message to all would-be sex offenders that abusing a relationship or a position of authority in order to gratify sexual impulse will inevitably be met with the harshest penal consequences. In such cases, the sentencing principle of general deterrence must figure prominently and be unmistakably reflected in the sentencing equation.

In explaining the need for deterrence in the area of computer crime, the judge in *Navaseelan* stated:

> An offence under Section 4 of the Computer Misuse Act (SCMA) is undoubtedly a very serious crime. That gravity of the offence is reflected by the maximum prescribed punishment – up to 10 years' imprisonment and a fine not exceeding $50,000. In terms of severity, the prescribed punishment for a section 4 offence ranks second on to that of section 9 (the latter provides for enhance punishment for offences involving 'protected computers').

During the second reading of the Computer Misuse (Amendment) Bill on 30 June 1998, the Minister noted that:

> … crimes committed through the electronic medium and through use of computers are difficult to detect but they are just as serious as traditional crimes and we must equally protect our population against such crimes. To ensure that Singapore remains an attractive place for investors and businesses to operate effectively and securely, computer crimes must be treated as other criminal offence.

Thus, the Singaporean court is of the view that a custodial sentence would be preferable for an offence related to computer or technology. It is fundamental to note that the Bruneian courts have followed the benchmark tariffs fixed by the Singaporean court for CMA cases. The Bruneian Court in the case of *Norhayati*[177] prefers to impose on custodial sentences rather than a fine for the offence of the BCMA. The Court considered the factors whilst referring to the case of *R v Barrick [1958]* where the repetition of such committal acts renders a custodial sentence. High degree of planning and premeditation renders a deterrent sentence.[178] Other factors that warrant imprisonment include unauthorized withdrawals within a short period of time, involvement of a criminal syndicate which used sophisticated methods to obtain confidential data and PIN numbers. The Judge in *Pathmanathan*, following the

[177] Public Prosecutor v Norhayati Binti Hj Zaini (Criminal Trial No. 9 of 2017) pg 5.

[178] Urbas. *An Overview of Cybercrime Legislation and Cases in Singapore.*

benchmark tariffs set by *Navaseelan*[179], came to the view that a minimum of 24 months is appropriate for a syndicate offence.

However, the opinion of the Court in *Law Aik Meng* emphasized that while foreign authorities are helpful in clarifying the relevant sentencing principles in connection with a particular offence, the precise quantum relating to sentences imposed by foreign courts cannot afford an appropriate guide or benchmark for sentencing by our court.[180]

For the reasons above, should one consider the technology aspect of sexual grooming, the factors put forth in the *Ooi Lye Guan* may be referred as a guideline. Although these factors were pronounced for the charges under the SCMA, but these factors are not oblique and can be referred to for the purpose of evaluating the technology aspect in a sexual grooming case. In doing so, it could act as a model and

[179] In *Navaseelan*, the court came to the view that for syndicated offence under section 4 of the Computer Misuse Act which involved the use of a counterfeit ATM card to commit theft of money, a sentencing range between 12 to 24 months would not be out of order.

[180] The court followed the rule established by court in Chia Kim Hem Fredeirick v PP [1992] 1 SLR 361 Yong CJ un equivocally declared that because the approach towards sentencing is governed by the objective in inflicting punishment, which in turn reflects the social environment in a country, it would not be appropriate for a court in Singapore to follow completely the approach and practice followed by English courts in sentences for imprisonment.

guideline to improve on our own benchmark for sexual grooming offences.

Conclusion

The Attorney General Chamber's renewal of commitment 2019 shows its determination in curbing this growing menace. There is no doubt that this issue is inevitable as the country is willing to become an international player in the ICT field and be at the same level as other progressing countries. The ICT world is complex to comprehend as it innovates every second, but like any other previous worldly issues, it is not impossible to overcome.

This paper has discussed on Section 4 of the BCMA and its applicability in a sexual grooming offence. In hindsight, the scope in Section 4 is limited and cannot be used in a sexual grooming charge. Although Section 377G is silent on the aspect of technology, both Bruneian and Singaporean courts have found that this provision is leaning more towards the commission of the sexual grooming offence through technology. The legislative intent for the implementation of this provision was for both online and offline circumstances. However, the factors laid down by the court in *PP v Ooi Lye Guan* can be guidance to assess the technology aspect in a sexual grooming offence. The courts in Brunei and Singapore has also found and preferred a custodial sentence for the protection of children against sexual grooming.

In conclusion, this paper has put forward the gap and the potential key areas for the advancement of Brunei's cyber

legislations. Legislators and academia must be aware of the fast-changing crimes committed through the use of computers and technology. Conventional crimes are now committed through cyber and due to its accessibility, commission of crimes can be easily be done.

References

Cases

Navaseelan Balasingham vs Public Prosecutor [2006] SGHC 228
Norin bin Pungut/Yussof vs Public Prosecutor (Criminal Appeal No. 16 of 2016)
Public Prosecutor vs Alias Bin Rosli (2010)
Public Prosecutor vs Fernando Payagala Waduge Malitha Kumar [2007] SGHC 23
Public Prosecutor vs Law Aik Meng [2007] SGHC 33
Public Prosecutor vs Lee Seow Peng (2016) SGHC 2017
Public Prosecutor vs Mohammad Shahdon Mohammad Ramlee (2015)
Public Prosecutor vs Norhayati Binti Hj Zaini (Criminal Trial No.9 of 2017)
Public Prosecutor vs NF [2006] 4 SLR 849
Public Prosecutor vs Ooi Lye Guan [2005] SGHC 228
Public Prosecutor vs Pathmanathan Jegan (Criminal Trial No. 7 of 2013)
R v Mansfield [2005] All ER(D) 195

Journal Articles
Ayswariya, G. K. and Rajan, A., A Comparative Study on the Difference Between Conventional Crime and Cyber Crime, International Journal of Pure and Applied Mathematics, Volume 119 No. 17 2018, 1451-1464 ISSN: 1314-3395
Berson, E., "Grooming Cybervictims: The Psychosocial Effects of Online Exploitation for Youth" (2008) 2(1) *Journal of School Violence* 9 at 11
Craven, S., Brown, S. & Gilchrist, E., "Sexual Grooming of Children: Review of Literature and Theoretical Considerations" (2006) 12(3) *Journal of Sexual Aggression* 287
Mohan, S.C. and Lee, Y., Sexual Grooming As An Offence in Singapore, Singapore Academy of Law (e-First).
O'Connell, R., "A Typology of Child Cyberexploitation and Online Grooming Practices" (July 2013)
Lee, G.M.C. Offences Created by the Computer Misuse Act 1993. *Singapore Journal of Legal Studies*

Legislations
Brunei
Computer Misuse Act 2007, Chapter 194
Penal Code 1957, Chapter 22

Singapore
Computer Misuse Act 1993, Chapter 50A
Penal Code 1871, Chapter 224

United Kingdom
Computer Misuse Act 1990

Sexual Offences Act 2003

Reports

Ministry of Home Affairs and Ministry of Law, Penal Code Review Committee, Report (August 2018)

Books

Wang, Q.Y. (2016), A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe.

Websites

Brunei Times Archive, https://btarchive.org/news/national/2015/07/02/man-pleads-guilty-18-counts-sex-offences-minors

Faisal, F. (2017, October 19). *Local man jailed for sexual grooming autistic boy*. Borneo Bulletin. Retrieved from https://borneobulletin.com.bn/local-man-jailed-for-sexually-grooming-autistic-boy/page/9197/

First Cybercrime Conviction Brunei, https://news.hitb.org/content/first-cybercrime-conviction-brunei

Othman, A. (2017, November 29). Cybercrime on the rise, *Borneo Bulletin*, Retrieved from: https://borneobulletin.com.bn/cybercrime-on-the-rise/

Working Papers

Jiow, H.J. (2015). Singapore's Cybercrime Regulation based on Lessig's Modalities of Constraint, Working Paper No. 179

Urbas, G. (2008) An Overview of Cybercrime Legislation and Cases in Singapore, Working Paper Series No. 001, Asian Law Institute