ASLI
Asian Law Institute
Working Paper Series No. 001

An Overview of Cybercrime Legislation and Cases in Singapore

Gregor Urbas
ANU College of Law, Australian National University, Australia
urbasg@law.anu.edu.au

ASLI Visiting Fellow
(13 September to 13 October 2008)

December 2008

The **ASLI Working Paper Series** is published electronically by the Asia Law Institute, whose Secretariat is based at the Faculty of Law, National University of Singapore.

© Copyright is held by the author or authors of each Working Paper. ASLI Working Papers cannot be republished, reprinted, or reproduced in any format without the permission of the paper's author or authors.

Note: The views expressed in each paper are those of the author or authors of the paper. They do not necessarily represent or reflect the views of the Asia Law Institute or of the National University of Singapore.

Citations of this electronic publication should be made in the following manner: Author, "Title," ASLI Working Paper, No. #, Date, www.law.nus.sg/asli/pub/wps.htm. For instance, Chan, Bala, "A Legal History of Asia," ASLI Working Paper, No. 101, December 2009, www.law.nus.sg/asli/pub/wps.htm.

Asia Law Institute
c/o Faculty of Law,
National University of Singapore
Eu Tong Sen Building
469G Bukit Timah Road,
Singapore 259776
Tel: (65) 6516 7499
Fax: (65) 6779 0979
Website: http://law.nus.edu.sg/asli
Email: asli@nus.edu.sg

The Asian Law Institute (ASLI) was established in March 2003 by a group of leading law schools in Asia. Its goal is to facilitate academic exchanges as well as research and teaching collaboration among colleagues from the thirteen founding institutions. The establishment of ASLI stems from the recognition that the diversity of legal traditions in Asia creates an imperative for Asian legal scholars to foster greater engagement with each other through collaborative research and teaching. The acronym "ASLI", which means "indigenous" in the Malay and Indonesian languages, represents the commitment of the founding institutions to establish a truly home-grown law institute in Asia. The ASLI membership has grown beyond the founding members and includes 27 new member institutions.

AN OVERVIEW OF CYBERCRIME LEGISLATION AND CASES IN SINGAPORE

GREGOR **URBAS***

I. LEGISLATION

As with other jurisdictions in the Asia-Pacific region and around the world, Singapore has a number of statutes that apply to criminal misuse of computers and computer-related technology such as the Internet.[1]

A. *Computer Misuse Act*

Introduced in 1993, the *Computer Misuse Act*[2] (the '*CMA*') is Singapore's principal legislative response to cybercrime.[3] Its offence provisions are based primarily on the United Kingdom's (UK's) 1990 legislation of the same name, but there are some divergences. For example, the definitions used in the Singapore statute (section 2, Interpretation) also draw on the *Criminal Law Amendment Act 1985* of Canada,[4] and the *Evidence Act 1929* of South Australia.

1. *Definitions*

Section 2 of the *CMA* contains definitions including the following:

> "computer" means 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) an automated typewriter or typesetter;

---

* BA(Hons), LLB(Hons), PhD, Senior Lecturer in Law, ANU College of Law, Australian National University (ANU). This working paper was written while the author was an Asian Law Institute (ASLI) Visiting Fellow based at the Law Faculty of the National University of Singapore (NUS) during September / October 2008. The support and kind hospitality of the staff of ASLI and NUS are gratefully acknowledged. Any errors, omissions or inaccuracies are the responsibility of the author.

1 See Gregor Urbas, "Cybercrime Legislation in the Asia-Pacific Region" in R.G. Broadhurst & P.N. Grabosky, eds., *Cyber Crime: The Challenge in Asia* (Hong Kong: Hong Kong University Press, 2005), at Chapter 12: pp. 207 – 241; Russell Smith, Peter Grabosky and Gregor Urbas, *Cyber Criminals on Trial* (Cambridge: Cambridge University Press, 2004).

2 Cap. 50A, Rev. Ed. 2007, Sing.

3 First Reading, 18 March 1993; Second and Third Readings, 28 May 2003; Date of commencement, 30 August 1993. The *Computer Misuse Act* has been amended several times since its enactment, most notably by the *Evidence (Amendment) Act 1996* (No. 8 of 1996), the Computer Misuse (Amendment) Act 1998 (No. 21 of 1998), Computer Misuse (Amendment) Act 2003 (No. 25 of 2003) and the Statutes (Miscellaneous Amendments) (No. 2) Act 2005 (No. 42 of 2005).

4 *Criminal Law Amendment Act*, R.S.C. 1985, c. 19

(b) a portable hand-held calculator;

(c) a similar device which is non-programmable or which does not contain any data storage facility; or

(d) such other device as the Minister may, by notification in the *Gazette*, prescribe;

“computer output” or “output”means a statement or representation (whether in written, printed, pictorial, graphical or other form) purporting to be a statement or representation of fact —

(a) produced by a computer; or

(b) accurately translated from a statement or representation so produced;

"computer service" includes computer time, data processing and the storage or retrieval of data;

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer;

"electro-magnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer;

"function" includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer;

"intercept", in relation to a function of a computer, includes listening to or recording a function of a computer, or acquiring the substance, meaning or purport thereof;

"program or computer program" means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function.

These definitions help to clarify the application of the statute to different forms of digital technology. In general, such definitions are broadly worded so as not to become obsolete with rapid technological change.

2. *Offence Provisions*

Singapore’s *CMA* has a number of offence provisions that apply both to unauthorised and authorised uses of computers:

Unauthorised access to computer material
3. —(1) Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the act in question is not directed at –

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

Access with intent to commit or facilitate commission of offence

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 any computer with intent to commit an offence to which this section applies shall be guilty of an offence.

(2) This section shall apply 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 shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both.

(4) For the purposes of this section, it is immaterial whether —

(a) the access referred to in subsection (1) is authorised or unauthorised;

(b) the offence to which this section applies is committed at the same time when the access is secured or at any other time.

Unauthorised modification of computer material

5. —(1) Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the act in question is not directed at –

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

(4) For the purposes of this section, it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary.

It is noteworthy that sections 3 and 5 require unauthorised access or modification, while section 4 does not, which makes this offence a broadly applicable "preparatory" style of offence which can be used where the a computer use involved is done with intention to commit a further offence of the kinds specified.[5]

A variant of the unauthorised access / modification offences applies also to unauthorised use or interception of computer services:[6]

> **Unauthorised use or interception of computer service**
> **6.** —(1) Subject to subsection (2), any person who knowingly —
>
> (a) secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service;
>
> (b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electro-magnetic, acoustic, mechanical or other device; or
>
> (c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (*a*) or (*b*),
>
> shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.
>
> (2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.
>
> (3) For the purposes of this section, it is immaterial that the unauthorised access or interception is not directed at —
>
> (a) any particular program or data;
>
> (b) a program or data of any kind; or
>
> (c) a program or data held in any particular computer.

Sections 7 and 8 deal with unauthorised obstruction of the use of computers, and unauthorised disclosure of access codes:

---

[5] The CMA, s. 4, offence may be contrasted with a similar offence in s. 474.14 of the *Criminal Code Act 1995* (Cth) in Australia: using a telecommunications network with intention to commit a serious offence, which was introduced by the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act 2004 (No.2)* (Cth) with effect from 1 March 2005. Unlike the CMA offence, the Australian version extends to intention to commit or facilitate any serious Commonwealth, State, Territory or even foreign offence, defined as one punishable by 5 years or more. There is no limitation to particular categories of intended offence.

[6] Unlike the preceding offence provisions, s. 6 is based on Canadian legislation, namely s. 301.2 (1) of the *Criminal Law Amendment Act*, *supra* note 4.

Unauthorised obstruction of use of computer
7. —(1) Any person who, knowingly and without authority or lawful excuse —

(a) interferes with, or interrupts or obstructs the lawful use of, a computer; or

(b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

Unauthorised disclosure of access code
8. —(1) Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any computer shall be guilty of an offence if he did so —

(a) for any wrongful gain;

(b) for any unlawful purpose; or

(c) knowing that it is likely to cause wrongful loss to any person.

(2) Any person guilty of an offence under subsection (1) shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

It should be noted that enhanced penalty provisions apply to specified “protected computers”:

Enhanced punishment for offences involving protected computers
9. —(1) Where access to any protected computer is obtained in the course of the commission of an offence under section 3, 5, 6 or 7, the person convicted of such an offence shall, in lieu of the punishment prescribed in those sections, be liable to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 20 years or to both.

(2) For the purposes of subsection (1), a computer shall be treated as a “protected computer” if the person committing the offence knew, or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for —

(a) the security, defence or international relations of Singapore;

(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;

> (c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or
>
> (d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services.
>
> (3) For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in subsection (2) if there is, in respect of the computer, program or data, an electronic or other warning exhibited to the accused stating that unauthorised access to that computer, program or data attracts an enhanced penalty under this section.

The protection of computers and data on which national security depends is enhanced by section 15A of the *CMA*, which was added in 2003. Subsection (1) provides:

> **Preventing or countering threats to national security, etc.**
> **15A.** —(1) Where the Minister is satisfied that it is necessary for the purposes of preventing or countering any threat to the national security, essential services, defence or foreign relations of Singapore, the Minister may, by a certificate under his hand, authorise any person or organisation specified in the certificate to take such measures as may be necessary to prevent or counter any threat to a computer or computer service or any class of computers or computer services.

It does not appear that section 15A has yet been invoked in Singapore. While other jurisdictions normally recognise executive or emergency powers with respect to national security matters, section 15A is unusual in legislatively defining such powers with respect to threats to computers and computer servicers.

3. *Abetments and attempts*

Section 10 of the *CMA* deals with abetments and attempts:

> **Abetments and attempts punishable as offences**
> **10.** —(1) Any person who abets the commission of or who attempts to commit or does any act preparatory to or in furtherance of the commission of any offence under this Act shall be guilty of that offence and shall be liable on conviction to the punishment provided for the offence.
>
> (2) For an offence to be committed under this section, it is immaterial where the act in question took place.

Subsection (1) is in similar terms to section 511 of the *Penal Code*,[7] which also provides a number of illustrations:

[7] Cap. 224, Rev. Ed. 1985, Sing.

> (*a*) *A* makes an attempt to steal some jewels by breaking open a box, and finds after so opening the box that there is no jewel in it. He has done an act towards the commission of theft, and therefore is guilty under this section.
>
> (*b*) *A* makes an attempt to pick the pocket of *Z* by thrusting his hand into *Z*'s pocket. *A* fails in the attempt in consequence of *Z*'s having nothing in his pocket. *A* is guilty under this section.

By analogy, it is apparent that an attempt to gain unauthorised access to computer data which fails due to protective measures such as passwords or encryption, or an attempt to steal funds which fails because a bank account turns out to be empty, may nonetheless be punishable as attempted offences under the *CMA*. Where an offence involving computers would be charged under the *Penal Code* rather than the *CMA* (as with the "child grooming" offence in section 376E discussed below),[8] then section 511 of the *Penal Code* ensures a similar result. This may be critical in enabling the use of assumed identities in policing such online crimes.

It is notable that subsection (2) of section 10 of the *CMA* extends the territorial reach of the abetment and attempt offences, so that a preparatory act may be committed outside Singapore, and this may nonetheless still constitute an attempt under the statute. In fact, the territorial scope provision of the *CMA* extends the jurisdictional reach of the legislation for all its offences.

4. *Territorial Scope*

Section 11 of the *CMA* provides:

> **11.** —(1) Subject to subsection (2), the provisions of this Act shall have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within Singapore.
>
> (2) Where an offence under this Act is committed by any person in any place outside Singapore, he may be dealt with as if the offence had been committed within Singapore.
>
> (3) For the purposes of this section, this Act shall apply if, for the offence in question —
>
> (a) the accused was in Singapore at the material time; or
>
> (b) the computer, program or data was in Singapore at the material time.

This provision ensures that computer misuse involving computers or data in Singapore, even if committed from outside the country, nonetheless falls within the scope of the *CMA*, thus giving the legislation extra-territorial effect.[9] This is a feature shared by some other

[8] See *infra* Section I.B.

[9] By contrast, Malaysia's *Computer Misuse Act 1997*, s. 9, extends liability under the Act "if, for the offence in question, the computer, program or data was in Malaysia or capable of being connected to or sent to or used by or with a computer in Malaysia at the material time": see Koops and Brenner, *Cybercrime and Jurisdiction: A Global Survey*, Info Technology & Law No.11, 2005.

statutes in Singapore, including legislation directed at the protection of vulnerable victims from exploitation:[10]

> Singapore has several statutes with extraterritorial effect, most notably the *Misuse of Drugs Act* (Cap 185), the *Computer Misuse Act* (Cap 50A) and the *Prevention of Corruption Act* (Cap 241). It has yet to enact child sex tourism law with extraterritorial effect, although it is considering doing so. While the existing extraterritorial statutes in Singapore have rarely been invoked, arguably the existence of these statutes acts as a deterrent, and when the occasion arises, affords a mechanism for doing justice. If Singapore takes the view that it should be entitled to prosecute one of its citizens who, during an overseas visit to a country where it is legal to consume marijuana, does consume marijuana before returning to Singapore, then it is very difficult to argue against enacting child sex tourism laws to prosecute Singaporeans who go overseas in order to have sex with children, which is both a crime in the other country as well as in Singapore.

B. *Other Legislation*

Legislative provisions dealing with crimes of dishonesty, intimidation or conspiracy may be involved in computer misuse cases, and in many cases section 4 of the *CMA* can be charged using such an offence as the "foundation crime". There are also intellectual property infringement offences under Singapore law that could similarly be involved in computer misuse.[11]

Likewise, the use of the Internet to disseminate or download offensive content, such as child pornography or racial vilification, is dealt with by statutes such as the *Undesirable Publications Act*,[12] which deals with material which is obscene "such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it" (section 3), or objectionable because it describes or depicts (section 4):[13]

> (a) matters such as sex, horror, crime, cruelty, violence or the consumption of drugs or other intoxicating substances in such a manner that the availability of the publication is likely to be injurious to the public good; or
>
> (b) matters of race or religion in such a manner that the availability of the publication is likely to cause feelings of enmity, hatred, ill-will or hostility between different racial or religious groups.

---

10 Kumaralingam Amirthalingam, "Protection of victims, particularly women and children, against domestic violence, sexual offences and human trafficking" [2006] A.L.A. 17 (notes omitted).

11 Copyright Act (Cap.63, Rev. Ed. 2006, Sing.), s 136 Offences; and Trade Marks Act (Cap.332, Rev. Ed. 2005, Sing.), ss. 46 - 49 Offences.

12 Cap. 338, Rev. Ed. 1998, Sing.

13 See further *Undesirable Publications Act*, s. 11: Offences involving obscene publications; s. 12: Offences involving objectionable publications; *Penal Code*, s. 505: Statements conducive to public mischief; *Maintenance of Religious Harmony Act* (Cap. 167A, Rev. Ed. 2001, Sing.).

).

In addition, the *Penal Code* has recently been amended to include an offence of "child grooming":[14]

> **Sexual grooming of minor under 16**
> **376E.** —(1) Any person of or above the age of 21 years (A) shall be guilty of an offence if having met or communicated with another person (B) on 2 or more previous occasions —
>
> (a) A 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.
>
> (2) In subsection (1), "relevant offence" means an offence under —
>
> (a) section 354, 354A, 375, 376, 376A, 376B, 376F, 376G or 377A;
>
> (b) section 7 of the *Children and Young Persons Act* (Cap. 38); or
>
> (c) section 140 (1) of the *Women's Charter* (Cap. 353).
>
> (3) For the purposes of this section, it is immaterial whether the 2 or more previous occasions of A having met or communicated with B referred to in subsection (1) took place in or outside Singapore.
>
> (4) A person who is guilty of an offence under this section shall be punished with imprisonment for a term which may extend to 3 years, or with fine, or with both.

This offence is based on section 15 of the UK's *Sexual Offences Act 2003*, but applies in Singapore to persons over 21 years as opposed to the UK's threshold of 18 years. Interestingly, there is a requirement that there be two or more previous communications or contacts before the physical act of meeting or travelling in order to complete the physical requirements for the offence. Further, the intended offence must fall within the designation of a "relevant offence" as detailed in subsection (2).[15] Under both the

---

[14] *Penal Code (Amendment) Act* 2007 (No. 51 of 2007).

[15] "Relevant offences" as listed in subsection (2) are:

(i) Penal Code (Cap.224) offences
s354 - Assault or use of criminal force to a person with intent to outrage modesty
s354A – Outraging modesty in certain circumstances
s375 – Rape
s376 – Sexual assault by penetration
s376A – Sexual penetration of minor under 16
s376B – Commercial sex with minor under 18
s376F – Procurement of sexual activity with person with mental disability
s376G – Incest
s377A – Outrages on Decency

(ii) Children and Young Persons Act (Cap.38) offence
s7 – Sexual exploitation of child or young person

(iii) Women's Charter (Cap.353) offence

Singapore and UK offences, the person receiving the communications must be a child under the age of 16 years.[16]

The Second Reading Speech makes clear that the new section 376E offence is designed to enable early intervention by law enforcement authorities, before a child is physically assaulted:[17]

> The section, modelled after section 15 of the *UK Sexual Offences Act 2003*, provides that an adult of or above the age of 21 years who meets or travels to meet a minor, either male or female, under 16 years of age within Singapore with the intention of committing a sexual offence, will be guilty of an offence if the person had met or communicated with the minor on 2 or more previous occasions. Like the UK, we had set the bar at 2 or more communications/meetings as this signals repeat behaviour, that is to say, rather than being one-off, the offender is more likely priming the victim by gaining his or her trust and confidence for a "strike" later. These prior meetings or communications can take place face to face or over the Internet.
>
> Besides the two prior communications or meetings, a key element in this new offence is that the offender possesses a criminal intent at the time of meeting the child or at the time of traveling to meet the child to commit a sexual offence against her. The meeting or traveling must take place in Singapore, even if the earlier communications or meetings had taken place outside Singapore.
>
> This new offence will strengthen Police's hand in preventing any harm from befalling the victim. Currently, in order to secure a successful prosecution for an attempted sexual offence, it would require the offender to be caught in doing something very close in proximity to the sexual offence in question, for example, undressing the victim. This, of course, is not satisfactory. With the new offence, Police will be able to intervene much earlier. What is needed is for Police to show that there has been the requisite number of communications wherein the predator has prepared the ground, after which he acts with the intention of committing a sexual offence against the victim, that is, by traveling to meet her or actually meeting her. The penalty is a maximum term of imprisonment of 3 years, or fine or both.

---

s140(1) – Offences relating to prostitution [includes carnal knowledge of girl under 16].

16 Contrast the Australian provisions in the *Criminal Code Act 1995* (Cth), s. 474.26: Using a carriage service to procure persons under 16 years of age; and *s*. 474.27: Using a carriage service to "groom" persons under 16 years of age. These offences introduced in 2004 are punishable by a maximum of 15 years and 12 years respectively, and importantly apply not only where a real child under 16 is being procured or groomed, but also where the recipient of the communications via a carriage service (e.g., email) is someone who the sender believes to be under 16 years of age, thus allowing police officers to engage in "sting operations" by posing as a child online: see Tony Krone, "Queensland police stings in online chat rooms" *Trends & Issues in Crime and Criminal Justice*, no. 301 (2005), Australian Institute of Criminology; and Tony Krone, "International police operations against online child pornography" *Trends & Issues in Crime and Criminal Justice*, no.296 (April 2005), Australian Institute of Criminology.

17 Second Reading Speech of The Penal Code (Amendment) Bill, by Senior Minister of State A/P Ho Peng Kee on 22 October 2007, paras. 39 – 42 (notes omitted).

> 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.

II. CASES

The following cases and commentary illustrate the *CMA* and other offences discussed above, as prosecuted in Singapore up to the time of writing (October 2008), ranging across a number of broad categories of computer misuse.

A. *Unauthorised Access to / Modification of Computer Material*

The term 'hacking' is generally applied to a range of activities that involve deliberately obtaining unauthorised access to computers or their contents. The motivation may be idle curiosity (as in the activities of "script kiddies" or "hobby hackers"), malicious (as with political or other sabotage) or financial gain (as engaged in by criminal syndicates or individual offenders seeking illicit gains). At the core of such offending is the idea that persons other than those who have proper authorisation to use computers or data commit a kind of "intrusion" or "trespass" if they seek ways of circumventing protective devices such as login names, passwords or encryption.

Few jurisdictions have large numbers of criminal cases involving actual or attempted cases of computer hacking. It is likely that a significant proportion of such cases are dealt with by less public means, such as dismissal from employment, expulsion from educational institutions or other disciplinary measures. Nonetheless, some cases have emerged, including in Singapore. The following is arguably the most prominent of Singapore's hacking cases thus far.

1. Public Prosecutor v. Muhammad Nuzaihan bin Kamal Luddin[18]

The accused in this case was a 17-year old student who, during the year-end school vacation of 1997, had become interested in computer security and had discovered that certain flaws in Linux operating systems allowed outside parties to check for vulnerabilities in computer networks. Sometime in June 1998, he decided to "hack" into various foreign servers, believing that this would not be easily detected or traced by the relevant system administrators who were mostly located abroad. He managed to hack into four foreign sites successfully without being detected by their system administrators. As a result of this "achievement", he became more confident about hacking and subsequently decided to test his skills on local servers.

His progression to the servers of Swiftech led to his being charged with three offences under the *CMA*:[19]

[18] [2000] 1 S.L.R. 34; [1999] SGHC 275

> Sometime in June 1998, the respondent detected certain vulnerabilities in some of the servers comprised in Swiftech's network whereupon he decided to hack into one of the proxy servers of the network, namely *Cloud4*, as its role was of the least importance and consequently any intrusion would be less likely to be detected by the system administrator. In July 1998, the respondent downloaded an exploit known as "ROTShB" (Riders Of The Short Bus) from the Internet. He compiled the program codes of this exploit into a program which he executed on Swiftech's network, via the server *Cloud4*. The execution of the program caused the server *Cloud4* to process and grant access request to the respondent, allowing him to secure access to the computer files contained in *Cloud4*. All the accesses made by the respondent to the computer files of *Cloud4* were done without the authority of Swiftech's system administrator.
>
> After gaining root access to the server *Cloud4* of Swiftech, the respondent executed a program known as "bounce" which he uploaded to *Cloud4*. Upon execution of "bounce", the port 31337 of the server *Cloud4* was automatically reconfigured to allow the respondent to utilise the server to gain access to the Internet Relay Chat ("IRC"). The respondent had thus successfully created a user account for himself in the server *Cloud4*, which account he made use of to connect to the IRC. While on the IRC, the respondent indicated to the other users on the channel that he was able to compromise a server which ran on a Linux operating system.
>
> At or around the same time that the respondent did the above acts, he also hacked into the File Transfer Protocol ("FTP") server *Brahms* of Singapore Cable Vision Ltd ("SCV"). The respondent had earlier applied to SCV for an Internet account but was rejected as the cable modem service was not then available to his estate. As such, he decided to gain unauthorised access to the server *Brahms* in order to make use of the cable network's high-speed link to download files from the Internet. Upon gaining access to *Brahms*, the respondent amended several files in the server and later configured a backdoor known as "nightman" at port 22 of the server which allowed him to access the server *Brahms* in future without having to hack into the system again. He would remove his trails from the server *Brahms* by deleting the system logs every time before logging out from the server.
>
> No tangible damage was caused to the computer systems of both Swiftech and SCV.

In consequence of these activities, the accused faced three charges under, respectively, sections 3(1), 5(1) and 6(1)(a) of the *CMA*. He pleaded guilty, and on sentencing a further fifteen similar charges were taken into account. He was sentenced in the District Court to undergo 30 months' probation. The prosecution appealed on the basis that this sentence was manifestly inadequate.

In allowing the appeal, the High Court judge took the view that probation, designed to afford young offenders rehabilitation by removing their opportunity to re-offend, was not an appropriate response to computer offending:[20]

---

19 *Ibid* at paras. 6-9.

20 *Ibid.* at para. 18, per Yong Pung How C.J.

> The inherent nature of offences under the *CMA* makes probation orders ineffective, as keeping the offender at home in such cases does not guarantee that the offender will not repeat his actions. There is no doubt that a majority of these computer-related crimes are committed at home, and certainly this was the case here. That the parents have failed to avert the commission of these offences in the first place, despite the fact that they were committed at home, fortifies the view that responsibility for the offender's future behaviour can no longer be left in the hands of his parents. The public interest requires that offenders such as the respondent be put away in a place where access to the major instrument of his crime is not available to him in order that he is not afforded any opportunity to re-offend.

In addition, the judge accepted the prosecutor's arguments that the youth's activities in this case had been accompanied by "criminal intent" and that, although no tangible damage had been caused to the computers involved, this did not mean that no societal harm was threatened:[21]

> In my view, such anti-social conduct on the part of the respondent not only undermines public and international confidence in the commercial integrity and viability of our computer systems, it also gravely compromises Singapore's efforts to position itself as a global e-commerce hub. The potential for which these cyber-crimes have in undermining Singapore's burgeoning information technology (IT) industry cannot be ignored. IT security is a major consideration which many foreign companies take into account before deciding whether or not to develop and invest in the local IT sector.

The judge quashed the probation order and imposed sentences of 2 months' imprisonment on each of the three charges, with two to run consecutively, making an aggregate sentence of 4 months. The judgment concludes with an optimistic note:[22]

> I recognise that the respondent is an intelligent and resourceful young man whose true talent and potential, when harnessed under the right conditions, can be of immense value to the country. It is hoped therefore that the experience of life in prison will instil in him a sense of maturity and responsibility, and teach him to put his computing skills to legitimate use upon his release, thus enabling him to contribute usefully to society.

A different kind of unauthorised access to computer networks is involved in the activity of "mooching" or "piggybacking" on an unsecured wireless network.[23] Although prosecutions for this kind of activity are rare in Asia and indeed globally, Singapore already has a reported case. In March 2007, it was reported that a 17-year-old who piggybacked on his neighbour's wireless Internet connection in order to engage in online chatting was sentenced to 18 months' probation in the District Court.[24]

---

21 *Ibid.* at para. 18.

22 *Ibid.* at para. 27.

23 See Tony Krone and Gregor Urbas, "Mobile and Wireless Technologies: Security and Risk Factors", *Trends and Issues in Crime and Criminal Justice*, No. 329, November 2006, Australian Institute of Criminology.

24 Channel News Asia, Technology News, "Wireless piggybacking case sets precedent: experts", 26 March 2007, online: <http://www.channelnewsasia.com/stories/technologynews/view/266368/1/.html>.

B. *Computer Sabotage / Confidential Information*

In a recent article, it is pointed out that preventing access to computers by changing passwords without authorisation may also fall within the offence provisions of the *CMA*:[25]

> Any unauthorised modification, interception and obstruction of a company's computer materials or services are also offences under the *CMA*. For example, sabotaging a computer programme before leaving the company by secretly setting password protection within the programme that prevents the company from being able to check, modify or upgrade the system could amount to an unauthorised modification or obstruction of computer services. [Further], it is an offence under the *CMA* to disclose one's access code (such as user-id and passwords) of any programme or data to other people without the company's permission. Companies are advised to include a clause in the company's employment contract or in their IT Use Policy to remind employees not to disclose their access codes to other people.

Just such a scenario occurred in a recent case that reportedly involves the first ever private prosecution under the *CMA*, as well as civil action for breach of confidence. A systems engineer formerly employed by SMC Marine Services has been accused of secretly setting passwords within a program that he developed before leaving the company, allegedly leaving his former employer unable to check, modify or upgrade the system.[26] This could constitute an offence under section 5 (Unauthorised Modification) or section 7 (Unauthorised Obstruction) of the Act. Civil litigation seeking injunctions to prevent disclosure of the company's confidential information was also commenced in the High Court.[27]

C. *Counterfeit Card Fraud*

In the recent case of *Public Prosecutor v. Fernando Payagala Waduge Malitha Kumar*,[28] the judge commented:[29]

> Credit cards are now widely accepted as a preferred mode of payment for daily transactions. Unfortunately, the plethora of credit card transactions has in turn engendered a multiplicity of credit card offences. The financial burden perpetrated by such credit card frauds falls on the shoulders of the issuers, the banking industry and credit card holders. Indeed, the very substantial interest that credit card issuers and banks charge for instalment payments and defaults can also be directly attributed to the substantial losses these institutions continue to chalk up from card frauds and scams. It would be no exaggeration to assert that the entire credit card holding community bears the palpable and painful brunt of such offences. In addition, the inconvenience, frustration, distress and perhaps even loss of reputation suffered by victims of fraud are often incalculable and irremediable. It is

---

25 Elaine Tan, "IT breaches: a firm's legal recourse" *The Business Times* (Singapore) (24 June 2008).

26 See Selina Lum, "Firm takes systems engineer to court", *The Straits Times* (Singapore) (14 June 2008).

27 *SMC Marine Services (Pte) Ltd v. Thangavelu Boopathiraja and Others* [2008] SGHC 29.

28 [2007] SGHC 23 [*Fernando Payagala*].

29 *Ibid.* at paras. at 1–2.

> therefore important to have a coherent and consistent sentencing regime to deter the commission of such offences in Singapore.

The case itself involved only an opportunistic misuse of a credit card found by a passenger on a Singapore Airlines flight, who then used the card to make several unauthorised purchases while in transit at Changi International Airport. However, many of the cases dealt with by Singapore courts over recent years have involved organised syndicates using cloned credit or ATM cards in order to commit a series of transactions causing loss to the legitimate owners of the accounts and/or the financial institutions involved.[30]

The computer misuse provision that best applies to the use of counterfeit or forged cards in order to obtain unauthorised access to funds is section 4 of the *CMA*.[31] Where the attempt to obtain funds succeeds, offenders may also face charges under the *Penal Code* for theft (section 378) or other offences. The following leading case illustrates the approach that Singapore is taking in relation to the punishment of organised credit card fraud involving the use of computer technology.

1. Public Prosecutor v. Navaseelan Balasingam[32]

The accused was a British national of Sri Lankan descent who had entered Singapore on 28 February 2006 on a 14-day social pass. At the invitation of a person called 'Kumar', he engaged in a course of conduct that involved withdrawing cash from ATMs of the United Overseas Bank (UOB) using fake ATM cards, which had been supplied by Kumar. During the illegal cash withdrawals, the accused wore a cap provided to him by Kumar in order to avoid identification by CCTV cameras installed at the ATMs. Despite this, video images of the accused withdrawing cash from the ATMs were captured by the cameras.

On 4 March 2006, the accused was seen and detained by a bank officer while trying to make an unauthorised withdrawal from an ATM located on Havelock Road in Singapore's city centre. The police were called. On being arrested, a search revealed that he had 22 counterfeit ATM cards in his possession, cloned from originals belonging to account holders living in the UK.

At trial, the accused pleaded guilty to 5 charges of computer access with intent to commit or facilitate the commission of an offence under section 4 of the *CMA* and 5 charges under section 379 of the *Penal Code* for stealing funds from UOB through these transactions. In addition, for the purposes of sentencing, the District Court judge took into account a

---

30 The judgment of V K Rajah J. in *Fernando Payagala*, *ibid.*, includes a detailed discussion of previous counterfeit card cases and sentences imposed, with reference also to cases in Hong Kong and the UK.

31 Other recent cases where s. 4 of the CMA was charged alongside dishonesty offences and/or conspiracy in relation to credit card fraud include Public Prosecutor v. S Kalai Magal Naidu [2006] SGDC 226; Public Prosecutor v. Chong Shih Wai and Another [2006] SGDC 268; Public Prosecutor v. Tang Soong See [2006] SGDC 269; Public Prosecutor v. Law Aik Meng [2006] SGDC 243; appealed at Public Prosecutor v. Law Aik Meng [2007] SGHC 33; and Public Prosecutor v. Ratnavel Pratheeskumar [2006] SGDC 285 [Ratnavel Pratheeskumar]. Cases in which computers were used in breaching provisions of lotteries legislation include Public Prosecutor v. Lim Li Ling [2006] SGMC 8; appealed at Lim Li Ling v. Public Prosecutor [2006] SGHC 184.

32 [2006] SGDC 156 [*Navaseelan Balasingam* (D.C.)]

further 129 charges under section 4 of the *CMA* and 129 mirroring theft charges with which the accused was charged at the time of his guilty plea.

The accused was sentenced to 18 months' imprisonment on each of the 5 computer misuse charges and 6 months' imprisonment on each of the 5 theft charges, with 3 of the former and 2 of the latter to run consecutively, so that the effective total sentence was 66 months' imprisonment to run from the date of first remand on 20 April 2006. The convicted accused appealed against sentence, and on 1 August 2006 the District Court judge set out at length his reasons for imposing the sentences. In explaining the need for deterrence in the area of computer crime, the judge stated:[33]

> An offence under section 4 of the Computer Misuse Act is undoubtedly a very serious crime. The 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 only to that of section 9* (the latter provides for enhanced punishment for offences involving 'protected computers').
>
> During the second reading of the Computer Misuse (Amendment) Bill on 30 June 1998, the Minister noted at column 392 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 seriously as other criminal offences.
>
> In accordance with the above Parliamentary statement, the High Court decided in *PP v Muhammad Nuzaihan bin Kamal Luddin* [2000] 1 SLR 34 @ para 21 to mete out *'a deterrent sentence'* on the respondent in that case 'to give effect to Parliament's express intention that all computer crimes will be dealt with severely in Singapore' …
>
> Policy considerations, the far-reaching effects which the offences have on the public interest if their pervasion is not halted at an early stage, and the seriousness with which Parliament views cyber-crime, all mandated the imposition of a custodial sentence.
>
> In my view, the policy considerations articulated in *Muhammad Nuzaihan bin Kamal Luddin* ring even louder in the Accused's case, where the computer crime was *more serious and sinister in nature* – in that the unauthorised access through an ATM was for the purpose of compromising a bank's computer system to facilitate the theft of monies, and not out of boredom or curiosity (as in *Muhammad Nuzaihan bin Kamal Luddin*).

[33] *Ibid.* at paras. 18–22.

The District Court judge went on to observe that the accused's offences "*did not appear to be an isolated incident* where cloned ATM cards had been used to withdraw monies in Singapore",[34] as during the proceedings the prosecutor had informed the court that "the authorities had in fact arrested another 6 Sri Lankans (residents in the UK) who had used exactly the same modus operandi as the Accused to target UOB ATMs in Singapore".[35] The judge concluded:[36]"Without a doubt, the increasing prevalence of such crimes has a potentially chilling effect on the public's embrace of ATM banking."

Other factors mandating a deterrent sentence including the high degree of planning and premeditation, involving 134 unauthorised withdrawals across virtually all parts of Singapore in a period of 4 days, and the involvement of a criminal syndicate which used sophisticated methods to obtain confidential data and PIN numbers from genuine cards in the UK and encrypt these onto the cloned cards used by the accused. Meticulously weighing considerations of deterrence and proportionality, the judge arrived at a general range appropriate to such offending:[37]

> After careful consideration, I came to the view that for a 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 of *between 12 to 24 months* would not be out of order.

Although a sentencing discount for a guilty plea might be applicable in some cases, the judge held that the accused had little choice but to plead guilty in this case, having been "caught red-handed" attempting to make an unauthorized ATM withdrawal, which was recorded on CCTV, and with 22 cloned ATM cards in his possession.

2. Navaseelan Balasingam v. Public Prosecutor[38]

On appeal, a judge of the High Court (Tay Yong Kwang J.) revised the sentence handed down. While generally agreeing with the approach to the seriousness of the offences that was taken in the District Court, the High Court judge considered that the *CMA* charges warranted sentences would run consecutively:[39]

> Anyone who visits this country with a view to going ATM-shopping with cloned bank cards should realise that we take a very serious view of offences which strike

---

34 *Ibid.* (emphasis original)

35 As described in the media release "Six Foreigners Arrested for Theft From ATM and Access with Intent To Commit an Offence under the Computer Misuse Act" issued by the Public Affairs Department of the Singapore Police Force on 16 May 2006. The six were convicted after each pleaded guilty to multiple counts of conspiracy to commit theft and conspiracy to commit an offence under s. 4 of the *CMA*. The sentencing judge (District Judge Francis Tseng) followed *Navaseelan Balasingam* (D.C.), *supra* note 32 in imposing individual sentences of 6 months' imprisonment on each computer misuse count, with the result that the aggregate sentences of the six accused ranged from 6 years 3 months to 10 years 6 months, as set out in the appeal judgement of *Ratnavel Pratheeskumar*, *supra* note 31.

36 *Navaseelan Balasingam* (D.C.), *supra* note 32 at para. 25.

37 *Ibid.* at para. 53.

38 [2006] SGHC 228 [*Navaseelan Balasingam* (H.C.)].

39 *Ibid.* at paras. 34–39.

> at electronic financial and commercial transactions. Such crimes gnaw at public confidence and can stymie the growth of a very efficient way of life.
>
> Technology is capable of making our lives much better and ATM cards have become an integral part of life in Singapore. Abuse of technology to commit crimes especially on a large scale, therefore becomes all the more insidious in this electronic landscape and it calls for a decidedly deterrent sentence.
>
> On the facts of this case, 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 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 had 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 not 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 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 made a clean and easy exit and returned home, or, perhaps, moved on to his next ATM "El Dorado".
>
> The appellant's *modus operandi* presented extreme difficulty in detection and apprehension by the authorities. The accumulated loot of about $54,380 had disappeared with remarkable speed and efficiency even as the appellant was busily traversing the ATM network of the bank. How this was done remains to be seen but it is clearly another hallmark of a well-organised crime.
>
> As I have stated, the security of Singapore's financial institutions and protection of public interest against electronic financial scams are paramount in a case like this. Even if the local bank in question did not ultimately suffer any financial loss, there was no doubt that some other financial institution somewhere did suffer loss and that the syndicate involved did benefit from the loot, which was not of an insignificant amount. I am therefore of the opinion that the appropriate sentence to mete out here is 7½ years, arrived at by ordering all sentences for the *Computer Misuse Act* charges to run consecutively. In the light of the many offences and the circumstances in which they were committed, such a sentence could hardly be said to be a crushing one.

However, the serving of the sentences was back-dated to the time of the appellant's arrest on 4 March 2006 as that was the time at which he was taken into custody and therefore

deprived of his liberty. The result of the appeal against sentence was therefore an increase from 5½ years (i.e. 66 months) to 7½ years, but commencing 1½ months earlier.[40]

D. *Copyright and Related Rights*

There are numerous cases in Singapore involving infringement of copyright and related rights through unauthorised production of or dealings with music recordings, videos and film, or computer software.[41] It is also an offence for a company to install pirated software on its machines.[42]

In principle, section 4 of the *CMA* could be charged against a person who used the Internet to commercially distribute pirated music, film or software as these are offences involving "property, fraud [or] dishonesty" within the meaning of subsection (2) and which are punishable under the *Copyright Act* and/or *Trade Marks Act* by 3 years or more.[43]

E. *Cyber-Stalking, Harassment and Online Grooming*

Online harassment, bullying or insulting behaviour using the Internet or mobile phones is hardly uncommon, particularly amongst older children or college students.[44] However, most cases do not result in legal consequences. Where the behaviour is exceptionally concerning, such as where it amounts to stalking, harassment or grooming, prosecution can occur. As the following case shows, a mix of physical and electronic acts may be involved, and some of these may be dealt with under the *CMA*.

1. Lim Siong Khee v. Public Prosecutor[45]

The accused in this case was charged under section 3(1) of the *CMA* in relation to his alleged tampering with the email account of a female acquaintance with whom he had had a relationship until she ended it, after which he began to stalk and harass her using email, phone calls and physically following her. In particular, the accused managed to get access to the victim's email account (she used her birth date as her password) and posted messages to her friends, with offensive descriptions of her purported intimate relations and some including pornographic attachments.

---

40 This was not the last example of ATM fraud using cloned credit cards to be reported in Singapore. In a media release 'Foreigners Arrested For Theft Using Cloned Cards' issued by the Public Affairs Department of the Singapore Police Force on 20 June 2008, the arrest of a Ghanian man and an Ethiopian woman for using cloned ATM cards in the Orchard Road vicinity is reported.

41 See for example, *Public Prosecutor v. Md Hapiz bin Tahir* [2007] SGDC 40; *Public Prosecutor v. Chan Soon Fatt* [2007] SGDC 54; and *Public Prosecutor v. Koh Eng Kian* [2007] SGDC 166.

42 See *Public Prosecutor v. PDM International Pte Ltd* [2006] SGDC 91, in which the defendant company pleaded guilty through its manager and was fined $ 15,000 on each of two counts.

43 *Copyright Act*, *supra* note 11, s. 136 (Offences); and *Trade Marks Act*, *supra* note 11, ss. 46-49 (Offences).

44 See Gregor Urbas, "Look Who's Stalking: Cyberstalking, online vilification and child grooming offences in Australian legislation", 10(6) *Internet Law Bulletin* 62 (2007).

45 [2001] SGDC 32

In his defence, the accused claimed that the victim had in fact told him her email password and had asked him on one occasion to check her email on her behalf. The court did not accept this case of consent, and found the accused guilty as charged. He was sentenced to 5 months' imprisonment:[46]

> In devising novel methods to stalk and harass Ms Chong the accused had exploited the advancements made in information technology and abused his expertise in the said field. …The contents of the nuisance mails and the alarming regularity with which the accused circulated them reflect the scale and extent of the accused's mischief. Having regard to the manner in which the offence was perpetrated I deemed a custodial sentence necessary.

An appeal against the conviction and sentence was filed.[47]

In a more recent case, it has been reported that a 24-year-old undergraduate was sentenced to 27 months in prison for stealing the MSN instant messenger identities of several women, using these to assume their identities to chat with other people on their contact lists, and doctoring pictures by superimposing the heads of some of the women on naked bodies. He further threatened to make public the image of one victim unless she sent him photos of her breasts. The offender faced nine charges under the *CMA* and one charge of criminal intimidation, pleaded guilty, and was sentenced in January 2007.[48]

As this case shows, the use of computer technology to target potential victims of predatory sexual behaviour is relatively simple. In particular, Internet chat rooms and social networking sites such as FaceBook and MySpace have provided child sex offenders with ready access to children online, which some exploit in order to contact and "groom" their intended victims. Now that Singapore has a grooming offence on its statute books (section 376E of the *Penal Code*, discussed above),[49] it is expected that reported cases will emerge.[50]

As noted earlier, law enforcement investigators in other countries have been able to infiltrate child pornography and paedophile networks using assumed identities. Internet groomers are also routinely flushed out by officers posing as children, who are able to arrest after a meeting between the groomer and "child" is arranged. In some legal systems, a defence of entrapment may be raised in response to such "sting operations"[51], a stay of proceedings may be ordered, [52] or evidence may be excluded due to police illegality or

---

46 *Ibid.* at paras. 44–45, per P Siva Shanmugam.

47 The outcome is not reported.

48 See Vivian Yeo, "MSN hacker gets 27 months' jail", *ZDNet Asia*, 16 January 2007, online: <http://www.zdnetasia.com/news/security/0,39044215,61982282,00.htm>.

49 See *supra* Section I.B.

50 At the time of writing, no such completed cases had yet been reported in Singapore.

51 As in the United States: see *Sorrells v. United States*, 287 U.S. 435 (1932); and the child pornography case of *Jacobson v. United States*, 503 U.S. 540 (1992).

52 As in the United Kingdom: see *R v. Looseley* [2001] 4 All E.R. 897; see also Simon Bronitt, "Sang is Dead, Loosely Speaking – R v Loosely" [2002] Sing. J.L.S. 374.

impropriety.[53] In Singapore there is no common law defence of entrapment that would stand in the way of law enforcement investigators posing as children online in order to identify child groomers.[54] However, the section 376E offence does not (unlike some counterpart grooming offences in other countries) cover the situation where the offender merely believes that the person he is grooming is a child under 16 years. In this situation, it appears that the offence could be prosecuted as:

(i) attempt to commit a child sex offence under the *Penal Code* – though the problem here is that the conduct may not be sufficiently far along the way to a completed offence (particularly as no real child is involved);

(ii) attempt to commit a section 376E grooming offence (noting that under section 511 of the Penal Code and the illustrations that follow it, an attempt to groom a non-existent child would arguably be seen in analogy with attempt to steal non-existent goods); or

(iii) a *CMA* section 4 offence, where computer access is used with intent to commit a later sexual offence (though here there may be a problem with whether the intended offence, such as those detailed in subsection (2) of section 376E) would qualify as involving dishonesty or causing bodily harm as required under section 4(2) of the *CMA*.

Future cases prosecuted in Singapore will reveal which prosecutorial strategies are pursued to a successful conclusion.

III. CONCLUSION

Singapore has a broad range of *CMA* offences and others in the *Penal Code* and elsewhere, that serve to criminalise most known varieties of cybercrime. The abetment and attempt provisions of both the *CMA* and the *Penal Code* allow law enforcement officers to intervene at preparatory stages of crimes, and the extra-territorial scope of the *CMA* allows prosecution even where the preparatory conduct occurs outside Singapore. Sentences imposed in decided cases indicate that the misuse of computers, particularly with intent to defraud or intimidate others, is punished appropriately. It remains to be seen whether the same success will be demonstrated in regard to the new grooming offence in section 376E of the Penal Code.

IV. REFERENCES

Kumaralingam Amirthalingam, "Protection of victims, particularly women and children, against domestic violence, sexual offences and human trafficking" [2006] A.L.A. 17

[53] As in Australia: see *Ridgeway v. The Queen* (1995) 184 C.L.R. 19; and s. 138 *Evidence Act 1995* (Cth and NSW).

[54] *How Poh Sun v. PP* [1991] S.L.R. 220; *Mohamed Emran bin Mohamed Ali v. PP* [2008] SGHC 103.

Stephen Blythe, "Singapore computer law: an international trend-setter with a moderate degree of technological neutrality" (2007) 33(2) Ohio N.U.L. Rev. 525

Simon Bronitt, "Sang is Dead, Loosely Speaking – R v Loosely" [2002] Sing.J.L.S. 374

Business Times, "IT breaches: a firm's legal recourse" *The Business Times* (Singapore) (24 June 2008)

Indira Carr and Katherine Williams, "Reflections on enforcement measures and penalty levels in computer misuse legislation: the Council of Europe Convention on Crime in cyberspace", *15th BILETA Conference: Electronic Datasets and Access To Legal Information*, April 2000, University Of Warwick, England

Warren B Chik, "Phishing with a poisoned bait" *Law Gazette*, January 2007 (1)

Christopher Lee Gen-Min, "Offences created by the Computer Misuse Act 1993" [1994] Sing. J.L.S. 263

Keystone Law Corporation, "Man behind bomb hoax gets 3 months' jail and fine" *Tech Law Alert*, Keystone Law Corporation, March 2007 (3)

Looi Teck Kheong, "Cybercrimes" *Law Gazette*, August 2000 (3)

Chua Siak Kim, "Electronic evidence: Singapore's approach", *Law Gazette*, July 2002 (1)

Yeong Zee Kin, "Computer misuse, forensics and evidence on the Internet" *Communications Law* 5.5 (Oct 2000) 153

Tony Krone, "Queensland police stings in online chat rooms" *Trends & Issues in Crime and Criminal Justice*, no.301 (2005), Australian Institute of Criminology

Tony Krone, "International police operations against online child pornography" *Trends & Issues in Crime and Criminal Justice*, no.296 (April 2005), Australian Institute of Criminology

Tony Krone and Gregor Urbas, "Mobile and Wireless Technologies: Security and Risk Factors", *Trends and Issues in Crime and Criminal Justice*, No. 329 (November 2006), Australian Institute of Criminology

Gilbert Leong, "The Computer Misuse Act 1993" (1993) 15(10) Eur.I.P. Rev.381

Selina Lum, "Firm takes systems engineer to court" *The Straits Times* (Singapore) (14 June 2008)

Conrad Raj, "Seven ex-Citibankers charged with stealing client information" *The Business Times* (Singapore) (24 January 2008)

Cheng Lim Saw and Susanna H.S. Leong. "Criminalising primary copyright infringement in Singapore: who are the real online culprits?" (2007) 29(3) Eur. I.P. Rev. 108

Russell Smith, Peter Grabosky and Gregor Urbas, *Cyber Criminals on Trial*, Cambridge University Press, 2004

Rajesh Sreenivasan, "Cracking the online vault" *Law Gazette*, October 2002 (5)

Mavis Tan, "Network service provider liability revisited" *Computer Law & Security Report* 19.4 (July-August 2003) 295

Irene Tham, "OK to share your neighbour's Wi-Fi if he says it's OK?" *The Straits Times* (Singapore) (29 July 2008)

Sujin Thomas, "High-tech crimes on prosecutors' agenda" *The Straits Times* (Singapore) (29 August 2008)

Gregor Urbas, "Cybercrime Legislation in the Asia-Pacific Region", in *Cyber Crime: The Challenge in Asia* (ed. R.G. Broadhurst and P.N. Grabosky), Hong Kong University Press, 2005, Chapter 12: pp. 207 – 241

Gregor Urbas, "Look Who's Stalking: Cyberstalking, online vilification and child grooming offences in Australian legislation", 10(6) (2007) *Internet Law Bulletin* 62

Wan Kwong Weng and Thomas Allen, "Computer software and Singapore's law of copyright" (1994) 16(11) Eur. I.P. Rev. 500

Katherine Williams and Indira Carr, "The Singapore Computer Misuse Act - Better protection for the victims?" (1994) 5 J.L. & Info. Sci. 210

Katherine Williams and Indira Carr, "A step too far in controlling computers? The Singapore Computer Misuse (Amendment) Act 1998" (Spring 2000) 8 Int J Law Info Tech 48