UiTM LAW REVIEW

ARTICLES

Irwin UJ Ooi	The Legal Status of Shipping Orders and the Shipping Manifest as Documents of Title under the Hague Rules in Malaysia
Jashpal Kaur Bhatt	The Legal Implications of the Changing Nature of Employment in Malaysia
Lim Heng Gee	Who is the Inventor under the Patents Act 1983? - The Concept of Invention and Inventorship
Michael Blakeney	Intellectual Property Traditional Knowledge and Genetic Resources
Mohammad Rizal Salim	Corporate Insolvency : Separate Legal Personality and Directors' Duties to Creditors
Mohd Darbi Hashim	The Social Dynamics of Law: An Inquiry into the Multiformity of Law in Contemporary Malaysia
Shad Saleem Faruqi	Secularism or Theocracy - A Study of the Malaysian Constitution
Sharon K Chahil	A Critical Evaluation of the Constitutional Protection of Fundamental Liberties in Malaysia : The Meaning of "Law"
Tunku Intan Mainura	Malaysia and the Law of Outer Space
Zaiton Hamin	The Legal Response to Computer Misuse in Malaysia - The Computer Crimes Act 1997

NOTES & COMMENTS

Irwin UJ Ooi	Sri Inai (Pulau Pinang) Sdn Bhd v Yong Yit Swee : The Duty of Care Owed by a Landlord to the Lawful Visitors of a Tenant

Vol 2 **2004**

ARTICLE

THE LEGAL RESPONSE TO COMPUTER MISUSE IN MALAYSIA - THE COMPUTER CRIMES ACT 1997

by *DR ZAITON HAMIN**

Introduction

Malaysia is embarking onto a massive and ambitious plan to become a fully developed nation with a value-based society by the year 2020. The Prime Minster, Dr Mahathir, had laid down the groundwork for this government policy in 1991 with his announcement of Vision 2020. The government perceives the application of information and communication technologies across both Malaysian society and economy as a means of achieving these goals and symbols of success.[1] Thus, the present thrust in Malaysia's development plans is to build a "knowledge-based economy" which leads to the establishment of a National IT Agenda (NITA) to formulate a combination of goals and means as the roles of information, knowledge and "echnopreneurship" working together to transform the economy into a "knowledge economy" (k-economy) and the society into a "knowledge society" (k-society).[2] To achieve these broad aims a legislative platform or what is termed by NITA, as "infostructure" is needed. Six cyber laws involving digital signature, computer crimes, telemedicine, and electronic government, copyright and multimedia convergence have been identified as necessary and were created since 1997.[3] The Computer Crimes Act 1997 was amongst the first to be enacted. It was published in the Gazette on 30 June 1997 and received Royal Assent on 18 June 1997. However, it only became enforceable three years later on 30 June 2000.

The purpose of this article is to critically examine the legal response to computer misuse in Malaysia as provided for in the Computer Crimes Act 1997 (hereinafter "the 1997 Act"). It seeks to examine the broad objectives of the 1997 Act. Also, it seeks to critically examine the statutory provisions contained therein in order to assess whether the 1997 Act can achieve these aims. The article is divided into four sections. The first section discusses briefly the political background of the creation of the 1997 Act, the legislative settings in which it was created and the broader objectives of the legislation. The second section critically examines its legislative

---

* Senior Lecturer in Law, Faculty of Law, Universiti Teknologi MARA, Malaysia, PhD (Leeds), LLM (King's College, London),LLB (Hons), DPA (ITM).

1 F Tipton, "Bridging the Digital Divide in Southeast Asia: Pilot Agencies and the Policy Implementation in Thailand, Malaysia, Vietnam and the Philippines" (2002) 19(1) *ASEAN Economic Bulletin* 83-99.

2 Ibid at 95.

3 See http://www.nitc.my.

scope having regard to the substantive offences, the evidential, procedural and jurisdictional issues involved. The third section offers some critiques for its improvement and the last section concludes the article.

Political Background of the Creation of the 1997 Act

Rapid economic growth in the early to mid-1990s has not only resolved many of the country's economic problems of the 1980s, but it had enabled the ruling party, Barisan Nasional, to consolidate its power. Towards this goal, Dr Mahathir created a vision of modernity for Malaysia, what he terms as 'Wawasan 2020' (Vision 2020),[4] which refashioned the relations between the state and the civil society.[5] The objective of this vision is Malaysia's emerging position as an economically developed and industrialised nation by the year 2020. Central to this undertaking is the Multimedia Super Corridor (hereinafter the "MSC"), a designated area of 750 square kilometer of high technology zone from Kuala Lumpur City Centre to the KL International Airport. The MSC was launched in 1997 amid much government-orchestrated fanfare with Dr Mahathir envisioning that it will be a "global gift to the information age".[6] Instrumental to its success is the participation of knowledge based industries such as Microsoft, Oracle and Silicon Graphics, which the government hopes would establish research and development facilities and make the MSC a hub for "software solutions". The MSC relies on the "hard" IT infrastructure as well as "soft" infrastructure to attract foreign investors.[7] The former relates to the modern high-speed telecommunication media links between all businesses, government offices and homes in the area and direct links to the rest of the world. The latter is concerned with business and investor-friendly incentives including tax exemption between 5 to 10 years, unrestricted employment of knowledge workers and non-censorship of the Internet. [8]

The "soft" infrastructure also involves the creation of two sets of forward-thinking cyber laws, commerce-enabling cyber laws and societal cyber laws.[9] On the one hand, the former are the Digital Signature Act 1997 which governs electronic signatures, the Copyright (Amendment) Act 1997 to enhance intellectual property protection and the Multimedia Convergence Act 1997 to streamline communication, information and broadcasting services. On the other hand, the latter are manifested in statutes such as the Computer Crimes Act 1997, which criminalises unauthorised access to and modification of computer contents and the Telemedicine Act 1997 that allow

---

4 See http://www.nitc.my.

5 KK John, The Malaysian Growth With Equity (GEM) Story: Leapfrogging to a K-Society. Paper presented at the *Asian Development Bank 3rd Annual Meeting of Board of Governors*, Hawaii, 7 May 2001 available at < http://www.nitc.org.my>.

6 "MSC given thumbs up by advisers", *New Straits Times* 2 February 1998 at 1.

7 Abdul Halim Ali, "Toward Malaysia's Knowledge Empowerment in the 21st Century" in *'Building Knowledge Societies: Access, Empowerment and Governance'* MIMOS available at http://www.nitc.org.my xiii.

8 Othman Yeop Abdullah, "Malaysia Plans for Technology Change" (1997) 67(11) *Australian Accountant* at 26-27.

9 N Annamalai, "Cyber Laws of Malaysia: The Multimedia Super Corridor" (1997) 12(12) *Journal of International Banking Law* 473-481.

remote provision of medical services. These legislative measures were introduced to reassure potential investors of the seriousness of the government in protecting technology and in the prevention of "cyber crimes".

Legislative Setting

The 1997 Act was drafted in early 1997 and was modeled after the UK Computer Misuse Act 1990. In contrast to the UK 1990 Act, the creation of the Malaysian 1997 Act was not preceded by a Law Commission report. The Computer Crimes Bill was tabled together with the Digital Signature Bill during the parliamentary session on 25 March 1997. The then Energy, Telecommunication and Post Minister, Datuk Leo Moggie presented it for the first reading and the House of Representatives passed the bill on 5 May 1997. One would observe that this is typical of the Malaysian law-creation practice, in that there was a lack of discussion and consultation with the public on the policy underlying the law. Any discussion of the social or legal implications of the proposed cyber laws was also lacking. Hence, its creation was shrouded in controversy, not so much from its criminalizing implications but from the secrecy in which it was introduced in Parliament.[10] Numerous calls from the opposition party for public discussions prior to its introduction in the Lower House in Parliament were rejected. The leader of the opposition party had called for the formation of a Parliamentary Cyber Law Committee, the function of which was to vet all cyber laws before being tabled in Parliament.[11] However, such call was largely ignored and the law was finally adopted in June 1997.

Legislative Goals

Although the creation of the 1997 Act was primarily aimed at criminalising hacking activities, which is intended to prevent and punish the perpetrators of computer crime,[12] the wider objectives of the 1997 Act cannot be denied. Given the social and economic conditions under which it was created, the 1997 Act together with other cyber laws proposed and/or created are also designed to establish Malaysia as a leader in the development of cyber laws.[13] Dr Mahathir had proposed that other ASEAN countries adopted the cyber laws that Malaysia had enacted.[14] To a large extent, the growth of these cyber laws was driven by the need to reassure major foreign investors in the MSC project that there is ample protection for intellectual property and the risks of computer crime.[15] The then Deputy Prime Minister, Datuk Seri Anuar Ibrahim, was

10 DL Beatty, "Malaysia Computer Crimes Act 1997: Gets Tough on Cyber Crime but Fails to Advance the Development of Cyber Laws" (1998) 7 *Pacific Rim Law and Policy Journal* 351.

11 "DAP Wants Public Discussions on Proposed Cyber laws", *New Straits Times*, 4 May 1997 at 8.

11 "DAP Wants Public Discussions on Proposed Cyber laws", *New Straits Times*, 4 May 1997 at 8.

12 Mahathir Mohamad, Speech by PM of Malaysia, M2 Presswire, 27 May 1997 available at LEXIS, World Library, M2pw File.

13 Mahathir Mohamad, "We Want to be a Leader in Cyber law Development", *FT Asia Intelligence Wire*, 1 June 1997, available in LEXIS, News Library, Aiwsel File.

14 "Malaysia Proposes Common Laws for ASEAN Covering Media Technology", *Agence Fr. Presse*, 18 May 1997, available in LEXIS, News Library, Afp File.

15 DL Beatty, n 10 at 353.

reported to say that the six proposed cyber laws in the form of "commerce enabling laws" and "societal laws" were vital in encouraging the use of electronic commerce and the provision of security to users of the Multimedia Super Corridor project.[16] In the course of winding up the debate on the Computer Crimes Bill, the Energy, Telecommunication and Post Minister reiterated that the creation of the 1997 Act was to ensure confidence amongst foreign investors in the MSC project that the Malaysian Government was serious in protecting the information technology industry.[17] Along the same lines, the *New Straits Times* stated that these "cyber laws are to attract and encourage corporations to use the MSC and turn Malaysia into the region's IT hub".[18] Ken Wasch, the President of Software Publishers Association was reported to say that Malaysia's cyber laws are "just the kind of legislation needed to lure operations of foreign IT companies into the country".[19]

The next section examines the scope of the 1997 Act and evaluates its merits as against these broad goals. Comparisons of the relevant provisions with similar provisions adopted in other jurisdictions and tested in the courts will be made in the evaluation of its potential efficacy.[20] Its internal consistency, clarity and transferability to other countries will be examined and compared to the recommendations of international organisations responsible for addressing cyber crimes in determining whether the 1997 Act promotes Malaysia's goals of becoming a leader in the development of cyber laws, which is one of the aspirations of Dr Mahathir.[21] However, whether or not the 1997 Act can provide reassurance to potential MSC investors can be assessed in the light of concerns expressed by businesses about computer misuse and crime and the 1997 Act's ability to address these concerns.

Legislative Scope

The 1997 Act is heavily modeled on the UK Computer Misuse Act 1990 with some modifications. The Act is the first Malaysian criminal statute designed to tackle the misuse of computers, creating four new offences of computer misuse, with attendant matters of jurisdiction and procedure. Divided into three parts, the preliminary matters contain short title and definitions. The second part provides for the offences relating to computer misuse and specific penalties for each offence. The last part deals with procedural and jurisdictional matters. We will now examine the provisions of the 1997 Act to determine the liability of computer users, the jurisdictional issues, the procedural matters, particularly the powers of the law enforcers, and the evidential issues that arise.

---

16 *The New Straits Times*, 26 March 1997 at 9.
17 *The New Straits Times*, 30 April 1997 at 12.
18 *The New Straits Times*, 4 March 1997 at 11.
19 Sharifah Kassim, "Attracting Software Vendors to Invest in Malaysia", *The New Straits Times*, 1 May 1997, available in LEXIS, Asiapc Library, Nstrit File.
20 DL Beatty, n. 10 at 358.
21 Ibid at 356.

Definitional Issues

Contrary to the UK 1990 Act, which provides no definition for the word "computer" the 1997 Act takes a different approach. Section 2(1) defines a computer as "an electronic, magnetic, optical, electro-chemical, or other data or processing devices, or a group of interconnected or related devices, performing logical, arithmetic, storage and display functions, and it 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 device".

The 1997 Act, however, excludes from the definition any "automated typewriter or typesetter, or a portable hand held calculator or other similar device which is non-programmable or which does not contain any data storage facility".[22] Any reference to a computer[23] in the 1997 Act would seem to include a computer network[24] as well.[25] This would include hubs and routers in the local area network and in the wide area network; the term 'computer' will cover the network management systems of the telecommunications service provider.[26] Unlike the Computer Misuse Amendment Act 1998 of Singapore (hereinafter "the CMAA 1998"), the 1997 Act does not provide for the ministerial power to extend the list of computer by official notification in view of rapid technological advances.[27]

Almost identical to the Singaporean counterpart, "data" is defined in section 2(1) as "representations of information or of concepts that are being prepared or have had had been prepared in a form suitable in a computer". Similarly, the meaning of "program" is identical to the Singapore 1998 Act. Section 2 (1) provides that "data representing instructions or statements that, when executed in the computer, causes the computer to perform a function". In line with the Singapore counterpart, the 1997 Act envisages removable storage facilities such as floppy disks and tapes. Section 2(6) provides that any program or data held in a computer includes reference to those held in any removable storage medium, which is for the time being in the computer.

Criminalising Unauthorised Access

Section 3(1) of the 1997 Act which is identical in its wording to the 1990 Act[28] provides for the criminalization of any intentional access to a computer without authorization. Intended to act as a general deterrent and to criminalise any form of hacking, the punishment of a maximum fine of RM50, 000 or a maximum

---

22 1997 Act, section 2(1).

23 For the operations of a computer, see *Creative Purpose Sdn. Bhd. V Integrated Trans Corp Sdn. Bhd.* [1997] 2 MLJ 429, following *Ibcos Computers Ltd v Barclays Mercantile Highlands Finance Ltd* [1994] FSR 275.

24 Defined in section 2(1) of the 1997 Act as 'the interconnection of communication lines and circuits with a computer or a complex consisting of two or more interconnected computers.'

25 1997 Act, section 2(10).

26 J Ding, *E-Commerce: Law and Practice* (Sweet & Maxwell [Asia] Kuala Lumpur 2000) at 265.

27 CMAA 1998, section 2 (1)(d).

28 1990 Act, section 1(1).

imprisonment of five years or both, which was provided for in section 3(3) is rather harsh. The offence can be committed if the perpetrator "causes a computer to perform any function".. Securing access [29] to a program[30] or data is completed where the accused, by causing the computer to perform any function, alters or erases the data or program, copies it, moves it, uses[31] it or displays it.[32]

Similar to the Singapore Computer Misuse (Amendment) Act 1998, the prosecution must prove that the accused intends to secure access and that he knows that the access he intends to secure was unauthorised.[33] It is immaterial whether he succeeds in obtaining such access. The offence is to cover cases where the ultimate target computer may be unknown to the perpetrator. Although this type of criminalization of simple hacking without proof whether or not security measures were circumvented are similar to the legal provisions of some states in the USA,[34] it goes beyond the Organisation for Economic Cooperation and Development (OECD) recommendation which provides that hacking is an offence if security measures such as password protection are encroached in order to gain access to the computer.[35] The recent Council of Europe Convention on Cyber Crime in 2001 contains a similar proposal. Article 2 proposes that illegal access is when it is "committed intentionally the access to the whole or any part of a computer system without right' and it may be committed by infringing security measures".[36]

By section 2(5) access is "unauthorised" if the person gaining access does not have control over the kind of access and either the person does not have consent to the kind of access, or he/she has exceeded the consent given to him/her for that kind of access. In cases where consent has been obtained, access may still be unauthorised if the person has exceeded such consent or right to access. Such a provision of access in excess of consent or authority is evidently an extension of the UK 1990 Act, which merely provides that for unauthorised access,[37] the accused is not entitled to control access to the program or data and he/she does not have the necessary consent from any one who is entitled to give it. When using the computer at work employees may be committing this offence if they intend to access any program or data, which to their knowledge they do not have the authority to access.

---

29 The circumstances of securing access for the purpose of the Act are defined in section 2(2), further elaborated in (3) and (4).

30 "Program" includes "part of a program": section 2 (9).

31 Section 2(2)(c) extended by section 2(3) that states that using a program involves causing the program to be executed or the function in itself a function of the program.

32 1997 Act, section 2(2)(a)(b)(c)(d).

33 This is similar to section 1(a)(b)(c) of the Computer Misuse Act 1990.

34 This is similar to Californian Penal Code 5029(c) and Iowa Code 716A.2.

35 The minimum list of offences in Recommendation No. R (89) 9 OECD includes unauthorised access in which the access must be 'access without right to a computer system or network by infringing security measures' in International Review of Criminal Policy: United Manual on the Prevention and Control on Computer-related Crime (hereinafter "the UN Manual") available at http://www.ifs.unvie.ac.at/pr2gq1/rev4344.html/crime.

36 Council of Europe, *The Convention on Cyber Crime (ETS No 185)*, available at http://conventions.coe.int/treaty/EN/cadreprojets.htm.

37 1990 Act, section 17(5)(a)(b).

The criminalisation of mere hacking, which has been considered as "bold and decisive"[38] would augur well for reassuring potential investors in the MSC that anti-hacking law in Malaysia is punitive enough. It is the preferred mode of legislative strategy because more often than not hackers access one computer in order to gain access to another computer, sometimes more than once.[39] This method of attack is taken to take advantage of the existence of the "trusted system",[40] which saves hackers the trouble of cracking the password of the second system. This would also enable them to cover their electronic tracks and make it more difficult to identify them. However, Section 3 has been criticised by many, including the leader of the opposition party, as being too harsh, which tends to criminalise young computer hobbyists, who have gained unauthorised access without malicious intent or causing damage to the computer.[41] He suggested that the Malaysian government should adopt a system based on the Hawaiian legislation, empowering the court to dismiss a prosecution for unauthorised access with no malice or no damage to the computer.[42] The criminalization of mere hacking in 1997 Act was criticised for being too wide and bringing accidental or unintentional unauthorised access into the purview of the law. The 1997 Act will now cover cases where a person is unknowingly led to access unauthorised data. For example, some Internet user might, during a relay chat session receive an Internet address with a user ID and password to access a particular website. Once he gains access he has committed an offence.[43]

The offence of unauthorised access with intent in section 4(1) is considered more serious than the section 3(1) offence. As such, the penalty under section 4(3) is more severe than mere unauthorised access which is a maximum imprisonment of ten years or a maximum fine of RM150, 000 or both. Section 4 envisages several ulterior offences involving the *mens rea* of fraudulent intention,[44] dishonest intention[45] or causing injury.[46] If for example, an insider or external hacker who has gained

---

38 DL Beatty, n 10 at 360.

39 See Carolyn Hong, "Keeping Hackers at Bay with Help of New Organisation", *New Straits Times*, 23 March 1997 at 13, available in LEXIS, Asiapc Library, Nstrt File.

40 A "trusted" computer is one, which is able to connect with another computer, which recognises its Internet Protocol address number.

41 *The New Straits Times*, 24 April 1997 at 9.

42 Ibid.

43 *The Star*, 1 April 1997 at 6.

44 Section 25 of the Penal Code defines 'fraudulently' as 'if he does that thing with intent to defraud, but not otherwise'. Offences involving fraud includes cheating (s 415), forgery and counterfeiting of currency notes or documents (Chapter XVIII), fraudulent deeds and disposition of property (ss 421-424).

45 "Dishonestly' is defined in section 24 of the Penal Code as 'whoever does anything with the intention of causing wrongful gain to one person, or wrongful loss to another person, irrespective of whether the act causes actual wrongful loss or gain. Section 23 further defines 'wrongful gain' as 'gain by unlawful means of property to which the person gaining is not legally entitled.' Examples of such gain are when there is wrongful retention and acquisition of property. 'Wrongful loss' is defined in section 23 as 'loss by unlawful means of property to which the person losing it is legally entitled.' Examples of such loss are when the victim is wrongfully kept out of any property and wrongfully deprived of it. Offences involving dishonesty includes theft (ss 378-382), extortion (ss 383-389), robbery (ss 390-402), criminal misappropriation (ss 403-404), criminal breach of trust (ss 405-409), receiving stolen property (ss 410-414), dishonest cheating (s 420), cheating by personation (s 419).

46 Injury in section 44 of the Penal Code is defined as 'any harm illegally caused to any person, in body, mind, reputation or property'. Offences involving injury includes voluntarily causing hurt (ss 321 & 323), voluntarily causing grievous hurt (ss 322 & 325), causing hurt or grievous hurt by dangerous weapons or means (ss 324 & 326), causing hurt or grievous hurt endangering life (ss 336-338).

unauthorised access to a computer or its systems diverts funds from some other person's bank account into his/her own account, he/she would now run foul of section 4(1).

The element of "causing injury" in section 4(1) suggests that while the protection of property is uppermost for this type of offences, the protection of the person is not neglected.[47] Otherwise, a more serious offence involving injury to human lives such as murder[48] or culpable homicide not amounting to murder,[49] which resulted not merely in injury but death, would in effect be excluded. Similar to the 1990 Act,[50] sections 3 and 4 would seem to be hierarchical, in the sense that failure to convict under section 4 would enable an alternative prosecution under section 3. This is so because obtaining unauthorised access initially is a prerequisite to section 4.

The offence appears to catch offenders who merely prepare to commit further offences but have not attempted to do so.[51] This would in effect remove the limitation of the traditional law of attempt in dealing with the activity at which the new law is directed. Suppose a hacker hacks into a computer to obtain confidential information intending to blackmail someone. He is not guilty of attempted extortion as his conduct is merely preparatory to extortion, but he would be guilty of unauthorised access with intent to extort under the new section 4. Significantly, this aggravated offence of hacking is in line with OECD recommendations, which do not limit criminalization to occurrence when the computer being accessed was secured.[52]

Criminalizing Unauthorised Modification

Section 5(1) offence is directed at the increasing practice of active interference with a computer data or programs. It creates an offence of unauthorised modification of the contents of a computer if the person knows that his/her act will cause an unauthorised modification of program and data, even if the person does not target a specific data or program. This would suggest that the Malaysian provision is restricted only to computer program or data and is not as wide as the UK provision to cover the machine itself, which is any particular computer.[53] The wording of the 1997 Act is rather different from the 1990 Act whereby nothing short of intention suffices. However, under the 1997 Act mere knowledge that an act causes unauthorised modification is sufficient to constitute the simple offence. The excluded *mens rea* which is evident under the UK law refers to the intention of the accused to impair the computer's operation, hinder access to computer material by a legitimate user or

47 Mah Weng Kai, Computer Crimes Act 1997. Paper presented at the *Seminar on Cyber Laws in Malaysia*, organised by the Bar Council Malaysia, 29 November 1997, Bar Council Auditorium, Kuala Lumpur, Malaysia.
48 Penal Code, section 300.
49 Penal Code, section 299.
50 Sections 1 and 2 of the 1990 Act is hierarchical.
51 1997 Act, section 7(2).
52 See the UN Manual para 118 at 23.
53 See 1990 Act, section 3(3)(a).

impair the operation or the reliability of computer held material.[54] In *Lai Fook Kee v PP*[55] the court seems to suggest that the word "knows" should bear its ordinary meaning and that it should be conscientiously made.[56]

The "modification" in section 2(7) occurs where a function[57] of the "target" computer itself is operated. Such effects of the modification under the Malaysian law is limited, as it merely requires that any program or data held in any computer is altered or erased,[58] or introductions or additions are made to its contents[59] or any occurring events, which impairs the normal operation of any computer.[60] However, unlike the 1990 Act, section 5(1) does not extend the effects of the modification to those acts, which "prevent or hinder access to any data or program or impair the operation of any such program or the reliability of any such data".[61] The simple offence in Section 5 would cover cases where the defendant knowingly introduces a computer "worm" [62] or a "virus" [63] into a computer system, without impairing the operation of any program or data. In the former case such a program uses up all the spare capacity on the computer by adding programs or data to the computer's contents[64] thereby impairing the operation of the computer. In the latter case some viruses might be schoolboy pranks but some may contain time bombs, which on a certain date performs a task such as printing a message or destroying data.

The effects of section 5(1)

What would the position be in Malaysia if a case such as *Turner,*[65] where a hacker who has gained an unauthorised access into another person's computer was to encrypt the data, rendering the data inaccessible to the users? Or a similar case such as *Goulden,*[66] where a disgruntled former employee/consultant, used a "logic bomb"[67] to hinder access to information stored on the employer's computer system? On the one hand, it could be contended that as long as the offender does an act, which he/she

---

54 1990 Act, section 3(2).

55 [1970] 1 MLJ 134, *per* Abdul Aziz J at 136.

56 Ibid. The court cited and followed *London Computator Ltd v Seymour* [1944] 2 All ER 11 and *Sinniah Sokkan v PP* [1963] MLJ 249.

57 Defined in section 2(1) as "logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer".

58 1997 Act, section 2(7)(a). See also 1990 Act, section 17(7)(a).

59 1997 Act, section 2(7)(b).

60 1997 Act, section 2(7)(c).

61 1990 Act, section 17.

62 Defined as "a destructive program containing code that replicates itself until it fills the target drive or network, thereby causing it to malfunction" in *Computing Dictionary: The Book of Terms and Technologies* (PC Novice/ Smart Computing 1997) at 237.

63 Ibid at 232 defined a virus as "a program designed to destroy or halt operation on systems by copying itself into files and executing when those files are loaded".

64 1997 Act, section 2 (7)(b).

65 (1984) 13 CCC (3rd) 430.

66 Unreported, 1992, Southwark Crown Court.

67 GS Howard, in *Introduction to Internet Security* (Rocklin Prima Publishing California 1995) defines it as a type of attack which is detonated by the occurrence of some specified date, time or event (eg, after the execution of a certain program, after a certain user logs on or after disk consumption reach a specific level), resulting in erasure of data, system shutdown, or viral incubation or proliferation.

knows will cause an unauthorised modification he/she is guilty of an offence under section 5(1), irrespective of what his/her intention is or the consequences of his/her act. On the other hand, if such acts do not modify the materials one could argue that they do not come within the ambit of section 5.

Section 3 of the UK 1990 Act, which is similar to section 5, has been successfully applied in the case of *Pile*,[68] involving a virus writer who published several viruses on the Internet, from where many corporate computers were infected and costing considerable damage to those companies. He was sentenced to eighteen months imprisonment. If such a case were to occur in Malaysia, a similar result could well be achieved by applying section 5. The creation of a statute that is textually similar to the 1990 Act, which was used to obtain a successful conviction against a computer criminal, should provide some sense of security to MSC potential investors that the Malaysian law is effective and that the protection of their interests is paramount to the government.[69]

The 1997 Act is in a similar vein to the 1990 Act due to the broad scope of the offence that extends to "any act that contributes towards causing such a modification shall be regarded as causing it".[70] By section 5(3) it is irrelevant whether the modification is permanent or temporary. The offence might be made out if a person enters a virus onto a floppy disc and then puts that disc into circulation with the result that ultimately a computer somewhere becomes infected with the virus.[71] This is because such an act could constitute an "act which contributes towards causing such a modification" and "shall be regarded as causing it".[72] However, for the offence to be made out the prosecution must prove a causal relationship between the act and the effect it possesses (i.e. of modifying the computer contents).[73]

According to section 2(8) modification is "unauthorised" if the accused is not personally entitled to determine whether it should be made and he/she does not have the necessary consent from anyone who is entitled to give it. For this offence the concept of authority without consent or authority is similar to the UK position.[74] As opposed to the 1990 Act, which applies a similar type of authority for both the offences of unauthorised access and unauthorised modification, one would observe that the Malaysian law provides a different concept of authority for both the offences. For unauthorised access the concept of authority is wider than that for section 5 offence, because it encompasses those who are not entitled to control access to program or data; or those who do not have consent; or those who exceed any right or consent given to him. This last requirement of access in excess of authority appears to

---

68 Unreported, see "Programmer jailed for planting computer viruses", *The Times*, 16 November 1995, at 12.
69 DL Beatty, above n 10 at 362.
70 1997 Act, section 2(7). See also 1990 Act, section 17 (7).
71 Contrast J Ding (2000), n 26 at p 277, who contends that the introduction of virus via a disk & placing it for circulation may hot be caught by section 5 due to insufficiency of cause and effect. Such an interpretation, however, might be correct if it is read within first part of section 2(7) (a), (b), and (c).
72 1997 Act, section 2(7)(c).
73 J Ding, n. 26 at 277.
74 1997 Act, section 17.

be missing from the unauthorised modification offence. During the tabling of the Act there was no plausible policy reason given by the relevant minister for the distinction in the concept of authority in sections 3 and 5.

Unlike the 1990 Act, the Malaysian statute provides for a specific offence of unauthorised modification with intent to cause injury[75] suggesting the primacy of human life. The more severe punishment (a maximum imprisonment of ten years and/or a maximum fine of RM150, 000 or both) than the simple offence (a maximum imprisonment of seven years or a maximum fine of RM100, 000 or both) also indicates that it is an aggravated offence.[76] While the OECD recommendation includes modification of program or data for purposes of committing an illegal transfer of funds or thing of value, committing a forgery and intending to hinder the functioning of a computer or telecommunication system,[77] the Council of Europe Select Committee on Crime Problem recommendations included alteration of computer data or program.[78] In this respect the Malaysian provision is more restrictive than these recommendations because the unauthorised modification need not damage a computer system or impair its functioning. As such, a person can be theoretically prosecuted for releasing a virus even if the virus is non-destructive.

The Convention on Cyber Crimes in 2001 provides extensive recommendations for unauthorised modification. Article 4 proposes an offence relating to data interference when the act is committed intentionally to damage, delete, deteriorate, alter or suppress data.[79] Article 5, which seeks to prevent system interference, recommends that it is an offence to intentionally and seriously hinder the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.[80] In view of this legal development that is to cater for Internet-related behaviour, it would be beneficial for Malaysia to review the 1997 Act and to extend the protection to any computer (as in the 1990 Act). Not only would such step broaden the scope of protected components, it would also add clarity to the 1997 Act. This would bring the law more in line with many developed nations and with the developments of the Internet.

Criminalizing Wrongful Communication of Password etc.

This offence seems to aim at rectifying any weakness in the computer security and at reducing the risks of unauthorised access in any organisation. The UK law, however, is notably silent on this point. Section 6(1) makes it an offence to disclose any means of access such as a code or password to an unauthorised person and the penalty provided for such act is a maximum imprisonment of three years or a maximum fine

75 Section 44 of the Penal Code.
76 1997, section 5(4).
77 UN Manual, n 36 para 118 at 23.
78 Ibid, para 118 at 23.
79 The Convention on Cyber Crimes 2001, n 37 at 6.
80 Ibid at 6.

of RM25, 000. In contrast to the new Singapore provision[81] that requires knowledge and lack of authority, there seems to be no requirement as to the *mens rea* in section 6. The question then is whether this section is creating a strict liability offence. One could argue that the presumption against such an offence that is applicable in the UK, similarly applies in this situation.[82] The fact that the provision contains a criminal offence[83] as opposed to a quasi-criminal or civil one, the mischief of the crime,[84] the maximum punishment[85] provided and the view that a strict liability might not assist in the enforcement of the law,[86] would suggest that the Malaysian Parliament did not intend a strict liability offence.[87] Moreover, carelessness or inadvertence might not suffice, as the word "wrongful" would indicate the requirement of some kind of culpability on the part of the perpetrator. One commentator has contended that intention would be required for this offence.[88] However, in view of the fact that the penalty provided for this offence is much less severe than the three other offences, perhaps knowledge or a *mens rea* that is similar to the Singapore statute would be adequate.

If the government's intent was to create a strict liability offence concerning this offence, then that intent should be clearly stated. The decision whether or not mens rea applied should not be left to the discretion of the judiciary. Trial judges might find it difficult to sentence an accused person who has no intention of committing the offence with which he/she is charged.[89] Although a strict liability offence might work in favour of the prosecution as it removes the burden of proving the defendant has the necessary mens rea,[90] it can be an inadequate measure for retributive, deterrent and rehabilitative purposes.[91] The imposition of strict criminal liability would be wide enough to cover mistakes made by employees and others and this is of questionable value.[92] This provision lacks clarity and can be subject to different interpretations, which could undermine the ability of Malaysia to become a leader in the development of cyber laws.

The OECD and the Council of Europe did not include this provision in their recommendations. However, the Convention on Cyber Crimes 2001 has recommended that intentional production, sale, procurement for use, import, distribution and possession of computer password, access code or similar data with the intention of using them in the commission of a crime is unlawful. This in effect would criminalise the conduct such as the publication of lists of passwords or compilation of a program such as "password sniffer" that can be used in attempting to discover valid passwords

---

81 SCMA1998, section 6B.
82 See *Sweet v Parsley* (1970) AC 132.
83 See *Sherras v De Rutzen* [1895] 1 QB 918, [1895-96] All ER Rep 1167.
84 *R v St Margaret's Trust* [1957] 2 All ER 289.
85 *Warner v Metropolitan Police Commissioners* [1969] 2 AC 256.
86 *Lim Chin Aik v R* [1963] 1 All ER 223.
87 For a similar view see J Ding, n 26 at 279-280. Contrasting view can be found in Mah Weng Kai, n 47 at 8.
88 J Ding, n 26 at 281.
89 LL Levenson, "Good Faith Defences: Reshaping Strict Liability Crimes" (1993) 78 *Cornell Law Review* 401.
90 Ibid at 404.
91 AA Cuomo, "Mens Rea and Status Criminality" (1967) 40 *South Carolina Law Review* 516-22.
92 Ibid at 522.

relating to a particular Internet site.[93] In view of this recent development there is a stronger case for removing the ambiguity relating to the *mens rea* requirement in the offence of wrongful communication of password to unauthorised person. There is also a need to keep abreast with the risks of Internet-related conduct because the Internet does present challenges to the efficiency of "new" computer crime laws such as the 1997 Act.

In contrast to the Singapore provision,[94] which requires that disclosure relates to any password, access code or other means of gaining access to a program or data held in any computer, the Malaysian statute states that such disclosure must relate to a computer *per se*. This would suggest that the latter law is broader than the former in that it would be sufficient if the code, password etc. allows access to be obtained. It would appear to be immaterial whether further acts are required to gain actual access to the program or data. In view of the wide definition of "computer" in the 1997 Act, one could contend that even causing a telephone company to make a connection may fall foul of the section, as that company can "by other means" cause or enable access to a computer to occur. As opposed to the Singapore statute, which provides that disclosure is for any wrongful gain, or unlawful purpose or wrongful loss to any person, section 6 does not provide for any purpose. As such, disclosure to unauthorised person for any reason could fall within the ambit of the law.

Inchoate offences issues

Unlike the 1990 Act, the 1997 Act is in line with the Singapore counterpart, regarding making it an offence to abet the commission of, or to attempt to commit, any offences under the Act. Section 7 provides that anyone who abets the commission of an offence under the Act, or does any act preparatory to or in furtherance of an offence, is guilty of the substantive offence.[95] Abetting or attempting to commit an activity criminalised by the Act is punishable by the same penalty as the substantive offence.[96] Preparatory acts or acts in furtherance of an activity criminalised by the Act are punishable by half the maximum imprisonment term of the substantive offence, the full fine or both.[97]

This section envisages three stages of conduct, namely the preparatory acts, attempts and finally the commission of the offence. In view of the drafting of section 7, preparatory or preliminary acts could occur at the moment the computer is activated, in the case of an employee using a stand-alone system or when a log-in password is imputed via another computer, in the case of an external hacker.[98] Similar to above-mentioned section 4, this section would seem to bring forward the point in

93 IJ Lloyd, *Information Technology Law* (Butterworths London 2000) at 253.
94 SCMA, section 6B.
95 1997 Act, section 7 (1).
96 Ibid.
97 1997 Act, section 7(2).
98 Mah Weng Kwai, n 47 at 9. Cf J Ding, n 26 at 283-284.

time at which an offence may be said to have been committed.[99] Hence, the effect of this section would be that acts that do not amount to attempts, but are merely preparatory could still attract criminal liability by virtue of section 7 being read together with other substantive sections. Section 7(2) provides for a jail sentence but is silent as to the fines. Hence, one could speculate that the maximum fine that the court can impose is still intact. This would mean that the court could impose the maximum fine rather than half of the sum permitted under the penalty section.

Furthermore, there is an apparent inconsistency between section 7 and section 6. Given that the latter criminalises the unauthorised communication of passwords or computer access coded it is rather difficult to construe the scope of section 7's anti-abetting provision. According to the basic principles of statutory presumption where inconsistency within a statute occurs the Act must be taken as a whole. Thus, in order to give effect to the term "any act in furtherance" in section 7 it must be interpreted narrowly, which could mean that several activities might not be caught by section 7, as they are not "an act in furtherance" of section 6 offence. These could include password trafficking or deliberate insertion of "trap door" into the operating system, a program that allows everyone with a predetermined access code to log into the affected system. This instrumental inconsistency has led to the view that "Malaysia cannot expect to be considered a leader in this area of law when it adopts seemingly conflicting provisions that judges of other nations might not be able to reconcile".[100]

Jurisdictional Issues

Computer crime presents a problem in jurisdictions because under the general principle of criminal procedure, criminal offences can only be prosecuted in the *locus delicti*. However, in such cases it may be difficult to determine the locus of the defendant's hacking activity. The problem for the law enforcer is compounded by the fact that the courts have traditionally determined the "loci" by reference to the place where the activity was "completed". Now the problem with this is that the perpetrator can be located in one jurisdiction, access a computer in another jurisdiction and the hard copy representation of the hacker's activities might be produced in another jurisdiction.

The 1997 Act contains provisions directed at computer crime across international boundaries. Section 9 extends the jurisdiction of Malaysia to the offender under the Act if the computer, program or data accessed or modified was in Malaysia or capable of being connected to, sent to, used by or with a computer in Malaysia at the material time.[101] In contrast to the detailed, complex and cumbersomely worded provisions of the 1990 Act, the new provisions in the 1997 Act are simpler. The extra-territorial

99 CMA 1990, section 2(1)(b).
100 BL Beatty, n 10 at 365.
101 1997 Act, section 9 (1) and (2).

nature of the offences is recognised and that nationalities other than Malaysians are still liable to prosecution for offences that are committed under the 1997 Act.

At first glance, section 9(2) suggests that the Malaysian courts will have jurisdiction in respect of the four new computer crimes (together with their inchoate offences), where a significant link exists with domestic jurisdiction. Such a link is established if either the computer crime originates in Malaysia or is directed against any computer systems in Malaysia, or even if Malaysia is only used as a transit point. This would mean that prosecutions could be made where either the accused or the victim computer was within the Malaysian jurisdiction at the time of the offence. Additionally, even the physical location of the program or data would be sufficient to found jurisdiction.[102] Alternatively, the words "capable of being connected to or sent to" would suggest that the Malaysian courts would have jurisdiction even where the country is used as a transit point. This is an extension of the UK position in that not only would physical presence suffice but a mere transient presence would also be adequate.[103] However, on closer scrutiny the provisions are not only wide but also problematic as any computer in Malaysia with Internet connections can be accessed by, or receive a program or data from any other computers with similar capabilities. As a result, Malaysian law applies to any hackers who access or infect any computer, whether or not a Malaysian computer is ever involved in, or affected by, the activity.[104]

However, jurisdiction is subjected to the principle of double criminality. This means that if the perpetrator is operating within Malaysia, but the criminal intent envisaged by him will occur abroad, the Malaysian courts would only have jurisdiction where the contemplated conduct was a criminal offence in that other country as well as in Malaysia.[105] The 1990 Act contains appropriate extradition provisions to facilitate prosecutions in such cases. However, unless there are proper extradition treaties between Malaysia and other countries, a criminal action against a foreign hacker might be difficult to prosecute even though it has been detected. The existing extradition legislation will have to be reviewed to include computer crime as one of the extraditable offence.[106]

The adoption of these provisions suggests that just as the case of the USA, Malaysia is circumventing the principle of territoriality, a generally accepted principles in criminal jurisdiction doctrine.[107] Mutual respect for the state sovereignty is the premise upon which this doctrine is based and it is allied to the principle of non-interference in the exclusive domain of other states.[108] However, there are certain exceptional circumstances justifying the adoption of extra-territoriality such as the nationality of

102 J Ding, n 26 at 285.
103 For a similar view see ibid at 285.
104 DL Beatty, n 10 at 365.
105 1997 Act, Section 9(3).
106 Extradition Act 1992.
107 UN Manual, n 35 at para 249.
108 Ibid at para 249.

the accused, nationality of the victim, the protection of national security and the protection of universal values.[109] Despite the absence of international law to restrict the application of extra-territoriality, the UN has suggested that states are expected to take into account the principles of co-operation and reasonableness in exercising such jurisdiction.[110] One could speculate the difficulty that the Malaysian police would encounter in enforcing the 1997 Act beyond its border without the international co-operation and mutual assistance.[111] This wide and unrealistic assertion about jurisdiction does not augur well for the aspiration of the political leadership into making Malaysia as a leader in cyber law reforms.

Evidential Issue

A unique feature of Malaysian law is the provision for the burden of proof relating to unauthorised access. The UK and the Singapore counterparts are silent on this point. Such a burden is made easier for the prosecution by the unique requirement of section 8, which provides that a rebuttable presumption of unauthorised access arises unless the contrary is proved, upon proof of these elements: a) that the accused must have in his custody[112] or control,[113] any program, data or other information; b) that the program, data or other information which he has in his custody or control is one which he is not authorised to have and c) that the program, data or other information is held in any computer or is retrieved from any computer.

Put simply, section 8 creates a statutory presumption that anyone who has unauthorised custody or control over information held in a computer has obtained unauthorised access to that information. The accused is deemed to have obtained the program etc through unauthorised access if the defence is unable to adduce sufficient evidence to show that he did not have custody or control of the program etc, or that he is duly authorised. Neither the OECD nor the Council of Europe has included this presumption in their recommendations.[114] This section is said to be the most beneficial provision "both in the prevention of computer crimes and in instilling investor confidence"[115] particularly, in preventing software piracy and theft of trade secrets, two important concerns of the foreign investors in the MSC.

One of the foreign participants in the panel discussion on the MSC was reported to say that assurances that trade secrets and other technology would be protected were crucial to Malaysia's ability to attract foreign companies to the MSC.[116] The Energy,

---

109 Ibid at para 255.
110 Ibid at para 259.
111 Ibid at paras 245-88.
112 In *PP v Ang Boon Foo* [1981] 1 MLJ 40, Gunn Chit Tuan J suggests that "custody" requires some elements of care and that the custodian has no power of disposal. J Ding on the other hand suggests that "custody" implies *de facto* possession of the thing in question. See J Ding, n 6.
113 In *PP v Ang Boon Foo* [1981] 1 MLJ 40, Gunn Chit Tuan J held that "control" requires more than mere knowledge and that there was dominion over the thing in question. He suggests that the person must have knowledge of its whereabouts, had access to it and could at any time have possession of it or capacity to direct its disposal.
114 UN Manual, n 35 at paras 118-122.
115 DL Beatty, n 10 at 365.
116 Cheah Chor Sooi, "Special Legislation Needed for MSC", *New Straits Times*, 30 September 1997, at 38.

Telecommunication and Posts Minister had reiterated that "software piracy in Malaysia is not as serious as in other countries, yet the country must strive to curb the problem in order to protect the country's software industry, particularly in view of the MSC development".[117] The section has been perceived as giving "added ammunition to the current campaign to wipe out software piracy' which previously had to shoulder the burden of proving that the "errant party actually committed the act of piracy".[118] The added ammunition to section 8 in preventing software piracy is the criminalization of knowingly possessing illegally obtained software, which inevitably will bolster the confidence of MSC investors that software piracy is taken seriously in Malaysia.[119] The fact that in Malaysia external economic pressure, in particular from the USA, has been the impetus for the growth of cyber laws such as the 1997 Act is reminiscent of the Indonesian experience whereby legal reform in intellectual property was driven by the US government offensive actions over abuse of intellectual property rights in South East Asia in mid-1980s.[120]

Contrary to this, section 8 has been criticised in that it may also criminalise systems owners whose systems are being used by hackers to deposit information retrieved from other less accessible systems because under section 8 an unknowing owner of the deposit site would be presumed to have obtained unauthorised access to that program.[121] The Opposition Party leader has, in Parliament, also criticised section 8 for its potential in criminalizing many computer users and that the government has not given any good reasons for its inclusion in the 1997 Act.[122]

The 1997 Act is silent on the provision of evidence of computer crime, which together with the issues of detection and prosecution, will take a centre stage once the legislation is enforced. This is perhaps intentional in view of the existing rules on computer evidence under the Evidence Act. The UK position is similar. The admissibility of computer-generated evidence is governed by section 69 of the Police and Criminal Evidence Act 1984, which provides that statement in a document produced by computer shall not be admissible in evidence unless it is reliable. Yet, recent decisions indicate that the section does not apply where a computer printout is tendered as real or original evidence and no hearsay rule exists.[123]

The nature of "evidence" for a successful prosecution of the new hacking offences can be a problem to the enforcement agencies. In all cases of computer intrusion, the target computer's electronic log files and audit trails are crucial and sometime the only indication of intrusion. However, owing to the nature of electronic data, the

---

117 Sharifah Kassim, "Delay in Cyber Law Implementation", *New Straits Times*, 2 December 1996, at 1 available in LEXIS, Asiapc Library, Nstrtt File.

118 "Bill Deals Blow to Hackers, Software Piracy" *New Straits Times*, April 6 1997, at 31 available in LEXIS, Asiapc Library, Nstrtt File.

119 DL Beatty, n 10 at 366.

120 A Rosser, "Intellectual Property Reform in Indonesia" in K Jayasuriya (ed) *Law, Capitalism and Power in Asia: The Rule of Law and Legal Institutions* (Routledge London 1999).

121 D Nair, "Cyber law Makers Must Look Into Hackers Minds" *FT Asia Intelligence Wire*, 25 April 1997, B41.

122 *The New Straits Times*, 24 April 1997, at 3.

123 *Sophocleus v Ringer* [1987] Crim LR 422. See also *Minors & Harper* [1989] 2 All ER 208.

operators of the target server or even the hacker himself/herself are in a position to modify and change the content of the log files, before, during and after the intrusion process. As such the accuracy or the integrity of the log files and other similar data can be compromised and cannot be guaranteed. Some experts have even suggested that due to its vulnerability to manipulation such logs should not be admissible as evidence in the court.[124] Furthermore, some computer experts have criticised the Act in failing to clarify the lines between evidence and identity. As computer surfers are bound to copy or modify information on the Internet for their own benefit, this blurs the identity lines. The problem is how they can be tracked down when the data or content need not be physically removed for unauthorised access to be detected.[125]

It is significant to ascertain at first instance whether the device or equipment in question is a "computer" before considering the elements constituting the offence. This is because it is without doubt that a computer is a "document" for the purposes of the Malaysian Evidence Act 1950. However, the definition of a "computer" differs from the one in the 1997 Act. Section 3 of the 1960 Act states that:

> A computer means any device for recording, storing, processing, retrieving or producing any information or other matter, or for performing any one or more of those functions, by whatever name or description such device is called; and where two or more computers carry out any one or more those functions in combination or in succession or otherwise howsoever conjointly, they shall be treated as a single computer.

Sections 90A, 90B and 90C of the Malaysian Evidence Act 1960 pave the way for documentary hearsay evidence produced by computers, i.e. computer printouts, to be admissible in a criminal trial as of right, subject only to the limitation imposed by the said sections. The effect of these sections was to enable computer-generated records and information to be admissible as evidence without the maker of the document (the person who actually type the document) being called as a witness, as he/she may not be found or not in a position to be called. Consequently, this would bring the evidential requirement of the "best evidence rule" up to date with the realities of the electronic age.[126]

Section 90A is an exception to the hearsay rule and provides that a statement in a computer record is admissible as evidence of the facts contained, provided it was recorded in the course of its ordinary use.[127] For the document to be admissible it is sufficient if the person who is responsible for the operation of the computer gives a certificate stating that to the best of his knowledge and belief it was made in the course of its ordinary use.[128] This section cannot be relied on by the accused if he/she

---

124 Dinesh Nair, *The Star*, 26 April 1997, at 5.
125 *The Star*, 1 April 1997, at 7.
126 *Gnanasegaran v PP* (1997) 3 MLJ 1, *per* Shankar J at 14A. See also J Ding, n 26 at 129.
127 1950 Act, section 90A (1).
128 1950 Act, section 90A (2).

was directly or indirectly involved in the production of the said document. This is to avoid self-serving evidence, which, if allowed can be used at will. Thus if the printouts were prepared by the opposing party, then they will be admissible under this section.

In the significant case of *Gnanasegaran v PP*, a case concerning breach of trust involving computerised records generated by the bank's computers, the Malaysian Court of Appeal held that section 90A provides that computer-generated record made in the ordinary course of its business is admissible if the following are proven: a) the documents were produced by a computer, and b) the computer records are produced in the course of its ordinary use. Such proof can be made either by way of a certificate signed by someone solely in charge of the computer that produces the printout as required by section 90A(2), or by an officer of the bank. The present case would seem to suggest that it is no longer necessary to call the person who keys in the data or information into the computers to be present in court as a witness, provided he does so in the course of ordinary course use of the computer.

Section 90B provides some guidelines to assess the weight or probative force of computer-generated evidence. It provides only some of the matters such as the manner and purpose of creation or accuracy and the list is not exhaustive. It also provides that the courts have to consider the time lapse between the occurrence of the fact and the supply of information into the computer. Regard must also be had as to whether the supplier of information or the person possessing the computer evidence had any incentive to conceal or misrepresent the facts in the document. This is to ensure reliability of the data or the programs used to process the data. By section 90C, any provision in the Evidence Act or any written law inconsistent with it (only actual documents as opposed to computer-generated ones are admissible) would be deemed to be inapplicable. Hence, this would obliterate the need to comply with any law requiring actual documents to be produced in evidence as opposed to the computer-generated one.

Search, Seizure and Hindrance to Investigation

The 1997 Act provides for wide powers of arrest, entry, search and seizure, which may be a cause for concern among MSC investors. Section 10(1) enables a magistrate to issue search warrants where there are reasonable grounds for believing that the offences under the Act has been committed, to permit entry to premises, by force if necessary, to search, seize and detain any evidence found therein.[129] However, the search of premises can be conducted without a warrant if the police have reasonable cause to believe that the evidence of the offence is in the premises and that there are reasonable grounds to believe that delay in obtaining the warrant would frustrate the purpose of the search.[130] Section 10(3) provides that the offences under the 1997 Act

129 *In re Kah Wai Video (Ipoh) Sdn Bhd* [1987] 2 MLJ 459.
130 1997 Act, section 10(2).

are seizable (or arrestable) offences and thereby attract the police powers of arrest without warrant.

The law enforcers have a power to make lawful demands in the execution of their duty[131] and failure to comply will attract a maximum jail sentence of three years and/or a maximum fine of RM 25,000.[132] The 1997 Act provides a safeguard for potential defendants in that a prosecution under the Act can only be instituted with the written consent of the Public Prosecutor.[133] Although failure to comply with section 11 applies to the accused, inevitably it covers victims as well since the evidence of a computer crime can often be found on the victim's computer. In view of the fact that failure to report a computer crime could hinder or delay police investigation of computer crime, section 11 could mean that victims are mandated or obliged to report such crimes.[134] If this is the case, then this provision lacks clarity and runs the risk of being misapplied. There is an apparent conflict between sections 10 and 11 and the government's objective of providing reassurance to MSC investors of their business and technology protection. It is an accepted fact that corporate victims are not willing to report to the police of intrusions into their computer networks.[135] Many reasons can be attributed to the lack of reporting. Suffice to say that they may be unaware of the breach,[136] or that they may be concerned that seizure of documents and computers will disrupt normal business operations,[137] or commercial embarrassment[138] and fear of adverse publicity.[139]

Duty to Report

Under the UK law there is no general duty to report cases of misuse to the police. The obligations to report have been considered by both the Scottish Law Commission and English Law Commission but were rejected.[140] As there is no duty to report any crime in the UK, creating such a duty in respect of computer crime would be anomalous. However, since 1994 there is such a duty under the Drug Trafficking Act, requiring those working in the financial sector to report knowledge or suspicion on money laundering.[141] The UN Manual on the Prevention and Control of Computer-related Crime has recommended victims' co-operation in reporting but stops short of recommending an obligation to report. However, the Convention on Cyber Crimes has recommended a duty to report for purposes of investigation into cyber crimes.[142]

131 1997 Act, section 11(1)(b).
132 1997 Act, section 11(2).
133 1997 Act, section 12.
134 DL Beatty, n 10 at 368.
135 DS Wall (ed) *Crime and the Internet* (Routledge London 2001) at 169.
136 Ibid at 169.
137 Department of Trade, *Dealing With Computer Misuse: Review of the Application of the Computer Misuse Act and the Associated Market for Information and Expert Advise* (DTI, London, 1992) para 240.
138 PN Grabosky and RG Smith, *Crime in the Digital Age* (Transaction Publisher-Federation Press Annandale Australia 1998) 215.
139 Ibid at 215.
140 Scottish Law Commission (1987) paras 5.8-5.11. See also Law Commission, Report No 186 (1989b) para 4.14.
141 See section 52 of the Drug Trafficking Act 1994.
142 See Article 19 of the Convention on Cybercrime 2002.

Despite the benefits that may accrue to law enforcement by an obligation to report computer crimes, it is an unrealistic expectation that corporate victims would readily comply to such law. Section 11 is suffused with lack of clarity and precision. This does not augur well towards promoting Malaysia's leadership in the growth of cyber laws as well as its ability to instill investor confidence. However, in view of the foreign investment-related goals of the government, it is rather unlikely that failure to report a computer crime is intended to be a violation of the section. It remains open for the courts to decide.

The Critique of the Act

The Computer Crimes Act 1997 can be improved at two levels. On the one hand, at the instrumental level existing provisions can be clarified by changing the statutory language, which can have far-reaching effects. Four provisions have been identified for these purposes, which are sections 5, 6, 9 and 11. On the other hand, at the normative level, new modern approaches to governing computer crime can supplement the traditional approach.

As section 5 is primarily concerned with modification as opposed to hindrance or obstruction to a computer system, there appears to be a lacuna in the law. Hence, in this respect the 1990 Act provides a broader and better protection than the Malaysian law. The loophole in the Malaysian law could be plugged by following the approach adopted by the UK and the Singapore positions. Such measure can include amending the 1997 Act to include a new offence of unauthorised obstruction of use of computer. The proposed section (which could be in the form of section 5A) should provide that:

(1) Whoever knowingly interferes with, or interrupts or obstructs the lawful use of, a computer or impedes, hinders or prevents access to any program or data or impairs the usefulness or effectiveness of, any program or data held in any computer commits an offence under this section.

(2) Whoever commits an offence under this section shall be punished with imprisonment for a term which may extend to seven years, or with fine not exceeding one hundred thousand ringgit.

Where wrongful communication of access codes is concerned, the government has two options, either to make section 6 a strict liability offence or alternatively, to create the defence of lack of *mens rea* into the offence. This would obviate the need for the prosecution to prove intent without creating a strict liability offence. The proposed statutory provisions are as follows:

(1) Whoever intentionally communicates, directly or indirectly, a number, code, password or other means of access to a computer to any person who he knows, or has reason to believe is not duly authorised to receive such information commits an offence under this section. OR

(1) Whoever communicates directly or indirectly a number, code, password or other means of access to a computer to any person other than a person to whom he is duly authorised to communicate commits an offence under this section, unless he can establish that he had no intention to communicate that information to an unauthorised person.

Asserting jurisdiction over individuals who have committed an offence that has a nexus with Malaysia can narrow the broad provision of jurisdiction in section 9. This could be an offence which affects a computer in Malaysia, but committed by a person who is located in Malaysia at the time, or by using a computer located in Malaysia regardless of the location of the computer(s) ultimately targeted, or the location from which the offence is initiated.[143] The proposed section 9 is as below:

(1) It is immaterial for the purposes of any offence under this Act if any act or other event, which is an element of the offence, occurred in Malaysia, provided there was a link with Malaysia in the circumstances of the act or event.

In relation to hindering police investigation in section 11, there are two possible options. On the one hand, if the section was intended to create a duty to report suspected cases of misuse this should be explicitly provided. On the other hand, if no such duty is intended, a new offence in section 11 should be created as follows:

(1) Any person who, knowingly fails to report his reasonable suspicion that an offence under the Act has been commited, commits an offence under this section. OR

(2) No person shall be required under the Act to provide any information in respect of any crime.

If Malaysia is serious about being a leader in the development of cyber laws there is a need to update the approaches to the 1997 Act, which were based on the law created before the widespread use of the Internet. Otherwise, despite the availability of other modalities of constraints such as the technology and management best practices Malaysia would be stuck to the legal solution that was only appropriate in that era. Several strategies can be undertaken such as by expanding the scope of the provisions to include a broader category of offenders, adopting a creative way of sentencing the offenders and creating a compliance model for information security.

An apparent limitation of the 1997 Act, that is similar to the 1990 Act, is that it does not provide for the prosecution of the growing number of "professional" virus writers who spread rogue codes in books and through computer bulletin boards, or who disseminate malicious materials, usually for profit. There are readily available software programs for hacking tactics like "war dialing", "sniffing" and "fingering",

143 DL Beatty, n 10 at 371.

all of which are used to exploit security weaknesses in computer systems. The publication and dissemination of these codes have, in a way, made the tasks of law enforcer more formidable. One could speculate that this unacceptable conduct would be within the ambit of the inchoate offence of abetment (by instigation)[144] to commit an offence contrary to section 7(1) of the 1997 Act that provides for abetting crimes within the ambit of the 1997 Act. The case of *R v Pile* could be of some guidance to the Malaysian courts in dealing with cases involving incitement to spread computer viruses or other malicious programs. As such, Section 7 should be reviewed to include criminalization of those supplying cracking software, malevolent codes and the like. Prosecution of those who disseminate or knowingly allowed such codes and information to be disseminated that can be used in the commission of computer crimes may go toward reducing their availability.

Despite the critics of the harsh punishment imposed by the 1997 Act, these punishments have an educative utility.[145] However, there are other options other than imprisonment and fines that can be more meaningful towards curbing computer crimes. One such penalty is the confiscation of the technology used in the commission of the crime, which had been adopted by the California Penal Code.[146] The deprivation of computers from this type of offenders who may be overly dependent on computers may be more effective than incapacitation penalty strategy. Confiscation of computers can be coupled with the proscription of the defendant's employment and activities involving computers. Although these penalties may seem punitive and retributive, they may arguably be useful in breaking the addictive pattern that hackers may have developed.[147]

Malaysia should also consider establishing an information security compliance model either through legislative measures or as a condition of granting participation in the MSC. Such security is important given the nature of many intrusions that are attacking multiple systems and the potentially vast amount of information and data kept by companies located in the MSC. Many Malaysian organizations are still lagging in establishing adequate information security, leaving them to be exposed to internal and external misuse. For instance, the Malaysian National Information and Communications Technology Security Emergency Response Centre (NISER) Security Survey 2000/2001 revealed that 68 percent of 205 private and public organizations had experienced security breaches in 2000.[148] Whilst 47 percent experienced virus attack, 33 per cent suffered from employee misuse in the forms of Internet and e-mail misuse, downloading pornography and pirated software.[149] Yet, only 27 per

144 There is no offence of incitement under the Malaysian Penal Code. However a similar offence of abetment by instigation is provided for in section 107(a) Penal Code. What is abetment by instigation is not defined in the Code. However, in *Hj. Abdul Ghani b. Ishak v PP* [1981] 2 MLJ 230, Raja Azlan Shah CJ stated that the element of active suggestion, support, encouragement or stimulation on the part of the abettor in the instigation is essential.

145 Zulkifli Othman, "Pikom: Cyber Laws Will Provide Clarity" *Business Times*, 28 March 1997, 2 available in LEXIS, World Library, Txtine File.

146 California Penal Code 502.01.

147 *R v Bedworth, The Times*, 18 March 1993.

148 NISER, *Security Survey for Malaysia*, Kuala Lumpur, 2001 available at http://www.niser.org.my.

149 Ibid.

cent of 108 respondents who experienced security breaches reported to the police or other third party. 59 per cent attributed their security measures to anti-virus software and firewalls and the level of management involvement in tackling security breaches was relatively low.[150] Such lack of concern by management for information security is one of the reasons prompting the UN to call on senior executives and management to commit their organizations to security and crime prevention.[151] Some measures towards emphasis on information security are already underway with the creation of NISER in early 1998, which is expected by the government to play a vital role in promoting good security practices, advising organizations on security issues and creating the National IT security policy.[152] Despite the creation of the 1997 Act to deal with computer misuse, the government has encouraged organizations not only to co-operate with the police in investigations of computer misuse but also to formulate and enforce information security policy and measures. [153]

Conclusion

In the provision of substantive offence, the Computer Crimes Act of 1997 is wider in scope than the UK legislation. The additional offence of wrongful communication of password etc. in the former statute can be viewed as a "preventive measure by imposing a duty of secrecy of those entrusted with important responsibilities".[154] However, the 1997 Act does not go as far as adopting the Singapore legislation on providing for unauthorised use or interception of computer services[155] or providing for the concept of a "protected computer".[156] The incorporation of the UK perspective into the 1997 Act no longer suffices to meet the current demand as the penalty imposed would appear to be related to the type of offence and the severity of that offence, rather than to the degree of damage caused by unauthorised access or modification as evidenced in the Singapore statute. This suggests that not only the English approach of sentencing, but also the justification for the criminalization of unauthorised access, are being adopted in Malaysia without modifications, thus bringing whatever problems that occur in the UK to Malaysia. Since the 1990 Act, on which the 1997 Act was modeled, was created before the Internet development, it may not be effective in dealing with new Internet-related activities such as denial of service.

Broader analysis reveals such protection afforded to computer owners against all forms of unauthorised access and modification, without exception or having regard to the level of damage caused, could be seen as conferring some kind of ethereal status upon the data or information held within[157] as well as extending the criminal law itself. In

---

150 Ibid.
151 UN Manual, n 35, para 294.
152 See http://www.niser.my
153 Speech by YAB Dato Seri Abdullah Ahmad Badawi, Deputy Prime Minister for the launch of the National ICT Security and Emergency Response Centre (NISER), 10 April 2001.
154 N Annamalai, n 9 at 6.
155 CMAA, section 6A.
156 CMAA, section 6C(2).
157 I Lloyd and M Simpson, *The Law on the Electronic Frontier* (Edinburgh University Press Edinburgh 1998) at 59.

one sense, the 1997 Act is worse than the 1990 Act, because with the definition of computers provided therein, the 1997 Act would seem to criminalise the conduct performed on a computer that will not be criminal if performed with a hard copy. However, despite this flaw, when compared to the 1990 Act, the 1997 Act would seem to be a better piece of legislation, as it provides for access in excess of authority, which consequently can give a clearer guidance on the level of authority, which is a pertinent issue in a workplace situation.

In the broader context of achieving the government's objectives and in fulfilling the national ideology of Vision 2020, the 1997 Act requires some fine-tuning to add more clarity and certainty to it. While some provisions are progressive and in line with international requirements, others are ambiguous, wide and inconsistent with the needs of the corporate victims of computer misuse who generally are not willing to report cases of misuse. The forfeiture of computers, the proscription of defendant's activities and employment involving computers and the criminalisation of virus writers and distributors are some of the modern strategies that can be adopted by Malaysia to complement the 1997 Act. In this way the 1997 Act would be able to promote Malaysia as a leader in cyber law development as well as reassuring the MSC investors that the government has their interests in mind.