Malayan Law Journal Articles/2012/Volume 6/Investigating Cybercrimes Under The Malaysian Cyberlaws and The Criminal Procedure:Issues and Challenges

[2012] 6 MLJ i

Malayan Law Journal Articles

2012

INVESTIGATING CYBERCRIMES UNDER THE MALAYSIAN CYBERLAWS AND THE CRIMINAL PROCEDURE CODE: ISSUES AND CHALLENGES

*Dr **Duryana** Mohamed*

Legal Practice Department

Ahmad Ibrahim Kuliyyah of Laws, International Islamic University Malaysia

Investigating cybercrimes requires full commitment and readiness to fight the criminals. This means the investigating officer or any authorised person must not only have good knowledge and skills to detect the suspect and investigate cases of cybercrimes but he must also be ready to face the consequences. In this regard, having good procedural laws and adequate statutory provisions are very important to face the challenges ahead. To ensure the smooth running of investigation process, it is very important that the rules of procedures and certain standards of practice are complied with. This paper will discuss the process of investigating cybercrimes under the Malaysian cyberlaws and the Criminal Procedure Code ('CPC') with the aim to identify any inadequacies and challenges faced by the investigators. The main reference would be the Computer Crimes Act 1997, the Communications and Multimedia Act 1998 and the Criminal Procedure Code. Other laws will also be referred to as background information.

INTRODUCTION

Basically, investigating cybercrimes is not an easy task. It requires not only knowledge and understanding about the law but also the skills of investigation as well as commitment to fight the criminals.[1] Thus, by having good

procedural laws and adequate statutory provisions, one can ensure that he or she is ready to face the challenges ahead. In this regard, the then CID Director, Tan Sri Musa Hassan in April 2004 admitted that there was a need to have adequate information technology legislation to combat Internet crime syndicates and to arrest the criminals. This implies that despite the existence of cyber laws, Internet crime is still difficult to combat, and as such, adequate laws are needed to arrest the criminals. Hence, in order to further understand the investigation process of cybercrimes in Malaysia, this paper will briefly discuss the process of investigating cybercrimes under the Malaysian cyberlaws and the Criminal Procedure Code (CPC) as well as identifying any inadequacy and challenges faced by the investigators.

CYBERCRIMES

Cybercrimes are sometimes known as computer crimes or high-tech crimes. They are committed by an individual whose intention is to either destroy other's property, personal integrity or life or to steal other people's valuable property and information. Some of the crimes include spreading computer viruses,

committing denial of service attacks ('DOS'), sending pornographic materials, committing unauthorised access or hacking, committing unauthorised modification of computer data, mass web defacement, committing phishing[2] or identity theft,[3] cyber squatting,[4] cyber stalking,[5] and many others. These crimes will not stop and will grow with the development of technology. This can be seen in 2003 when a total loss of RM579m resulted from commercial crime alone, indicating that the law on cybercrime must be

6 MLJ i at iii

tightened. While in 2011, the Norton study revealed that there were 431 million cybercrime victims worldwide in the past year with financial losses and time lost amounting to US$388 billion (RM1.1 trillion), just slightly below the US$411 billion (RM1.2 trillion) generated annually by the global illicit drug trade.[6] Malaysia on the other hand, recorded RM2.75 billion losses due to cybercrimes over a period of five years (from 2005-2010), with the financial sector having the worst hit.[7] These show that there must be something lacking either in the investigation, prosecution or the laws. Thus, it is very important to have an efficient process of investigating, detecting and gathering of criminal evidence to achieve a successful prosecution.

Cybercrimes are basically governed by the Computer Crimes Act 1997 ('CCA') (especially hacking), the Communications and Multimedia Act 1998 ('CMA') and the Penal Code. Other statutes such as Defamation Act however, are also referred to when necessary. Nevertheless, there are still loopholes in the above laws, which resulted with comments as well as criticisms by researchers, legal practitioners, law enforcers as well as the public. The CCA for instance, was criticised as being vague and limited to cases of unauthorised access offence, unauthorised access with intent to modify data and wrongful communication.[8] In fact, the CCA was also reviewed and discussed on April 2012 with the aim to cater for the challenging environment.[9] During the discussion, the researcher proposed that the CCA needs to include new provisions on unauthorised obstruction of use of computer and unauthorised use or interception of computer service. Suggestions were also made to improve the power of investigation under the CCA.

THE INVESTIGATION PROCESS AND THE PROCEDURAL LAWS

Basically, criminal cases are investigated under the Criminal Procedure Code ('CPC') of Malaysia. This Code is derived from the English criminal procedure and practice through the adoption of the Indian Criminal Procedure Code 1873. The Indian Code has been applied in the Malaysian criminal courts until

6 MLJ i at iv

1976. The Code was then amended several times. However, the amendment did not take into consideration the technological development except on the manner of recording evidence from a child witness.[10]

The investigation procedure under the CPC

Basically, the Police Act 1967 gives power to the police to investigate criminal cases, including executing summonses and warrants, conducting prosecutions, exhibiting information and attending the court. The CPC on the other hand, outlines the duties and obligations of the police officer to investigate criminal cases. The Code also provides a guideline for proper investigation and it starts when the officer in charge receives a report from the complainant. Chapter XIII deals with information given to the police and their powers to investigate. Further, the Code also provides specific powers to the court to issue a search warrant, authorising a search prior to the seizure process. However, there is no specific provision in the CPC on investigating cases of cybercrimes. Other than the CPC, the power to investigate cybercrime cases is also provided in the CCA and the CMA. This can be seen from certain provisions in those Acts that will be discussed later.

The investigation procedure under the CCA and the CMA

As mentioned above, the process of investigation for criminal cases are laid down in the CPC. However, for cybercrimes such as unauthorised access (hacking), unauthorised access with intent to modify the data and wrongful communication, the investigation can be done under both the CPC and the CCA 1997. For CMA 1998 however, cases under ss 232, 233, 234, 235 and 236 of the Act are investigated by an authorised officer from the Commissions (s 245: authorised officer). The police investigator, on the other hand, will investigate cases that fall under the scope of the CCA, the Specific Relief Act 1950 ('SRA'), the Penal Code ('PC') and the Defamation Act 1957 ('DA'). Among the relevant sections in the Penal Code ('PC') are s 292 of

the PC (Sale etc of obscene books etc) and s 500 of the PC (punishment for defamation).[11]

The procedure of investigation in the CCA 1997 is mentioned in s 10 (power to search, seizure and arrest) and s 11 (obstruction of search) while in

6 MLJ i at v

the CMA 1998 there are more provisions and more detailed procedures. Chapter 3 of the CMA lists down the power of the authorised officer to investigate cases under the CMA (s 246). The authorised officer here may include any public servant such as a magistrate and a police officer. Furthermore, the commission may also give reward to any police officer or other public officer or other person for services rendered in connection with the detection of any offence under this Act or its subsidiary legislation, or in relation to any forfeiture proceeding, or any seizure made, under this Act (sÂ 262).

Apart from that, there are other cyberlaws that provide power for the authorised officer to investigate. This include s 75 (authorised officer) to s 82 (additional powers of an authorised officer) of the Digital Signature Act 1997 ('DSA') and ss 110 (Authorised officer) to s 127 (power of arrest) of the Personal Data Protection Act 2010 ('PDPA'). However, detailed information relating to detection and investigation of the above crimes can only be obtained from the officer in charge at the Royal Malaysian Police ('RMP'), or the Cybersecurity.[12]

It is nevertheless observed that in practice, despite the similarities between the CPC and the cyberlaws in the search and seizure process, the investigating officer ('IO') relies greatly on the CPC due to its comprehensiveness. For instance, the requirement of recording the investigation and gathering process in the investigation diary under s 119 of the CPC must be thoroughly observed and strictly conducted using the prescribed forms and procedures. However, this requirement or provision is not provided in the CCA 1997 or any cyberlaws, although this requirement is necessary to ensure that the delicate process of the recovery of computer evidence is free from tampering or being destroyed and is collected in a proper manner by the IO or authorised persons.

However, it is of the opinion that there is something lacking in the CPC particularly on the right of access by the police. This power or right to access a computer is very crucial because the definition of 'access' is clearly provided for by s 24(2) of the CMA 1998 and s 2(2) and (5) of the CCA 1997. This right, however is not mentioned and emphasised in the CPC. Only the right to intercept communications is available under s 106C of the CPC.

6 MLJ i at vi

Besides the laws and procedures mentioned above, the IO is also required to follow the 'Manual on Computer Crime Investigation and Internet Banking Fraud'(or 'Manual Siasatan Jenayah Komputer dan Internet Banking Fraud') when investigating cybercrime cases. The manual, which was adopted in 2000, took into consideration development in information and communication technology ('ICT') and the content is in accordance with the legal requirements prescribed by the Evidence Act 1950. However, details of the investigation methods are not made available to the public for security reasons.[13] What is available is only brief information on how the police conduct the investigation.[14] It is suggested that a manual for search and seizure of computer evidence in either the CPC or the CCA 1997 is needed since the manual will enable defence counsel and criminal judges to examine and detect any break in the chain of evidence or any improper conduct of the investigating officer. This will also enhance the administration of the criminal justice system in Malaysia.

THE INVESTIGATION AND ITS PROCEDURAL STEPS

Usually, once the police receive report of cybercrime, the IO will first visit the place of the incident to gather information from the computer system and make a back-up copy of any temporary files.[15] The IO will record all findings and make a summary of the crime (or *'ringkasan jenayah harian'*). The statement of the complainant, the witness[16] and the suspect, if any, will be recorded as required by s 112 of the CPC.[17] Any information obtained from, or provided by the Internet Service Provider ('ISP') or the Telephone Service Provider ('TSP') will be analysed to trace the suspect.

The ISP will provide further information about the suspect's computer and the details about the message by sending the details about their customer's

6 MLJ i at vii

Internet activity for investigation by the police. Then, the police will analyse e-mail messages in order to trace the originating IP address, date and time the e-mail was sent and received and who is the receiver of the message. Logging and tracking of messages through a company and between companies or individuals may also be used to obtain information from the full header of the e-mail message.[18] In short, the system provides a complete audit trail of who is sending what and to whom. This is like a road map to finding incriminating statements or tracing a decision-making process to determine accountability.[19]

In a situation where false allegation is sent by an anonymous blogger to other bloggers, the case will be investigated by the police under the Communications and Multimedia Act (CMA) 1998. However, the authenticity of the message will first be ascertained before further action is taken by the RMP.

What to observe during the investigation process?

During the investigation process, the police investigator is under a duty to respect the personal liberty of the suspect. The issues are whether there is an abuse of power by the police and if yes, whether such abuse constitutes a deprivation of the suspect's personal liberty. These issues were raised in *Kwan Hung Cheong v Inspektor Yusof Haji Othman & Ors*.[20] In this case, the accused was charged under s 454 of the Penal Code (a non-bailable offence). The section provides that whoever commits lurking house-trespass or house breaking in order to commit any offence punishable with imprisonment, shall be punished with three years imprisonment and shall also be liable to a fine. If he intends to commit theft, the imprisonment would be ten years and shall also be liable to fine or whipping. Section 388 of the CPC provides that the accused that was detained or arrested without warrant by a police officer of an unbailable offence may be released and s 390 of the Criminal Procedure Code provides the amount of bond which is fixed based on the circumstances of the case. The police used police bail bond against the suspect. The plaintiff/suspect contended that the first to fifth defendants' use of the police bail bond against him was an abuse of power, rendering their actions unlawful, illegal and a breach of his constitutionally-guaranteed liberty. He applied to the High Court

6 MLJ i at viii

to dispose of matters under O 14A of the Rules of High Court 1980.[21] It was held that:

> It is clear that personal liberty is liberty relating to the person or the body of the individual and the negative right of not being subjected to any form of restraint or coercion. It was, therefore, the considered opinion of this court that the unlawful police bail issued by the 1st defendant against the plaintiff had subjected him to a form of restraint or coercion resulting in the deprivation of personal liberty in breach of art 5(1) of the Federal Constitution. On the issue of remedy, the maxim of ubi jus ibi remedium, namely, wherever there is a right there must be a remedy came to mind. As the right to personal liberty is such a constitutional right, a breach of that right must give rise to a suitable remedy or relief to enforce such constitutional right. Therefore, the answer to the third question was in the affirmative.

In this case, the court had allowed the plaintiff's application.

Besides that, the investigator must also ensure that there is no break in the chain of evidence collected. Although it is not necessary to call evidence to ensure that there is no break in the chain of evidence, it is important to produce reliable evidence since the effect would be on the prosecution later on to establish his case during the prosecution stage. This issue was highlighted in the Supreme Court case of *Teoh Hoe Chye v Public Prosecutor* and *Yeap Teong Tean v Public Prosecutor*[22] where it was held that 'the law is clear that it is unnecessary to call evidence to ensure that there is no break in the chain of evidence but where a doubt arises as to the identity of an exhibit, a failure to adduce evidence to provide the necessary link in the chain of evidence would be fatal to the prosecution case'.

COMPUTER FORENSIC INVESTIGATION

Computer forensic investigation is one of the methods used to identify cyber criminals and to solve complex cybercrime cases. It is adopted by the computer forensic expert who uses specific digital forensic tools to examine data from storage media.[23] In Malaysia, the computer forensic investigation team is available not

only at the Computer Forensic Laboratory in Cheras, Selangor but also at the Cybersecurity Office and the Military Office.[24] The computer

6 MLJ i at ix

forensic expert in Malaysia works based on several guidelines including the:

(a) United Nations Manual on Computer Forensic Examination;[25]
(b) IOCE Guidelines for Best Practice in the Forensic Examination of Digital Technology;[26]
(c) NTI Computer Incident Response Guidelines;[27] and
(d) FBI forensic investigations manual.[28]

As mentioned earlier, the CPC provides more detailed aspects of investigation as compared to the CCA 1997 and the CMA. However, none of the laws provide specific provision on forensic investigation. Therefore, the forensic department of RMP investigates computer crime by referring to a 'Manual Prosedur Kerja' or Standard of Practice ('SOP') prepared by the Computer Crime Section of the Police Forensic Laboratory, Malaysia. The forensic team had managed to crack down on several criminal cases using digital forensics. Among the cases are fraud by computer manipulation, damage to or modification of computer data or programs, unauthorised access to computer and programs of application, unauthorised reproduction of computer programs, financial crimes such as identity theft, fraud, forgery and theft of funds committed by electronic means and counterfeiting, or the use of computers or laser printers to print cheques, negotiable securities or store coupons.

Further, the application of digital forensics in Malaysia is comparable with the advanced countries. Nevertheless, issues such as high cost and legal aspects that are not evolving as fast as technology need to be looked into.[29] Thus, in order to achieve successful forensic investigation, the government has in the 2012 budget allocated RM200m for forensic investigation. The money would

6 MLJ i at x

be used to upgrade and buy the latest technology in forensic equipment. [30]

THE PROBLEMS AND CHALLENGES OF THE INVESTIGATOR

The problems and challenges of the investigator are not only faced by the Malaysian police but also by enforcement officers in other countries. Investigating cybercrimes cases becomes complicated due to its borderless nature. This fact was admitted by Toni Makkai when he stated that:

> Conducting investigations across national borders raises many practical problems. These include investigators having to contact people on the other side of the globe, documents having to be translated and witnesses from non-English speaking countries needing the assistance of interpreters. All of these impediments can be overcome by harmonising laws and procedures globally, and improving the technical capabilities of investigators. [31]

This is actually a worldwide issue. Therefore, it is best to resolve it through global harmonisation of laws and procedures and by improving the technical capabilities of investigators. As far as Malaysia is concerned, the then Deputy Inspector General of Police, Datuk Seri Mohd Bakri Omar, clearly stated that the Force needed more officers proficient in computer forensics to better investigate and analyse computer related crime. [32] This is to ensure that the Force will always be prepared to fight the increasing number of Internet crimes.[33]

Thus, in order to further strengthen the law enforcement unit, the Inspector General of Police ('IGP') Tan Sri Ismail Omar has assured that the police from cybercrime unit will be equipped with the latest high-tech gadgets to effectively combat online offences. They will also come up with a new mechanism and procedures to deal with cases involving the Internet, especially on Facebook.[34]

To the police investigators, the main problem with the investigation of computer crime is the difficulty of identifying a suspect due to the anonymity of the identity of the person. The crime may be committed by anyone from a remote webpage or WIFI, or by someone who uses someone else's computer to distribute pornographic materials.[35]

Conducting an investigation based on PIN ('personal identification number') or password belonging to a

certain individual also poses problems. It is because the password or PIN Number could be stolen and used by an unauthorised individual to commit an unlawful or unauthorised access, thus, creating difficulty for the police to investigate, to identify the real offender and prove the cybercrime cases. On this matter, the Australian Transaction Reports and Analysis Centre ('AUSTRAC') suggested some possible scenarios which may be established by the prosecutor with the help of the investigator to prove e-crime. These include:

(a) seizing the suspect's computer, download the contents and find the incriminating data;
(b) use information contained in the victim's data to show that he has been defrauded; or
(c) indicate to him that there has been unauthorised access to the victim's computer.[36]

The other challenge faced by the police is monitoring websites on the Internet. This is made difficult by the policy of the Malaysian Government not to censor the Internet. However, in the cases of rumour-mongering posted on websites,

6 MLJ i at xii

the then Ministry of Science, Technology and Innovation had made a promise to assist in investigating malicious e-mail cases involving prominent personalities.[37] In this sense, the government needs to reconcile between freedom from censorship and the need to mitigate the effects of rumour-mongering in cyberspace.[38]

Other than that, privacy issue has also become one of the challenges because an individual or a company may object to the investigation process in order to avoid or delay the investigations. Nevertheless, by virtue of s 249 of the CMA 1998,[39] investigators are allowed to access the computerised data thus protecting them from any claim of illegal unauthorised access. The common contention made by defence counsel are on the credibility of the log files of the police personal computers, post-event editing and tampering of evidence and on the lack of transparency on the methods of investigation.

As highlighted earlier, investigating cross border crime is very challenging since different countries have different laws. The significant impediments faced by investigators include:[40]

(a) choosing an appropriate jurisdiction to charge the offender,
(b) remote access to computer via the internet may be exposed to illegal interception of communications;
(c) the need to execute simultaneous warrants on offenders in different countries,
(d) retention of seized materials;
(e) accessing encrypted data, which in some countries can only be accessed by installing key logging program onto a computer to detect the password used for decryption;

6 MLJ i at xiii

(f) high costs for mutual assistance treaties, logistical and practical barriers;
(g) difficulty to contact and deal with the right people in other jurisdictions;
(h) documents may not be written in English;
(i) witness may not speak English; and
(j) lack of expertise and proficiency in dealing with and handling digital evidence.[41]

In such situations, the investigators are sometimes required to deal with issues like extra-territorial offences[42] and extradition. Hence, it is very important for the investigator to be able to identify, preserve and process computer related evidence effectively and possess tremendous skills as well as proficiency in dealing with cross border crime. Good investigation will result in successful prosecution. Thus, there must be good cooperation between the investigators and the prosecutors since the defence counsel will challenge the latter if the prosecutor cannot provide sufficient evidence in his case.[43]

PROBLEMS AND CHALLENGES IN COMPUTER FORENSIC INVESTIGATION

One of the essential elements of the computer forensic expert is that he or she must be able to provide information that is readily accessible to the judges, non-experts or can be understood by the public. Thus, besides being able to get the most out of the system, he must also have skills to present the evidence in a complete and concise manner in the court of law.[44] The role of a forensic expert is to focus on explaining to

the judge and the relevant parties about the

6 MLJ i at xiv

procedures and methods used to retrieve evidence from the computer.[45]

However, the most difficult challenge faced by the computer forensic expert is coping with the fast changing rate of technology. For example, computer hardware, operating systems and application programs can change dramatically over a period of five years. This will require the expert to dig out as much evidence as possible before new technology could be used by the criminal to erase or destroy the previous evidence. The dilemma faced by the forensic expert will be whether to hold back the examination using a new investigation technique until it has been properly tested or to offer to the court untested tools and run the risk that innocent people may be convicted.[46]

Development in software and computer forensic tools also causes problem to computer forensic experts, as it needs upgrading. This upgrading of software and the process of recovery of computer data normally incurs high cost. Using third party computer data recovery services may also require great expense.[47] In addition, the lack of properly trained computer forensic experts presents a major problem to Malaysia and some other countries, including the UK. In 2002, it was reported that in the UK, only 1000 out of 140,000 police officers are trained to handle digital evidence. Less than 250 personnel have high level

6 MLJ i at xv

computer forensic skills.[48] To close the gap, training of more police experts is very much needed.[49]

According to Sean Lim, Vice President of the EC-Council, digital forensics is a specialised science within the information security domain and there is a very low awareness of security in Malaysia. He further added that, the low awareness has resulted in fewer forensics professionals.[50] The computer forensic expert is normally called to give evidence as expert witness. They may also be cross-examined by the defence counsel particularly on the accuracy and reliability of the data and any report produced. Thus, the integrity and credibility of a computer forensic expert may be questioned. Knowledge in IT and related law is equally important to identify any weakness in the prosecution case and to challenge any techniques used or relied upon by the expert or police in conducting electronic investigation.[51]

CONCLUSION

Cyber criminals are always advancing in mastering the skills to commit cybercrimes and abusethe ICT. Thus, the law and procedures are supposed to be adequate and effective to curb their activities. Although the process of investigating cybercrime cases is challenging, this does not mean that there is no prosecution of cybercriminals. What the investigators should do is to equip themselves with computing skills and knowledge as well as familiarise themselves with the relevant laws and procedures. This is because any negligence on the part of the investigator will result with failure in the

6 MLJ i at xvi

prosecution. For the prosecutors, they must make sure that the evidence gathered by the IO is relevant and admissible in court and that the chain of evidence must not be broken. Furthermore, the police officers and other relevant authorities must always update their skills and knowledge because 'society's best defence is the ability of law enforcement to be fully cognisant of and fully use the vast electronic trails evidencing criminal activity so that technology-using criminals can be brought to justice. Unless the procedures and the law are clear and enforceable, finding ways to track down, arrest and prosecute the criminals will be forever challenged. For this reason, the procedural aspects of gathering evidence in computer crime cases must be emphasised and if needed, be reviewed. From the above discussion, it is concluded that the cyberlaws, namely the CCA 1997 is still lacking in addressing issues on crimes and investigation aspects while the CMA 1998 is quite sufficient. Nevertheless, the CPC is still relevant even though it is originally meant for conventional crimes. Finally, in order to achieve a successful investigation process, a continuous effort by the Malaysian Communication and Multimedia Commission (MCMC), Cybersecurity, the RMP and others is very important in order to ensure that Malaysia is a safe country for all.

1 See V P Sujata, 'Legislation Needed to combat Internet crime syndicate', *New Straits Times Online*, 9 April, 2004 at http://www.ctimes.com.my/and also 'Guidelines to tackle cyber crime', *The StarOnline,* 9 April 2004.

2 Phishing is an identity theft crime committed over cyberspace. This act will usually involves online or Internet banking whereby fraudsters will send dubious e-mails or create spoof websites hoping to entice users to hand over their credit card or banking details. See 'Cybercrimes cost billions in losses', *New Straits Times (Computimes) Online*, 1 March, 2004. at http://www.ctimes.com.my/and Abu Bakar Munir and Siti Hajar Mohd Yasin, 'Would the phishers get hooked?'. Paper presented at 22nd BILETA Conference, 16-17Â April 2007, Hertfordshire athttp://www.bileta.ac.uk/Document%20Library/1/Would%20the%20Phishers%20get%20Hooked.pdf

3 See Nehaluddin Ahmad, *Truth about identity fraud: Defence and safeguards*, [2009] 9 CLJ i.

4 Cybersquatting is also known as cyberpiracy. It is a derogatory term used to describe the practice of registering and claiming rights over internet domain names which are, arguably, not for the taking. The cybersquatter then offers the domain to the rightful owner at an inflated price, an act which some deem to be extortion. See Cybersquatting, http://en.wikipedia.org/wiki/Cybersquatting. In the United States of America ('US'), this crime is dealt under the Anticybersquatting Consumer Protection Act ('ACPA') of 1999.

5 Cyberstalking is when an individual or a group uses the Internet or other electronic means to stalk someone by harassing. The number of cyberstalking cases reported last year was 174 compared to 72 in 2010. See Subashini Selvaratnam, 'Cyberstalking a serious threat', *TheÂ Star*, 2 February 2010.

6 See 'Malaysians not doing enough to tackle cyber crimes', *New Straits Times*, 21 September 2011 at http://www.nst.com.my/nst/articles/22cyber/Article/#ixzz1YXnhX5Ia

7 See 'Best policies crucial to prevent cybercrimes', 8 April 2012 http://thestar.com.my/news/story.asp?file=/2012/4/8/nation/11027770&sec=nation

8 See Donna L Betty, *Comment: Malaysia's Computer Crimes Act 1997 gets tough on cybercrime but fails to advance the development of cyberlaws*', 7 Pacific Rim Law & Policy Association, Pacific Rim Law & Policy Journal, Pac Rim L & Pol'y, p 351.

9 See '*Legal Forum For You And Me: Computer Crimes Act Revisited*', 17 April 2012, Legal Affairs Division, Prime Minister Department, Putrajaya.

10 See Chapter XXV (ss264-272A) of the CPC. This Chapter provides on the mode of taking and recording evidence in inquiries and trials. See Criminal Procedure Code (Amendment) Act 2006 (Act A 1274).

11 This information was obtained from an interview with Superintendent Victor Sanjos from Commercial Crime Investigation Department (Cybercrime and Multimedia Unit) on 8Â February 2011.

12 Unlike Malaysia, the United Kingdom ('UK') Association of Chief Police Officers ('ACPO') has provided an online information on a 'Good Practice Guide for Computer-based Electronic Evidence' that covers matters such as computer-based electronic investigations including search and seizure process, evidence recovery, disclosure and preservation of evidence. See, Code of Practice for CRIME. http://www.police.nsw.gov.au/about_us/acts_and_legislations/legislation_list/code_of_practice_for_crime

13 In the UK, the Code of Practice governs the duties of the police officers while conducting Internet investigation. See D Davis, *The Internet Detectives -- An Investigator's Guide*, Police Research Group, Home Office, 1998.

14 Police investigation (as of 1997) at http://www.lawnet.com.my/lawnetpublic/LegalInfor mation/LegalAwareness/PoliceInvestigation/tabid/76/Default.aspx

15 See Victor Sanjos, *Pencarian Bukti Melalui Komputer*, lecture to Registrar of Societies ('ROS'), 4 August 2005, Vistana Hotel, Kuala Lumpur.

16 The witness can either be a person from ISPs such as Jaring (MIMOS), TmNet and Maxisnet.

17 Section 112 mentions about oral examination of witnesses by the police. The witness is bound to answer all questions relating to the case in a truthful manner. His statement then shall be reduced into writing and signed by him. This section is read together with s 113 of the CPC that states about admission of statements made by the person who is charged with any offence

18 See 'Best practices for seizing electronic evidence' at http://www.ustreas.gov/usss/electronic evidence.shtmlh

19 See G Jack Bologna and Paul Shaw, *Avoiding Cyberfraud in Small Businesses: What Auditors and Owners Need to Know*, Canada: John Wiley & Sons, Inc, 2000, at p 81.

20 [2009] 3 MLJ 263; [2009] 3 CLJ 496 (HC).

21 Order 14A provides that the court may upon application of a party or on its own motion determine any question of law or construction of any document arising in any cause or matter without the full trial provided such question is suitable to be decided as it is.

22 [1987] MLJ 220.

23 'Cybercrime detection makes headway, Tech & U', *New Straits Times*, 20 July 2009 at p 4.

24 'Round the clock monitoring', *ibid* at p 5.

25 See Michael J O' Brien, Computer Crime: The United Nations Manual on Cybercrime, Exhibit 4: Guidelines for forensic analysis, via SANS at http://www.sans.org

26 This guideline is prepared by the International Organization on Computer Evidence ('IOCE') in 2002 of Digital Evidence Standards Working Group. Among the aims of the guideline is to provide framework of standards, quality principles and approaches for detection, preservation, recovery, examination and use of digital evidence for forensic purposes. See IOCE Guidelines for Best Practice in the Forensic Examination of Digital Technology, via IOCE at 'http://www.ioce.org/2002/ioce_bp_exam_digit_tech.html'

27 See NTI: Computer Incident Response Guidelines at http://www.forensics-intl.com/guidelns.html

28 See Colleen Wade (edit), Yvette E Trozzi (assoc Edit), Handbook of Forensic Services, revised 2003, US Department of Justice, FBI Laboratory Division At http://www.hq/lab/handbook/Forensics.pdf

29 *Ibid*.

30 See 'RM200m for forensics', *New Straits Times* 8 October 2011 at p 8.

31 See Toni Makkai, media release on 'Effective investigation of high tech crime', No 9/04, 2Â December 2004 at http://www.aic.gov.au/media/2004/20041202.html

32 See 'Police want more cyber crime fighters', *New Straits Times*, 23 October 2003.

33

See Simon Moores, 'Opinion: Is cybercrime unstoppable?', 11 April, 2005, via Computer Crime Research Center (CCRC) athttp://www.crime-research.org/articles/1130/ and 'Combining anti-spam standards', *New Straits Times (Computimes)*, 31 May 2004, p 16.

34 See 'Insult on Islam: Government will not keep quiet', Dr Mashitah, *Bernama*, 27 September 2010 at http://www.bernama.com.my/bernama/v5/newsindex.php?id=530695

35 See Beryl A Howell, *Real world problems of virtual crime*, Digital cops in a virtual environment: Cybercrime and Digital Law enforcement, 26-28 March 2004, via Yale University at http://islandia.law.yale.edu/ISP/digital%20cops/papers/howell_newcrimes.pdf

36 See Australia Transaction Reports and Analysis Centre (AUSTRAC), 'Evidence and the Internet', Action Group into the Law Enforcement Implications of Electronic Commerce ('AGEC'), Issues paper, September 2000 at http://www.austrac.gov.au/text/publications/agec/evidence.htm

37 The victim can write a letter directly to the Ministry who will then forward the report to the police. See 'Malicious e-mail: Ministry to assist police in probe', *New Straits Times*, 24Â September 2004, p 24.

38 See Chow Kum Hor, 'Uphill task to police e-mail rumor mongering', *New Straits Times*, 17Â September 2004, p 20.

39 This section allows the police officer conducting a search under ss 247 or 248 of the CMA 1998 or an authorised officer conducting a search under s 247 of the same Act to access the computerised data whether stored in a computer or otherwise. Subsection (2) of s 249 further provides that the 'access' includes (a) being provided with the necessary password, encryption code, decryption code, software or hardware and any other means required to enable comprehension of computerised data; and (b) the meaning assigned to it by sub-sÂ 2(2) and (5) of the CCA 1997.

40 See Russell G Smith, *Impediments to the successful investigation of transnational high-tech crime*, Australian Institute of Criminology (AIC), No 285:, ISBN 0 642 53848 4; ISSN 0817-8542. October 2004 at http://www.aic.gov.au/publications/tandi2/tandi285.html

41 See also Marc D Goodman, *Why the police don't care about computer crime*, 10 Harv JL Tech p 465, Summer 1997, via Harvard Law School at http://www.law.harvard.edu/articles/10hjolt465.html

42 In Malaysia, the extra-territorial offences are dealt under the Extra-Territorial Offences Act 1976.

43 See further Zaiton Hamin, *Investigating cybercrime: The Politics of Law Enforcement*, 3rd MSC International Cyberlaws Conference, 2-3 March, Nikko Hotel, Kuala Lumpur and Mohd Shukri, Computer Forensics issues in enforcement, 3rd MSC International Cyberlaws Conference, 2-3 March 2004, Kuala Lumpur.

44 See Trevor Rothwell, 'Presentation of Expert Forensic Evidence' in *Crime scene to court: the essentials of forensic science,* edited by Peter White, United Kingdom: Royal Society of Chemistry (RSC), Information Services, Cambridge, 1998, Chapter 13. In England and Wales the Forensic Science Service of a Home Office Agency is handling computer forensic examination.

45 Information obtained by interviewing Superintendant Kamarudin Md Din. See also his paper entitled 'Electronic Evidence Analysis: Royal Malaysian Police Experience', paper presented at National conference on Electronic Evidence: Towards Legal Compliance of Electronic Records Management & Electronic Discovery Readiness, Conference Hall, Perbadanan Putrajaya Complex, Putrajaya, 14 February 2006.

46 See Peter Sommer, 'Emerging problems in digital evidence', paper presented at the 3rd MSC International Cyber laws Conference, Kuala Lumpur, 2004. See also Panagiotis Kanellis & Others, *Digital Camera and Forensic Science in Cyberspace*, Chapter IV, Idea Group Publishing, United Kingdom, 2006.

47 In the US, for example, the third party data recovery services depend on a number of variables namely, Project Lead Times, Resource requirements, type of storage media, volume of data, operating systems, data format, and condition of media. See Alan M Gahtan, *Electronic evidence*. Thompson Professional Publishing, Carswell, Canada, 1999 at pp 27-29.

48 Besides that, Michael Chissick stated that it is a realistic conclusion that in the 21st century, the English legal system can no longer entertain forensic examinations in computer evidence. The lawyers, advocates and judges do not have the skills to undertake this task. There is no adequate funding to commission experts to perform this task. Thus, it is likely that over the years ahead people will be convicted for crimes they did not commit on the basis of faulty computer evidence or misunderstood computer evidence. See Michael Chissick (Ed) and Alistair Kelman, *E-commerce: Law and practice*, (3rd Ed), Sweet & Maxwell Ltd, A Thompson Company, 2002 at p 197.

49 In the US, the US Federal Trade Commission ('FTC') has trained more than 700 law enforcement and consumer protection officials from 20 different countries, including 17 federal agencies, 25 state governments and 14 Canadian consumer protection offices in online investigation and law enforcement techniques in locations ranging from Anchorage, Alaska to Paris. See *Fraud in the Internet*, 11 April 2005, via Computer Crime Research Center (CCRC) at http://www.crime-research.org/articles/Internet_fraud_0405/2re

50 See 'Demand up, supply short for forensic professionals', Tech & U, *New Straits Times*, 20 July 2009 at p 5.

51 See, Craig Ball, *Cross-examination of the Computer Forensic Expert*, 2004, via Craigball at http://www.craigball.com/expertcross.pdf.This article can be a good reference for lawyers who want to be a trial lawyer as well as an expert in computer forensic.