COMPUTER EVIDENCE: ISSUES AND CHALLENGES IN THE PRESENT AND IN THE FUTURE

Asst Prof. Dr Duryana Bt Mohamed[1]

Abstract

Computer evidence is sometimes known as digital evidence. It is also categorized as electronic evidence. In Malaysia, computer evidence is described as computer printout or output and admissible in the court of law. The admissibility of computer printout is mentioned in sections 90A, 90B and 90C of the Evidence Act 1950. The most common issues on computer printout are, 'whether the printout is produced by a computer in the course of its ordinary use' and 'whether certificate is needed or not needed to prove the authenticity of the computer printout'. These issues are raised in cases where the computer printout is produced as evidence. However, the admissibility of computer printout may be challenged when the evidence is available in other forms or medium. In the past, paper is produced as documentary evidence so as in the present cases. But in future, there may be situation where lawyers or prosecutors may not be able to satisfy the court in proving the reliability and admissibility of computer evidence. Things will be more complicated if the case involve cyber-related cases and various jurisdictions. Consequently, the suspect may escape liability due to technical defect or mistakes. This paper aims to discuss the position of computer evidence and its application in the Malaysian courts. Decisions on computer evidence from other courts of similar jurisdiction will also be referred to as to identify issues and the possible challenges that may arise in the future.

INTRODUCTION

Computer evidence is data from computer systems that is used as evidence in legal proceedings.[2] It exists when a computer is used by any person to do his works, to access other person's computer or to communicate with others. This data is kept in the hard drives of the computer system and available in different software programs.[3] It will remain in the computer until it is removed, deleted or rewrite. The data is used as evidence in variety of cases including cases of computer misuses, conspiracy, murder, rape, breach of online contracts, internet defamation and many others. This data will be retrieved, analysed and used as evidence to prosecute and charge the suspects. This paper will discuss the position of computer evidence in Malaysia and some other jurisdictions while highlighting few issues and challenges in the present and in the future.

A. Computer Evidence : Definition

Basically, there is no specific definition for the word computer evidence. Sometimes the computer evidence is also known as electronic evidence or digital evidence. If electronic evidence is used it will include computer generated evidence, computer produced evidence, computer printout, computer output, computer-based evidence, computer -related evidence, electronic data and electronic document.[4] On the other hand, digital evidence refers to evidence which is available in digital form or binary form consisting of the numbers and 01.[5] It originates from a multitude of sources including seized computer hard-drives and backup media, real-time e-mail messages, chat-room logs, ISP records, web-pages and digital network traffic. It also includes local and virtual

[1] Lecturer, Legal Practice Department, Ahmad Ibrahim Kuliyyah of Laws, International Islamic University Malaysia, P.0 Box 10, Jalan Gombak, Kuala Lumpur, Tel: 03-61964854, Fax: 03-61964854, email: mduryana@iium.edu.my

[2] 'Computer evidence' at http://www.computerevidence.co.uk/ viewed 10th July 2011

[3] Alan M. Gahtan,(1999). *Electronic evidence*. Canada: Carswell, Thompson Professional Publishing at32-35

[4] Ibid.

[5] Andrew E. Taslitz, 'Digital juries versus digital lawyers', *Criminal Justice Magazine*, Spring 2004, Volume 19 Number 1, via Abanet. <http://www.abanet.org/crimjust/cjmag/19-1/electronic.html and http://en.wikipedia.org/wiki/Digital_evidence viewed on 29 June 2011

databases, digital directories, wireless devices, memory cards, and digital cameras.[6] Such evidence, which is generated by digital system is wider than the electronic evidence which is produced by analogue system.[7]

In short, digital evidence is confined to evidence produced by digital technology, but its application is wider than electronic evidence since it extends to cell phones, digital audio and video which are the prevailing technology at present. However, there is no statutory definition for digital evidence in Malaysia although the Digital Signature Act 1997recognizes the application of digital signature in commercial activities.

The word 'computer' itself has been given different interpretation. According to section 3 of the Malaysian Evidence Act 1950 '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 of those functions in combination or in succession or otherwise howsoever conjointly, they shall be treated as a single computer.' While section 2(1) of the Malaysian Computer Crimes Act 1997 (CCA 1997) defines the term 'computer' as, 'An electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, storage and display functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include an 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; '

From the above two definitions it is submitted that the definition given by the Evidence Act 1950 extends the scope of the term 'computer' by looking at the ability of the device. Any device is regarded as a computer if it is capable of recording, storing, processing, retrieving or producing information. Any networking or combination of functions between two or more computers is considered as a single computer. While for the CCA 1997, the main focus is on the function of the device. The functions of the electronic device or computer are divided into four namely, performing logical, arithmetic, storage and display functions. Thus, for a device to fall under the definition of computer, it must be capable of performing the above functions. In short, the definition under the CCA is more technical and it limits the scope by excluding automated typewriter or typesetter, a hand calculator and non-programmable device from being a computer.

However, the term 'computer output' is not defined by the EA 1950. The definition is only available under section 2(1) of the CCA 1997 which states that a computer output is 'a statement or a representation whether in written, printed, pictorial, film, graphical, acoustic or other form-(a) produced by a computer;(b) displayed on the screen of a computer; or (c) accurately translated from a statement or representation so produced;' The above definition is so wide since it covers all types of statement or representation including translation that is produced by a computer and displayed on the screen. This term is used in the Malaysian cases and also used by other countries including Singapore, Australia and the United Kingdom (UK).[8]

Other than the EA 1950 and the CCA 1997, the Penal Code of Malaysia also mentions the word 'computer' in illustration to section 29. Section 29 explains about the meaning of document and it includes 'a matter recorded, stored, processed, retrieved or produced by a computer.' As for the word 'electronic' it is defined by section 5 of the Malaysian Electronic Commerce Act 2006 as

---

[6] Chet Hosmer, 'Proving the integrity of digital evidence with time', Spring 2002, Volume 1, Issues 1, International Journal Of Digital Evidence (IJDE), via IJDE. <http://www.ijde.org/archives/chet_article.html> viewed on 29 June 2011.

[7] Digital evidence is any information of probative value that is either stored or transmitted in a binary form. (Scientific Working Group on Digital Evidence SWGDE, July 1998). The word 'binary' was later changed to 'digital'. See Carrie Morgan Whitcomb, 'An Historical Perspective of Digital Evidence', International Journal Of Digital Evidence (IJDE), Spring 2002, Volume 1, Issue 1, via IJDE, <Http://www.ijde.org/archive/carrie_article.html>viewed on 26 June 2011.

[8] In Singapore, the meaning of the word 'computer', 'computer output' and 'output' was inserted by the Evidence (Amendment) Act 1996(No 8/1996). (ss3 and 35 of the Singapore Evidence Act). The term 'computer output' or 'printout' is also used by the UK (s2 (1) of the CMA 1993) and Australia.

'the technology of utilizing electrical, optical, magnetic, electromagnetic, biometric, photonic or other similar technology'. This definition focuses on the technology of utilizing various technological devices and does not specifically mention about computer. It refers to the application of technology in electronic commerce.

In brief, although there are different interpretations given to the term 'computer' and limited definitions on the term 'computer output' and 'electronic', there is so far no dispute as regards to the application and the meaning of the term. The term has been cited in few decided cases (reported and unreported) and it is applicable based on the type of offences. However, the definition given by the Evidence Act 1950 is more general and shall be applicable to any type of computer related cases. As for 'computer output', most cases discuss its admissibility under sections 90A, 90B and 90C of the Evidence Act 1950.

B. The Position Of Computer Evidence Under The Statutes

It is admitted that, in Malaysia, computer evidence is admissible as documentary evidence and primary evidence. This fact is established based on sections 3 and 62 of the EA 1950. According to section 3 (Illustration), 'matter recorded, stored, processed, retrieved or produced by a computer is a document'. Based on this section, a computer output or printout is regarded as documentary evidence. Further, section 62 of the EA 1950 provides that primary evidence means the document itself produced for the inspection of the court and Explanation 3 of the section provides that, 'a document produced by a computer is primary evidence'. In contrast, in the UK there is inconsistency in determining the status of computer evidence because the printout can either be a real evidence or hearsay evidence.[9] While in Singapore, computer output is also admissible as evidence.[10]

Further, the admissibility of computer output is also established under sections 90A, 90B and 90C of the EA 1950. Section 90A requires the production of the printout from the computer in the course of its ordinary use. It also emphasises on the status or position of the person who makes or tenders the document and the requirement that the certificate must be signed by a person responsible for the management of the operation of that computer or for the conduct of the activities for which the computer was used. If the person responsible for that computer is present then the certificate is not required as oral testimony of that person is sufficient and shall be admissible as evidence.

On the other hand section 90A(6) deals with the admissibility of a document which was not produced by a computer in the course of its ordinary use and is only deemed to be so. This section can only apply to a document which was not produced by a computer in the ordinary course of its use, or, in other words, to a document which does not come within the scope of section 90A(1). Thus, it cannot apply to a document which is already one that is produced by a computer in the ordinary course of its use. It cannot therefore be used as a mode of proof to establish that such a document was so produced. The document must be proved in the manner authorized by section 90A(2). It can now be discerned with ease that section 90A(6) has its own purpose to serve and can never be a substitute for the certificate.[11]

Section 90B focuses on the weight to be attached to a document, or a statement in a document, admitted by s90A. These include the manner and purpose of the creation as well as the accuracy of the document, the interval of time between the occurrence or existence of facts mentioned and also the supply of the information including the real intention of the person who supplies or had custody of the document.

Section 90C further affirms the position of ss90A and 90B. This section implies that the admissibility of computer printouts in Malaysia under ss90A and 90B shall be determined by the EA 1950 only and not by any other written laws, locally or abroad. Other written laws include other

[9] For example, a computer printout was regarded as real evidence in *The Statue of Liberty* [1968] 1 WLR 739 and *R* v W*ood* (1983) 76 Cr App R 23, CA. while in *Director of Public Prosecutor* v *Bignell* [1998] 1 Cr App R 1 the printout was regarded as hearsay evidence. See Michael Chissick (ed) and Alistair Kelman, '*E-commerce: Law and practice'*, A Thompson Company, Sweet & Maxwell Ltd, 2nd edit, 2000 at 172.

[10] See section 35 Singapore Evidence Act. (Chapter 97, 1997 Revised edition) and *Lim Mong Hong* v *Public Prosecutor* [2003] SGHC 161. The case discusses the application of sections 34, 35 and 36(4) of Singapore EA.

[11] See *Ahmad Najib b Aris* v PP [2007] 2 MLJ 505

provisions of the EA 1950 itself and the Banker's Books (Evidence) Act 1949. But, based on the wording of s136 it can be stated that the court has a discretionary power to determine the relevancy and admissibility of computer evidence, testified or produced by the witness during his examination.[12] If the evidence is clear the court would admit it as it thinks just. How the issue on the admissibility of computer output is decided by the court?. This issue is discussed below.

C. Issues On Computer Output/Printout

Computer evidence can create many issues in variety of cases. Among the cases that involve computer evidence are copyright and trademarks, misuse of ATM machine, murder, defamation and child pornography. The issues in these cases are solved by referring to relevant laws including the cyberlaws and decided cases. Normally, the common issues raised by the prosecutor or the counsel for plaintiff and defendant are based on what is provided by the EA 1950.

The common issue raised on computer output is on whether the plaintiff or defendant has complied with the requirement of s90A(2) of the EA 1950. This section requires the production of certificate from the person responsible for the work of the computer. However, the certificate is not needed if the said person is present during the hearing of the case. This principle was adopted and affirmed in several cases namely, *Standard Chartered Bank* v *Mukah Singh,*.[13] *Gnanasegaran a/l Pararajasingam* v *Public Prosecutor*[14], *Petroliam Nasional Bhd & Ors* v *Khoo Nee Kiong, Hanafi bin Mat Hassan* v *Public Prosecutor*[15],*Ahmad Najib b Aris* v *Public Prosecutor* [16], *Azlan bin Alias* v *Pendakwaraya* [17] and *Bespile Sdn Bhd (in liquidation) v Asianshine Sdn Bhd & Ors*[18].

. However, in all these cases the decision was made based on different facts produced before the judge. In *Standard Chartered* case, the defendant's counsel submitted that the computer-generated loan ledger cards were inadmissible and should not have been admitted because the plaintiff failed to produce a certificate from the person responsible for the computer. However, the judge in this case emphasised that since there was no challenge made to the evidence adduced by the witnesses and the evidence was produced in the ordinary course of business it is not necessary for the plaintiff to comply with the requirement of s90A(2). The learned judge further stated that the certificate does not need to be produced unless the evidence is disputed at the time it was adduced. In this case the defendant seemed to agree with what had been adduced by the plaintiff. Finally, the court decided to allow the plaintiffs' claim for the amount due.

In *Gnanasegaran,* both oral and documentary evidence were produced by Mr. Zainal, a bank officer who was responsible for the printout and 'for the conduct of the activities for which that (branch) computer was used' during the relevant period. He was called to testify and a computer printout of statement of accounts was produced as evidence. The court decided that it is sufficient to accept Zainal's testimony that the statement of accounts was a computer printout. Furthermore, it would be superfluous for Zainal to issue a certificate under sub-section (2) to s90A when first hand evidence that 'the document so were produced by a computer' was given by himself. It would also be superfluous to have a provision such as in sub-section (6) if in every case a certificate must be produced. The subsection admits, 'a document produced by a computer, or a statement contained in such document whether or not it was produced by the computer after the commencement of the criminal or civil proceeding or after the commencement of any investigation or inquiry in relation to the criminal or civil proceeding or such investigation or inquiry. It considers and any document so produced by a computer shall be deemed to be produced in the course of the ordinary use of the

[12] Section 136 of the EA 1950 provides that the court has to decide as to the admissibility of evidence given by witnesses during the examination of witnesses. It is upon the discretion of the judge to admit or refuse to admit the evidence. The judge may refuse to admit certain facts produced by the computer printout if the fact is not relevant or if the fact does not seem to support the facts in issue. However, if proved, the evidence would be relevant then the court will admit it.
[13] [1996] 3 MLJ 240(HC).
[14] [1997] 3 MLJ 1(CA). This case was followed by the Court of Appeal in *Ahmad Najib b Aris* v *Public Prosecutor* [2007] 2 MLJ 505. The later case refers to s90A(1)(2) and (6) of the EA 1950.
[15] [2006] 4 MLJ 134.
[16] [2007] 2 MLJ 505
[17] [2009] MLJU 0480 (CA)
[18] [2010] 4 MLJ 824(HC)

computer. However, subsection 90A(7) disallows the admissibility of computer evidence in criminal proceedings if it is tendered by a person who manages the operation of the computer, or who is involved directly or indirectly in the production of the same document. This condition is also applicable to those who tender the documents on behalf of that person. Thus, based on the above statement the learned judge (Shaikh Daud) concluded that the evidence given by Zainal was admissible eventhough a certificate was not produced. His judgment was unanimously agreed to by Mahadev Shankar (JCA) and Abdul Malik Ahmad (J). According to Mahadev Shankar (JCA): (see p14)

> 'The viva voce evidence of the man in the witness box counts for more than a certificate issued by him'(p13)section 90A was enacted to bring the 'best evidence rule' up to date with the realities of the electronic age. Receipts for payments in and records of payments out of bank account are keyed in by the tellers into the terminals at the counter, and the information is electronically stored in the bank's computer. The information so stored is not in itself visible to the naked eye. To become visible, the raw data has to be projected on a video display unit and/or printout. So the definition of a 'document' in s 3 of the Act now provides that both the display on the video display unit and the print out qualify as documents. The last two items in the Illustration to the section have spelt this out.'

In the above case, the plaintiff's claim was allowed and the appeal was dismissed. Relying on s90A(2) above, the court in this case held that the evidence given by Zainal should be admissible.[19]

The decisions in the above two cases were referred to by the High Court in Penang in the case of *Petroliam Nasional Bhd & Ors* v *Khoo Nee Kiong*.[20] In this case, the plaintiffs' affidavit in support deposed that the contents of the affidavit are within his personal knowledge unless otherwise stated. The defendant did not challenge nor dispute this assertion of the deponent in the defendant's affidavit in reply. Pursuant to this matter Su Geok Yiam JC stated that there is no need for the plaintiffs to show a prima facie case but that it was sufficient to show that there was a bona fide serious question to be tried. She further stated that:

> 'there is no necessity for the plaintiffs to exhibit s90A certificate in his affidavit in support of the plaintiffs' application in respect of the computer printouts containing the impugned statements. The reason is because the plaintiffs need only tender the s 90A certificate if the plaintiffs do not wish to call the officer who has personal knowledge as to the production of the computer printouts by the computer to testify to that effect in the trial proper'

Thus, the plaintiff's application was allowed. In this case, the learned judge also relied on s90B when estimating the weight of such evidence.

In summary, the need to produce a certificate to prove the reliability of the computer printout depends very much on the facts of the case. The court has rejected the evidence by a witness who claimed no responsibility to the computer printout produced by him. (as decided in *Public Prosecutor v Ong Cheng Heong*[21].) Thus, the most important elements that need to be fulfilled are the printout from the computer should be produced in the course of its ordinary use and the person who makes or tenders the document is the person responsible to that output. There is no need for a certificate as his oral testimony is sufficient and shall be admissible as evidence. Since ss90A, 90B and 90C of the EA 1950 clearly establish that they are exceptions to hearsay evidence[22] it seems that there

---

[19] However, the ambit or application of s90A(2) is limited and circumscribed by s2 of the same Act. Therefore, this section is not applicable in an application for summary judgment since the application is decided upon affidavit evidence. See *Southern Finance Bhd (formerly known as United Merchant Finance Bhd)* v *Sun City Development Sdn Bhd & Anor* [2006] MLJ 673. (HC, Kuala Lumpur).

[20] [2003] 4 MLJ 216.

[21] [1998] 6 MLJ 678; [1998] 4 CLJ 209

[22] Hearsay or indirect evidence is evidence which is reported by a witness from other sources. It is produced or related by a person who either has seen or heard the incident from other person. See *PP* v *Mohd. Amin Mohd Razali &* Ors [2002] 5 CLJ 281 at p325. The requirement for hearsay evidence is very strict when it comes to establishing the truth of fact made. Normally, witness is not directly involved in the incident but merely related the facts in the form of oral, written or act.

is unlikely that in Malaysia the position of computer printout in the EA will be challenged. However, the admissibility of such evidence can still be challenged on the issue of its relevancy, reliability and weight. Thus, if the computer output is a record of human assertions, depending on human perception and the supply of such information to the computer, it would be hearsay and therefore inadmissible unless it falls within the hearsay exception.[23]

D. Present And Future Challenges

Gathering and proving computer evidence will be more challenging with the development of new technology. These challenges will continue to develop until certain measures are adopted and the laws are sufficient to tackle the problems. Certain countries have even reviewed and amended their evidential law, updated their technology and developed certain measures to deal with evidence derived from electronics means. [24] In Malaysia, the laws on computer evidence are still developing. Thus, it is important to identify the challenges presently faced by the investigators, prosecutors and the defence counsels and what may happen in the future. The followings are some of the common issues and challenges encountered by the investigator, prosecutor and the defence counsel.

a) Locating Computer Evidence

Locating data or evidence can be challenging since the data are created and stored in various places. The data can also be sent from various devices that may contain complex as well as large amount of data. These devices include desktop computer, laptop, Unsecured public Wi Fi, secured Public Wi Fi and VPN (Virtual Private Network).[25] A portable music player such as iPod is also one of the devices that will challenge the investigator's skills and knowledge as well as the forensic expert in locating the evidence of crimes.[26] The issue is how to locate the evidence and what is the appropriate law governing the process of retrieving data from such devices?.

Usually, specific software is used to locate and retrieve any data from computer system. Norton software, for instance, is used by the police investigator to recover the evidence including the deleted files or data. If the case is criminal in nature, the Investigating Officer (IO) with the assistance of the computer forensic expert will do the investigation and detection of computer evidence before the retrieval of data from the seized computer. The IO is allowed to do so under the Criminal Procedure Code (Chapter XIII of the CPC), the Computer Crimes Act 1997 (ss10 and 11 of the CCA), the Communications and Multimedia Act 1998 (ss245 to 262 of the CMA) and the Digital Signature Act 1997 (ss76 to 81 of the DSA). The IO may also do the investigation with or without the search warrants. However, with the search warrants the police may access the premise of the suspect and seize the computer belonged to him.

Nevertheless, the challenge to the IO and computer forensic expert is that they must ensure there is no break in the chain of evidence collected. Proper security procedures and mechanisms are needed to protect the integrity of the computer during the gathering of computer evidence. In other

---

[23] See Abu Bakar Munir, *Cyber law: Policies and challenges,* Butterworths, 1999 at 253.

[24] In India for instance, a proposal was made to develop a national digital forensic response model for efficient response to incidents of cybercrimes. This model focuses on processing digital evidence during an investigation process. See Ciardhuain Seamus O., " An extended model for cyber crime investigation", 2004 . International Journal of Digital Evidence Summer and Ayaz Khan, Uffe Kock Wiil & Nasrullah Memon, "Digital Forensics and Crime Investigation: Legal Issues in Prosecution at National Level", 2010 Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5491889 viewed on 5 May 2011

[25] Amelia Philips, E-evidence and International Jurisdictions: Creating Laws for the 21st century, proceedings of the 44th Hawaii International Conference on System Science, 2011 at IEEE at http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05719006 viewed on 20th June 2011. Other devices include personal cell phone, corporate cell phone, Black Berry and digital camera.

[26] Matthew Kiley, Tim Shinbara & Marcus Rogers, "iPod Forensics update," International Journal of Digital Evidence (IJDE) Spring 2007, Vol.6 Issue 1 at http://www.utica.edu/academic/institutes/ecii/publications/articles/B40DD0EA-D340-962F-F98B868F3C69129F.pdf viewed on 9 May 2011

words, the evidence collected should be properly preserved, remain original and authentic. These criteria are very important for the admissibility of computer evidence in the court of law.

b) Recovery And Discovery Of Computer Evidence And The Right To Privacy

Computer data or any data in electronic medium may be recovered by many ways using specific software. Procedurally, the recovery of data may be made using discovery method. This method of discovery is used to discover relevant documents kept by the other party in his computer or any places and believed to be relevant to the case. In this regard, the parties to the case may either mutually agree to exchange the documents in their possession or may comply with the court order for discovery. Order 24 of the Malaysian Rules of High Court 1980 allows this process even though there is no specific provision on discovery of computer evidence or electronic evidence in the Rules of High Court 198 and other rules of court. The lawyers should also learn to adopt electronic discovery method since it has been practiced in many countries including the United States, United Kingdom, Australia and Singapore.[27]

However, caution must be exercised during this process since the parties may challenge on the method used to recover the data. Among the issues are the violation of privacy and privilege information. These two issues can be settled if the discovery of data is done according to the law. In fact, there shall be no violation of privacy if the investigator or authorized officer access the computer according to s249 of the Communications and Multimedia Act 1998 (CMA) and s79 of the Digital Signature Act 1997 (DSA) which provide that the data stored in the computer or otherwise can also be accessed by the police officer or the authorised officer. Further, s10 of the Computer Crimes Act 1997 (CCA) also confers powers of search, seizure and arrest to any police officer. Nevertheless, both CMA and DSA require the officers, the police officers and the authorised officers to obtain written consent from the Minister of Energy, Water and Communications prior to conducting a search and seizure.[28]

c) Development of New Technology and New Crimes

Forensic analysis must present accurate result to the court. In order to do so the computer forensic expert must have good skills and knowledge on the computer forensic and also digital forensic science. Their findings will be considered by the court as expert opinion and their role is recognized not only in Malaysia but also other countries. Therefore, forensic examiners must be able to explain in detail about the analysis conducted and learn how to quantify and account for the resulting uncertainties which include the system clock of the computer which represents the time, date and sequence of events. However, determining whether the system clock is accurate can be a challenging task in a network environment.[29]

The admissibility of computer forensic evidence is not specifically stated in the Evidence Act 1950 but section 45(1) of the Act recognizes the opinion of persons specially skilled in science. Their opinions are considered as relevant facts.. The expert must also follow certain procedures when giving evidence.[30] However, what may challenge the computer forensic investigators or experts is on the new technology, new technique and new tools used by the criminals to commit crimes in cyber space. Thing such as cloud computing[31] is challenging since no one can accurately describe 'the

---

[27] See for instance Amalia R. Miller & Catherine E. Tucker, 'Electronic discovery and the adoption of information technology, 18 January 2010 at http://ssrn.com/abstract=1421244 viewed on 20 May 2011.

[28] Section 6 of the CMA 1998 provides that "Minister" means the Minister for the time being charged with the responsibility for communications and multimedia.

[29] See Eoghan Casey, Error, Uncertainty and Loss in Digital Evidence, IJDE, Summer 2002, Vol. 1 Issue 2. <http://www.ijde.org/archives/02_summer_art1.html> viewed on 29 June 2011

[30] *Wong Shop Soaw v PP* [1965] 31 MLJ 247. See further Mohd Akram Shair Mohamed, 'Limit to the role of an expert '[1996[2 CLJ xxiii.

[31] The US National Institute of Standard and Technology (NIST) defines cloud computing as ' a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It promotes availability and is composed of five essential characteristics**,** three service models, and four deployment models. 'It has several essential characteristics.

cloud' and all its implication.[32] According to one researcher, "Cloud forensics is difficult because there are challenges with multi-tenant hosting, synchronization problems and techniques for segregating the data in the logs Most of the cloud service providers are not open to talking about this because they don't know the issue".[33]

Hence, in order to tackle these challenges the investigator and forensic expert need to use and apply appropriate searching mechanism such as using abstraction layers,[34] correct digital forensic analysis tools[35] and be prepared to adopt new techniques to search for the computer data or digital evidence. In fact, it was also suggested that there is a need to adopt a new national model of digital forensics by removing the barriers of technical, judicial and legal issues.[36] In addition to that, the analysis or the process of obtaining on-line data will expose it to change or alteration whether intentionally or unintentionally. Therefore, strict precautions are required when police forensic team or a computer expert is extracting such evidence.

d) **Proving the Reliability, Authenticity and Accuracy of computer evidence**

Procedurally, criminal cases must be proved beyond any reasonable doubt while civil cases require the counsels to prove such cases on the balance of probabilities. Usually, proving the reliability, authenticity and accuracy of computer evidence may involve civil and criminal cases. Hence, it is not an easy task to do so since documents in electronic format have a number of features and available at various places. Since, the court accept only relevant documents the Evidence Act 1950 has laid down several provisions on the need to produce relevant documents. They are sections 6, 35 to38 and sections 90A to 90C.[37] Although there are facts which need not be proof[38]proving reliability of evidence is essential. The court will also accept admissions and witness statements to prove the authenticity of the evidence. Thus, the witness must be able to identify the evidence and explain in court.

The insertion of sections 90A, 90B and 90C to the EA 1950 affirm that evidence from computer is admissible if produced in compliance with the stated provisions. Although certificate is not needed to prove the evidence, the defence counsels can still rely on this defence. However, the issue of certificate was settled by the court in few decided cases mentioned above.[39] Further, the counsel may argue on the reliability of expert opinion who is supposed to maintain the originality of the data collected.[40] Sometimes, the data was tampered and even destroyed during the gathering process. This will render the evidence being rejected by the court. Further, the admissibility of computer evidence could be challenged by attacking the weight or reliability of the evidence.[41] If the court satisfied that the evidence is not reliable, the court may dismiss the case.

The NIST definition of Cloud Computing (draft) at http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf retrieved 5 May 2011

[32] Amelia Philips, E-evidence and International Jurisdictions: Creating Laws for the 21st century, fn. 24.

[33] 'Cloud computing crime poses unique forensic challenges', The DNS DIRECT Blog, 19th February 2011 at http://www.dns-direct.typepad.com viewed on 19th July 2011

[34] Brian Carrier, Defining Digital Forensic Examination and Analysis Tools using Abstraction layers, IJDE Winter 2003 Volume 1 Issue 4.

[35] Ibid.

[36] Ayaz Khan & Uffe Kock Wiil & Nasrullah Menon, Digital Forensics and Crime Investigation: Legal issues in Prosecution at National Level, 2010 Fifth Workshop on Systematic Approaches to Digital Forensic Engineering at http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05491968 viewed on 5 June 2011

[37] In Singapore, this requirement is mentioned under sections 35 and 36 of the EA.

[38] See sections 56, 57 and 58 of the Evidence Act 1950.

[39] The Singapore High Court decided that the computer evidence shall be admissible as long as the computer printout which was produced maintain its authenticity and accuracy as required by s35(1) (a) of the Singapore Evidence Act. See further *Alliance Management SA* v *Pendleton Lane P and Another And Another Suit* [2008] SGHC 76, [2008] 4 SLR 1.

[40] See further, Stephen Mason, Authentication of electronic evidence, Information Age, 18 October 2006 at http://www.ingfoage.idg.com.au viewed on 5 June 2011.

[41] See Michael Chissick (ed) and Alistair Kelman, '*E-commerce: Law and Practice',* 3rd edit, A Thompson Company, Sweet & Maxwell Ltd., 2002 at 192.

e) **Multiple Jurisdictions**

The borderless nature of the internet has allowed the commission of crimes from anywhere around the world. Since internet is one of the sources of computer evidence determining the law governing such evidence is sometimes very challenging. The challenge is to gather the evidence, investigate and prosecute the suspect who is living in other country but committing the offence in Malaysia. In this situation, working with INTERPOL is one of the best ways to arrest the suspect. However, if the evidence is not sufficient the suspect may escape from any liability.

In Malaysia, problem on cross border issue can be referred to provisions under the CPC (section 127A which provides on liability for offences committed out of Malaysia); Extra-territorial Offences Act 1976; Computer Crimes Act 1997 (CCA)(section 9 which provides that, ' the Act shall apply to any person who have committed an offence outside Malaysia'.) and the Mutual Assistance in Criminal Matters Act 2002 (MACMA).[42] Under these statutes the suspect will still be liable as if he has committed the crimes in Malaysia. However, MACMA does not authorise the arrest or detention of a person with a view to extradition. This means if a hacker is from outside Malaysia but committed hacking in Malaysia a request for assistance in locating or identifying the suspect can be made under MACMA, but to extradite the person may be difficult.[43] Furthermore, the application of MACMA 2002 is subject to approval by the Attorney General (the AG) who will only approve a request that is reasonable and made in the appropriate way. But under s18 of MACMA 2000 the Minister responsible for legal affairs in Malaysia is allowed to make a direction that provisions under MACMA 2000 be applied in relation to a request for mutual assistance in specified criminal matters by the United States.

Another issue that could be raised by the parties in determining which court to hear the case is on the issue of morality due to the fact that certain countries may consider certain offences as morally right and lawful. Hence, action may not be taken against the suspect if the law in his country says he has not committed any offences. Nevertheless, the problem can be resolved through mutual cooperation between countries and extradition treaties. The Council of Europe, for instance, has decided to approve the Cybercrime Convention in 2001[44] to deal with international issues. It plays a very important role in providing international legal framework in investigating, extraditing and prosecuting the computer or cyber criminals. However, this Convention only emphasizes on few things such as computer hacking, computer virus distribution and internet fraud. It does not cover the propagation of hate materials on the internet because that will violate the right of free speech to the citizen of Europe and the United States.[45] There is also no mention about its application in developing countries, many technical problems were neglected and there were also critics on human right issue.[46] In other words, although there are laws governing transborder crimes in the cyberworld, the enforcement of international law and international cooperation is very important.

f) The Law May Be Outdated And Reliance Will Be On The Case Law

The technology develops very fast but the law needs times for review and updated. Nonetheless, this does not mean there must be a new law in every new technology. Traditional law can still be used but with some modifications and updated. Further, the law reform committee must be aware

---

[42] (Act No. 621 of 2003). This Act came into force on 1st May 2003.[PU (B) 168/2003]. See Current Law Journal. <http://www.cljlaw.com/membersentry/legislationsectiondisplayformat.asp> viewed on 29 April 2005. The authority responsible to implement this Act is the AG. Among the requests that can be made under this Act are request for taking of evidence, assistance in locating or identifying persons and assistance in service of process (s8). See also Kamal Baharin bin Omar (DPP), a workshop on Criminal Law and Procedure: Amendments, 28 April 2005, Corus Hotel, Kuala Lumpur.

[43] The other extradition law in Malaysia is Extradition Act, 1992 (Act No. 479 of 1992).

[44] Convention on Cybercrime at http://conventions.coe.int/Treaty/EN/eTreaties/html/185.htm viewed on 9th May 2011

[45] Programme on "Strengthening the rule of law in the Arab states- project on the modernization of Public prosecution offices' United Nation Development Programme (UNDP), 19-20 June 2007 , Kingdom of Morocco at http://www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf viewed on 9 May 2011.

[46] Ibid.

about the new development in cyber attacks and the Ministry concern has to react immediately as to combat the attacks. On this regard, the then Inspector General of Police YDH Tan Sri Mohd. Bakri Bin Hj. Omar has even stated that, 'In this technological age, police work in all fields, and especially crime forensics, require equipment that is up-to-date. I would urge for a review of laws that govern police actions – laws that unduly inhibit the scope of police investigations must be amended to facilitate swift police action.'[47] The statement implies that there shall be no outdated law in combating the crimes.

In Malaysia, although there are several cyberlaws, only few laws are referred too when there are cases of hacking and misuse of network facilities, The relevant laws for these offences are supposed to be the Computer Crimes Act 1997 (CCA) and the Communications and Multimedia Act 1998 (CMA). But since those cases were not reported in any law journal it is difficult to further analysis the effectiveness of the laws. Conversely in Singapore, there are quite a number of cases decided under the Computer Misuse Act[48] and these cases have become the precedents and followed by the later cases.

The hacking attacks in June 2011 on almost 200 websites by 'Anonymous' hackers group had given impact to the way issues on cyber attacks are handled. The Government has tightened the level of security in this country while the public are more aware of the attacks. Although these attackers will continue to find new ways to launch the cyber attacks the challenges can be handled if the enforcement of the existing laws (particularly the cyberlaws) is improved. In fact, more laws are needed to combat the cyber attacks.[49]

CONCLUSION

The technology can change the landscape and the method of proving computer evidence. Thus, the laws should be able to cope with the technological changes. In future, there may be more complicated cases and tracing the electronic or computer evidence will be more challenging. The fear is the suspect can just escape from any liability due to inadequacy in the laws and lack of technological advancement. Hence, setting up a precedent from cases is very important in order to provide a good reference for future cases. At the same time, there must also be continuous update of the laws and regulations.

In addition, cooperation between countries needs to be upgraded and cultivated in preventing more acts of computer misuses and abuses. More MOUs are needed between countries in order to extradite the perpetrator. There is also a need to thoroughly examine the effectiveness of extradition treaties and how the law enforcement may face challenges in gathering computer evidence and prosecuting the offenders when it involves transnational jurisdiction. Knowledge on maintaining the cyber security, the effect of abusing computers, the risk and the legal consequences of computer abuses must be informed to the society at large. In other words, the law may seem to be adequate now but it may be obsolete and outdated in the future. Thus, so long as technology develops, the challenges to search for computer evidence or electronic evidence and proving its reliability will never end.

---

[47] See Key note address by the then Honourable Inspector-General of Police, YDH Tan Sri Mohd. Bakri Bin Hj. Omar in conjunction with the official opening of a Seminar on "Industrial Security Issues: A Business Solutions Approach", 26th July 2004, Gurney Hotel, Penang, <http://www.rmp.gov.my/rmp03/040901_igp_keynote.htm> viewed on 12 April 2005. and V.P Sujata, "Legislation Needed to combat Internet crime syndicate," *The New Straits Times*, 9 April 2004 at http:www.ctimes.com.my/ viewed on 12 April 2004.

[48] See for example, *Lim Siong Khee* V *Public Prosecutor* [2001] 2 SLR 342, *PP*. v *Muhammad. Nuzaihan bin Kamal luddin* [2002] 1 SLR 34 and *Tan Chye Guan Charles* v *PP* [2009] SGHC 128, [2009] 4 SLR 5

[49] For instance, in the UK, there is Fraud Act 2006 which deals specifically on computer related fraud cases.