ARTICLE:

DIGITAL EVIDENCE IN MALAYSIA

By **Gita Radhakrishna**

Introduction

Evidence is anything that demonstrates, clarifies or shows the truth of a fact or point in question. Traditionally there has been resistance to the acceptance of new forms of evidence that emerge as a result of evolving technology. For instance, in the thirteenth century, Emperor Frederick II proclaimed instruments written on paper to be invalid.[1] Eventually however, parchment was replaced by paper in general use, and hand written paper documents were accepted as evidence in courts. Later, with the introduction of typewriters, many lawyers failed to understand the technology and failed to obtain expert evidence giving rise to problems of authenticating the typewritten document.[2] A similar phenomenon is occurring today with respect to electronic documents. Information technology (IT) has become very much a part of the fabric of life. Specific legislation has been necessary to address issues arising from the application of technology in various areas of human endeavour. The law of evidence has had to take cognizance of this, because computer generated evidence (digital evidence) has frequently to be collected from various sources, even extra jurisdictional, for use in legal proceedings. Amendments to the Malaysian Evidence Act 1950 in 1993 provided for the admissibility of computer generated documents. This paper examines the legal framework for the admissibility of digital evidence in Malaysia and discusses a series of cases highlighting the issues that have arisen in this context.

Computer generated evidence under the Evidence Act 1950

By s 3 of the Malaysian Evidence Act 1950 (Evidence Act), the word 'evidence' includes:

> (a) all statements which the court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry: such statements are called oral evidence;
>
> (b) all documents produced for the inspection of the court: such documents are called documentary evidence;

'Document' under the Evidence Act means:

> any matter expressed, described or howsoever represented, upon any substance, material, thing or article, including any matter embodied in a disc, tape, film, sound track or other device whatsoever, by means of -
>
> (a) letters, figures, marks, symbols, signals, signs, or other forms of expression, description, or representation whatsoever;
>
> (b) any visual recording (whether of still or moving images);
>
> (c) any sound recording, or any electronic magnetic, mechanical or other recording whatsoever and howsoever made, or any sounds, electronic impulses, or other data whatsoever;
>
> (d) a recording, or transmission, over a distance of any matter by any, or any combination, of the means mentioned in paragraph (a), (b), or (c),
>
> or by more than one of the means mentioned in paragraphs (a), (b), (c) and (d), intended to be used or which may be used for the purpose of expressing, describing, or howsoever representing, that matter.

Section 3 provides illustrations of what is meant by a document; any writing words printed, lithographed or photographed; a map, plan, graph or sketch; an inscription on wood, metal, stone or any other substance, material or thing; a drawing, painting, picture or caricature; a photograph or a negative; a tape recording of

1 *Giorgio Bovenzi, 'Liabilities of System Operators on the Internet', 11 Berkley Tech. L. J. 93 (1996), 93, who in turn cites Douglas C. McMurtrie, The Book: The Story of Printing and Book Making (New York: Random House, 1943), 67.*

2 *Winsor C. Moore, 'The Questioned Typewritten Document', Minnesota Law Review Volume 43 [1959], 727-743.*

a telephonic communication, including a recording of such communication transmitted over distance; a photographic or other visual recording, including a recording of a photographic or other visual transmission over a distance; a matter recorded, stored, processed, retrieved or produced by a computer.

Further, a 'computer' is defined as

> 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;

However this definition has now been repealed by the recent Evidence (Amendment) (No. 2) Act 2012 in favour of the definition in the Computer Crimes Act 1997 which defines 'computer' as:

> 'An electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include —
>
> (a) an automated typewriter or typesetter;
>
> (b) a portable hand held calculator;
>
> (c) a device similar to those referred to in paragraphs (a) and (b) which is non-programmable or which does not contain any data storage facility.'

Although the two different definitions for 'computer' in the Computer Crimes Act 1997 and the Evidence Act 1950 did not give rise to any issues of interpretation in practice, the amendment has brought consistency in the definition of the term 'computer' in both the statutes.

Amendments to the Evidence Act in 1993 provided for the admissibility of 'computer-generated documents' in sections 90A, 90B and 90C. Section 90A is the principal section and with seven subsections, sets the requirements for admissibility and proof. Section 90B deals with the probative value to be attached to the evidence, while s 90C stipulates that the provisions of sections 90A and 90B shall prevail over any other provisions in any other statutes.

Section 90A(1) provides as follows:

> (1) In any criminal or civil proceeding a document produced by a computer, or a statement contained in such document, shall be admissible as evidence of any fact stated therein if the document was produced by the computer in the course of its ordinary use, whether or not the person tendering the same is the maker of such document or statement.

Section 90A(2) provides:

> (2) For the purposes of this section it may be proved that a document was produced by a computer in the course of its ordinary use by tendering to the court a certificate signed by a person who either before or after the production of the document by the computer is responsible for the management of the operation of that computer, or for the conduct of the activities for which that computer was used.

This provision has caused a great deal of argument on whether a certificate is required in every case where 'computer generated evidence' is sought to be adduced. The Court of Appeal went to great lengths to examine and clarify the provisions in the case of *Gnanasegaran Pararajasingam v PP* [1997] 4CLJ 6, discussed below.

As for the certificate, it shall be sufficient under s 90A (3) for a matter to be stated to the best of the knowledge and belief of the person stating it. It shall then be admissible in evidence as prima facie proof of all matters stated in it without proof of signature of the person who gave the certificate:

> (3) (a) It shall be sufficient, in a certificate given under subsection (2), for a matter to be stated to the best of the knowledge and belief of the person stating it.
>
> (b) A certificate given under subsection (2) shall be admissible in evidence as *prima facie* proof of all matters stated in it without proof of signature of the person who gave the certificate.

Once the certificate is produced, there is a presumption under s 90A(4) that the computer referred to in the certificate was in good working order and was operating properly in all respects throughout the material part of the

period during which the document was produced.[3]

By the provisions of s 90A(5), a document is deemed to have been produced by a computer, directly or indirectly, and whether or not there was any direct or indirect human intervention. Section 90A(6) provides a further presumption in relation to a document, whether produced by a computer or not:

> (6) A document produced by a computer, or a statement contained in such document, shall be admissible in evidence 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, and any document so produced by a computer shall be deemed to be produced by the computer in the course of its ordinary use.

It will be observed that s 90A(1) and s 90A(6) appear to be incompatible and inconsistent with each other. The 'deeming' provision in s (6) was seen as a way of circumventing the requirement for the certificate as stipulated in s 6(1) until the Federal Court in *Ahmad Najib Aris v PP* [2009] 2 CLJ 800, discussed below, clarified the distinction between subsections (1) and (6).

Section 90A(7) provides as follows:

> (7) Notwithstanding anything contained in this section, a document produced by a computer, or a statement contained in such document, shall not be admissible in evidence in any criminal proceeding, where it is given in evidence by or on behalf of the person who is charged with an offence in such proceeding the person so charged with the offence being a person who was—
>
> (a) responsible for the management of the operation of that computer or for the conduct of the activities for which that computer was used; or
>
> (b) in any manner or to any extent involved, directly or indirectly, in the production of the document by the computer.

As such, the subsection precludes an accused in any criminal proceeding from using self corroborating evidence generated by a computer under his own management or supervision.

Section 62 provides that 'Primary evidence means the document itself produced for the inspection of the court'. A document produced by a computer is primary evidence. Thus computer-generated evidence may be admitted in court without difficulty and such evidence is primary evidence, even though it is not possible to distinguish between 'original' and 'copy'. The provisions in s 90A ostensibly provide the necessary safeguards.

Section 90B deals with the weight or probative value to be attached to a document or statement contained in document, admitted by virtue of s 90A:

> In estimating the weight, if any, to be attached to a document, or a statement contained in a document, admitted by virtue of section 90A, the court—
>
> (a) may draw any reasonable inference from circumstances relating to the document or the statement, including the manner and purpose of its creation, or its accuracy or otherwise:
>
> (b) shall have regard to—
>
> (i) the interval of time between the occurrence or existence of the facts stated in the document or statement, and the supply of the relevant information or matter into the computer; and
>
> (ii) whether or not the person who supplies, or any person concerned with the supply of, such information or the custody of the document, or the document containing the statement, had any incentive to conceal or misrepresent all or any of the facts stated in the document or statement.

Challenging the admissibility of computer generated evidence

Gnanasegaran Pararajasingam v PP [1997] 4CLJ 6 was one of the early cases where direction was sought from the Court of Appeal on the admissibility and probative value of computer generated documents. Mahadev Shankar JCA, clarified that

> 's. 90A was enacted to bring the "best evidence rule"

3 *It is not clear what 'good working order' and 'operating properly' mean, and for a discussion of this problem that is also a problem in England & Wales, see Stephen Mason, gen ed, Electronic Evidence (2nd edn, LexisNexis Butterworths, 2010), Chapter 5.*

up to date with the realities of the electronic age. The effect of s. 90A(1) in the present scenario is that it is no longer necessary to call the actual teller or bank clerk who keyed in the data to come to Court provided he did so in the course of the ordinary use of the computer. This is a relaxation of the direct evidence rule in s. 60 beyond the extent to which its provisions have been diluted by s. 32(b) in the case of documents made in the ordinary course of business. A situation could thus arise under s. 90A(1) where the particular person who keyed in the information may not be individually identifiable, but the document would nevertheless be admissible.'

Shaik Daud Ismail JCA further clarified that there were two ways of proving 'in the course of its ordinary use':

'(i) it *may* be proved by the production of the certificate as required by sub-s.(2). – This is permissive and not mandatory. This can also be seen in sub-s.(4) which begins with the words '*Where*' a certificate is given under sub-s.(2)..... or

(ii) by calling the maker of the document. Therefore a certificate is not required to be produced in every case.

Once the prosecution adduces evidence through a bank officer that the document is produced by a computer, it is not incumbent upon them to also produce a certificate under sub-s.(2) as sub-s.(6) provides that a document produced by a computer shall be deemed to be produced by the computer in the course of its ordinary use.'

However, despite the clarification from the Court of Appeal in *Gnanasegaran*, these issues continued to arise as a means of challenging the admissibility of computer generated evidence. In *PB Securities S/B v Justin Ong Kian Kuok & Anor* KL HC [2007] 1 MLJ 153, the plaintiff's claim against the defendant was in respect of contra losses incurred in the defendant's share trading account arising from the purchase and sale of shares. The defendant contended that he did not give instructions to the remisier of the plaintiff's company to conduct the trading for and on his behalf which resulted in losses in the defendant's account, and that the trading was manipulated by the remisier. The defendant also alleged that numerous transactions were carried out far in excess of the trading limit. It was noted that the defendant did not challenge them nor lodge a complaint to the plaintiff regarding his account at the material time. The plaintiff furnished the certificate under s 90A of the Evidence Act 1950, and by virtue of s 90A, all the contract notes, contra statements and monthly statements were held to be properly admissible as evidence of the facts stated therein, namely, what shares had been bought and sold by the order of the defendant.

It is noted with concern that the mere production of the certificate was sufficient to admit all the contract notes, contra statements and monthly statements as proof of their contents without any concern about authenticity, particularly when the defendant disputes the authenticity. It should be necessary to examine the monthly statements and dispute any discrepancies immediately. However, it is interesting to note that in the American case of In *re Vee Vinhnee, debtor, American Express Travel Related Services Co. Inc. v Vee Vinhnee*, 336 B.R. 437 (9th. Cir. BAP 2005), American Express claimed that Vinhnee failed to pay credit card debts. The court found that American Express had failed to authenticate certain digital records. Klien J pointed out that the focus was not the circumstances of the creation of the records, but the preservation of the record, so as to assure that the document being proffered was the same as the document that was originally created. He explained that:

'.....the questions extend beyond the identification of the particular computer equipment and programmes used. The entity's policies and procedures for the use of the equipment, programmes and database are important. How access is controlled, how changes in the database are logged or recorded as well as the structure and implementation of the back-up systems and audit procedures for the continuing integrity of the database are pertinent ... to whether records have been changed since their creation.'[4]

In *PP v Hanafi Mat Hassan* [2003] 6 CLJ 459, the Court of Appeal embarked on a detailed examination of the provisions of s 90A, highlighting and carefully explaining the subtle requirements and distinctions. The question arose whether an automated bus ticketing machine, a thermalcycler and a DNA analyser were 'computers' and consequently whether the bus ticket produced by the automated ticketing machine and the DNA analysis laboratory reports were 'computer generated documents'. The accused, Hanafi bin Mat Hassan, was charged with

4 *For a comprehensive discussion on the tests for authenticity, see Stephen Mason, general editor, Electronic Evidence, Chapter 4.*

rape and murder. A bus ticket bought by the accused, which was produced by a ticket machine, was adduced by the prosecution. Its production was objected to by the defence counsel as being computer generated evidence. The High Court adopted the Court of Appeal's decision in *Gnanasegaran*, and held that the ticket machines installed on the buses were computers. Prosecution witnesses were called to give evidence to the effect that the ticket machines recorded and stored information and produced tickets, status reports, shift reports, and audit reports. Thus they were 'devices for recording, storing, and producing information' and the ticket, as well as the information printed on it, was admissible as evidence. On appeal, the defence contended that the tickets, as well as the DNA profiling laboratory reports, were inadmissible because both were 'computer generated documents' and therefore required a certificate under s 90A(2). The Court of Appeal took great pains to clarify the provisions of s 90A, in particular that the subsections under s 90A could not be read disjunctively but had to be read together. It stated that:

> 'a careful perusal of s.90A(1) reveals that in order for a document produced by a computer to be admitted in evidence it must have been produced by the computer "in the course of its ordinary use". It is therefore a condition precedent to be established before such a document can be admitted in evidence under s.90A(1). The manner of establishing this condition has been prescribed. It can be proved by tendering in evidence a certificate as stipulated by s.90A(2) read with s.90A(3). Once the certificate is tendered in evidence the presumption contained in s.90A(4) is activated to establish that the computer referred to in the certificate was in good working order and was operating properly in all respects throughout the material part of the period during which the document was produced. Section 90A(4) must therefore be given its full effect as it has a significant role to play in the interpretation and application of s.90A. Ordinarily a certificate under s.90A(2) must be tendered in evidence in order to rely on the provisions of s.90A(3) and (4). However, the use of the words "may be proved" in s.90A(2) indicates that the tendering of a certificate is not a mandatory requirement in all cases. Thus the use of the certificate can be substituted with oral evidence as demonstrated in *R v. Shepherd* [1993] 1 All ER 225 in dealing with a provision of law similar to s.90A. It follows that where oral evidence is adduced to establish the requirements of s.90A(1) in lieu of the certificate the presumptions attached to it, in particular, the matters presumed under s.90A(4) must also be proved by oral evidence. ... The resultant matter for consideration is the proper meaning to be ascribed to the "deeming" provision in s.90A(6) in order to determine whether it can be a substitute for the certificate. A deeming provision is a legal fiction and is used to create an artificial construction of a word or phrase in a statute that would not otherwise prevail. ... Its primary function is to bring in something which would otherwise be excluded ... the purpose of tendering in evidence a certificate under s.90A(2) is to establish that a document was produced by a computer in the ordinary course of its use. On the other hand s.90A(6) deems a document produced by a computer to have been produced by the computer in the course of its ordinary use. They are incompatible and inconsistent with each other. Every effort must thus be made to reconcile both the sub-sections in order to avoid a conflict between them.... S.90A(6) must have some other purpose to serve. S.90A(6) 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 s.90A(1).'

The members of the Court of Appeal held that the ticket from the automated ticketing machine was a 'computer generated document'. It was correctly admitted into evidence, although the trial judge failed to appreciate the need for oral evidence to satisfy sub-section (4). However, the oral evidence of prosecution witness 25 (PW25) had been sufficient to prove the proper working of the ticketing machine, and that it was produced in its 'ordinary course', thus satisfying both section 90A(1) and sub-section (4).

On the issue of the DNA laboratory report, these were documents produced by DNA analysers and a thermalcycler. These were found to be 'computers' within the meaning of the definition of 'computer' in s 3 of the Evidence Act 1950. Exhibit P17 involved more than one computer in its production. The question arose whether all the computers were involved or only one of them and, if so, which one must be proved for the purposes of s 90A.

Section 3 provides that where two or more computers carry out the function of recording, storing, processing, retrieving or producing any information, as in this case, they are treated as a single computer. Considering the requisite proof, the Court of Appeal held that what was relevant for the prosecution was not the document produced by the computer (exhibit P17), but the statements contained in it. The distinction is recognised by s 90A. The Court of Appeal thus pointed out that what was required to be established in order to comply with s 90A was the condition of the computers that produced the results as contained in exhibit P17, and not the computer itself which produced exhibit P17. In the absence of a certificate having been tendered in evidence under s 90A(2), the oral evidence of prosecution witness 11 (PW11) was found to be sufficient to establish the condition precedent contained in s 90A(1). However, there had to be further oral evidence in lieu of the presumptions attached to a certificate to satisfy s 90A(4) that the computer was in good working order, and that it was operating properly in all respects throughout the material part of the period during which the document was produced. Although the prosecution did not lead any evidence in proof of these matters, the Court of Appeal found that the cross-examination of PW11 by the defence had put on record the required evidence. The conviction of the appellant was upheld.

In *PP v Goh Hoe Cheong & Anor* [2007] 7 CLJ 68, the admissibility of 'computer generated' baggage tags were successfully challenged by the defence. Two accused were charged under s 39B(1)(a) of the Dangerous Drugs Act 1952 for trafficking, which is punishable with death under s 39B(2). Here, the issue was the continuity of the chain of evidence. The prosecution unsuccessfully sought to adduce electronically produced check-in baggage tags in evidence. The facts were that, based on information received, a team of police personnel planned to capture three suspects when they were about to board their flight at Kuala Lumpur International Airport (KLIA). At 9pm, the prosecution's witness, described as 'PW8', and his police team took their respective positions at KLIA. The suspects checked in their bags and had a blue ribbon tied to each of their baggage handles. They then left the check-in counter and proceeded to the departure gate for their flight at the Satellite Building. The police personnel followed but did not arrest them either before or after the three suspects had passed through Immigration and Passport Control, or stop them from boarding the aerotrain to proceed to the Satellite Building.

It was only when the bags of the three suspects arrived at the baggage assembly area, prior to loading on to the aeroplane at 10.35pm, that PW8 detained them and gathered them together in front of departure Gate C14. He then took them below the aerobridge to his team mates who were with the three bags. The men were subsequently brought to the Narcotics Department where a physical body examination and an examination of their belongings was conducted. A physical check of the accused revealed nothing. The baggage keys were obtained from the trouser pocket of the accused, and the bags were opened, searched, the interior lining cut and drugs found.

The issues before the court were whether there was admissible evidence before the court, and whether the prosecution had adduced prima facie evidence that the accused had custody and control of the bags. The court found the following:

(1) The police had allowed the suspects to board the aerotrain to proceed to the departure gate to board their scheduled flight without a hint of any imminent arrest. In the meantime, PW8 had left his position at the vicinity of the check-in counter E14 and proceeded to departure Gate C14 Satellite Building KLIA. He did not seize the bags of the suspects from the airport personnel who processed the check-in, at the check-in counter itself.

(2) There was no evidence given by the authority responsible for the management of the airport or the air carrier concerned, giving rise to serious doubts whether the exhibit bags were in fact the same bags checked in at counter E14 by the accused, notwithstanding the carrier's baggage tags were found attached to the bags, and the baggage claim tags attached to the respective tickets of the first and second accused, found in their possession. In fact and in law, in the absence of any express provisions as soon as a passenger checks in his bag at the check-in counter for his scheduled flight, the bag was in the custody and control of the carrier or its agents, until the same is claimed by the passenger, and the bag thereupon

delivered to the passenger.

(3) There was no evidence that the packages suspected of containing drugs found in the bags had been concealed by the accused, since there was no fingerprints of either of the accused on any of the packages, and no witness from the carrier or the authority managing KLIA called by the prosecution to prove the physical checking-in of the bags by the first and second accused. Therefore, the computer generated documents i.e. the baggage tags P6A, P23A and the respective baggage claim tags P16A and P31A, could not be admitted in evidence unless s 90A of the Evidence Act 1950 was complied with by the prosecution.

(4) No certificate was tendered to the court signed by a person who either before or after the production of the documents by the computer was responsible for the management of the operation of that computer, or for the conduct of the activities for which that computer was used.

In the circumstances, the baggage tags were inadmissible as evidence. Therefore, there was no admissible evidence before this court. As the chain of custody and control had not been established, there was no admissible evidence that the bags were in the custody and control of the accused, either at the time they were arrested by PW8 at the departure Gate C14, or at any time before the bags were checked-in.

In *Ahmad Najib A ris v PP* [2009] 2 CLJ 800, the Federal Court dealt with the vexing issue of the distinction between s 90A subsections (1) and (6). The issue arose as to whether CCTV audio video recordings were documents produced by a computer, and if so the manner of proving, and whether a presumption arose under s 90A(6) as to whether a computer was used in its 'ordinary course'. The appellant was convicted of rape and murder in the High Court. For the offence of rape, he was sentenced to 20 years' imprisonment and to 20 strokes of the cane. In respect of the murder, he was sentenced to death. On appeal the Court of Appeal maintained the High Court's convictions and sentences.

The appellant appealed further to the Federal Court on various grounds, amongst others the admissibility of documents produced by a computer pursuant to s 90A of the Evidence Act 1950 being of interest here. On the question of admissibility of 'computer generated documents', the Federal Court adopted the decisions in *Gnansegaran*, and *Hanafi Mat Hassan*. The Federal Court first addressed the issue of whether the CCTV recordings were 'documents' produced by a 'computer'. They found that a CCTV tape clearly falls within the definitions of 'document' under s 3 of the Evidence Act 1950 which includes 'disc, tape, film, sound track and any visual recording whether of still or moving images' and others. A 'computer' is defined in the same section as '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'. It therefore meant that the CCTV tapes (P19A-D) must satisfy the requirements of s 90A Evidence Act 1950 before they can be admitted in evidence. As this had not been done, they were inadmissible.

The Federal Court then went on to examine the distinction between the provisions under s 90A(1) and the presumption set out in s 90A(6). Section 90A(1) deals with the admissibility of a document which was produced by a computer in the course of its ordinary use. However, s 90A(6) of the Evidence Act 1950 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. The question then arises whether the presumption in s 90A(6) can be a substitute for the strict requirements of s 90A(1).

Under s 90A(1), there is a condition precedent that in order for a document produced by a computer to be admitted in evidence, it must have been produced by the computer 'in the course of its ordinary use'. This can be proven by tendering in evidence a certificate as stipulated by s 90A(2) read in conjunction with s 96A(3). Once the certificate is tendered in evidence, the presumption contained in s 90A(4) is activated to establish that the computer referred to in the certificate was in good working order and was operating properly. However, the use of the words 'may be proved' in s 90A(2) indicates that the tendering of a certificate is not a mandatory requirement in all cases, and can be substituted with oral evidence, as clarified in *Gnanasegaran*, following the English case of *R v Shepherd*. In such event, the matters presumed under s 90A(4) must also be proved by oral evidence.

On the other hand, s 90A(6) 'deems' a document produced by a computer to have been produced by the computer 'in the course of its ordinary use'. The Federal Court held that a fact cannot be 'deemed' to have been proved when specific provision has been made for the

mode of proof of the same fact. The correct interpretation has to be that s 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. Therefore the presumption contained in s 90A(6) can only be resorted to when the document was *not* produced by a computer 'in the course of its ordinary use'. This could arise for instance where a letter is produced by the computer which has no bearing on the ordinary use of the computer. Yet it is still a document produced by a computer and could be admissible under s90A(6).

In this case, no certificate was tendered as required by s 90A(2) for proof of the chemist report (P83). Neither was any oral evidence adduced to show that the report was produced by a computer in the course of its ordinary use. It therefore remains that the only evidence available is that the report was produced by a computer. The oral evidence of prosecution witness 27(PW27) in cross examination is relevant, because he categorically stated that he could attest to the 'computer's ordinary use' and its 'proper working condition'. The contents of the chemist report (P83) directly established the appellant's commission of the offence of rape and murder of the deceased. The linking evidence were DNA tests conducted on blood stains on a pair of jeans found in the appellant's house as well as blood stains in the car driven by the appellant, both of which established the blood as the appellant's. Vaginal swabs taken from the deceased during autopsy also established the semen as the appellant's, and DNA tests on six strands of hair found in the car driven by the appellant also confirmed it to be that of the deceased. On this basis, the appellants earlier conviction was confirmed.

In *Lau Chee Kai v PP* [2011] 9 CLJ 619, the question arose as to whether the serial numbers of money that were keyed into a computer satisfied the requirements of s 90A of the Evidence Act 1950. The accused appealed against conviction under s 5 of the Kidnapping Act 1961 for kidnapping one Seow Wei Sheng, a seven year old minor (the victim). Ransom money of Ringgit Malaysia (RM) 5 million was paid in Malaysian, Singapore and Brunei currencies by the victim's father, prosecution witness 9 (PW9). The notes had been photocopied and handed to the police. PW9 testified that the Malaysian Ringgit were in RM50 and RM100 denominations, while the Singapore Dollars were in $50, $100 and $1,000 denominations. He was unsure of the Brunei Dollar. He did not record the serial numbers of the notes. He also did not make any markings on the notes he photocopied. The photocopied copies of the notes were bound into five volumes which were produced by the prosecution as exhibits P12 (1-5). The accused was arrested while coming out of a bank in Petaling Jaya. Money was seized in various currencies – Malaysian Ringgit, Singapore Dollar, Hong Kong Dollar and Thailand Baht from the accused's master bedroom. The Singapore currency seized were, one hundred $50 notes and five $1000 notes totaling $10,000. The serial numbers of the notes were keyed into the computer by prosecution witness 16 (PW16). This was printed and tendered by the prosecution as exhibit P71. According to PW16, the serial numbers of 60 of the 105 Singapore Dollar notes seized from the accused's master bedroom tallied with the serial numbers of some of the ransom money. The amount involved was $7,750. PW16 testified that only three fourths of the ransom money was photocopied. Her investigations revealed that $2.3 million in Singapore and Brunei Dollars and RM650,000 were paid as ransom money. The accused's wife testified that she had obtained the Singapore currency from a money changer to be used for the treatment of the accused's father in Singapore, who was suffering from a lung illness. One of the issues before the Court of Appeal was whether the Singapore currencies seized from the accused's house were part of the ransom money. PW16 had not compared the money seized with exhibit P12 (1-5), but with exhibit P71 to find out whether the seized money was part of the ransom money.

Counsel for the defence challenged the admissibility of exhibit P71 (being a computer print-out) under s 90A of Evidence Act 1950 on the grounds that first, the serial numbers of the money found in exhibit P12 (1-5) were keyed in into the computer by PW16 and one Inspector Salwani over a period of two months. Only PW16 gave evidence. Inspector Salwani was not called to give evidence. Second, since the prosecution had not tendered a certificate under s 90A(2) of the Evidence Act 1950, it had not proved that the computer used by PW16 and Inspector Salwani was in the course of its ordinary use. The Court of Appeal considered the earlier cases of *Gnanasegaran, Hanafi Mat Hassan v PP*, as well as the Federal Court's decision in *Ahmad Najib A ris v PP*, and held exhibit P71 to be admissible under s 90A. They found that PW16 had testified that exhibit P71 was a document produced by a computer and that she and Inspector Salwani had keyed in the data into the computer. Although the prosecution had not tendered a certificate under s 90A(2) of the Evidence Act and PW16 did not say whether exhibit P71 was produced by a computer in the

course of its ordinary use, the prosecution, in view of the authorities cited earlier, could resort to the presumption under s 90A(6), which provides that a document produced by a computer shall be deemed to be produced by the computer in the course of its ordinary use. However, the appeal was successful and the conviction set aside on a different ground, and that it was unclear whether the learned trial judge had adequately evaluated the evidence adduced by the defence, because he had not given any reasons for rejecting it.

In *Navi & Map Sdn. Bhd.v Twincie Sdn. Bhd. & Ors* [2011] 7 CLJ 764, the certificate produced pursuant to s 90A Evidence Act 1950 was challenged. The plaintiff claimed copyright infringement over a set of compiled and published map data both in print and digital format entitled the '5th Edition, Street Directory of Kuala Lumpur and Klang Valley'. It claimed that the defendants, without its consent and authority, had substantially reproduced, manufactured and or sold the map data and the related digital maps to the public – particularly the seventh defendant, Navteq North America LLC. The seventh defendant was not named in the suit. The plaintiff obtained an ex parte Anton Pillar orders against the first to sixth defendants and confiscated copies of all documents, image digital maps and computer copy files in computers, laptop computers, a server and screen shots of a File Transfer Protocol server from the first defendant's premises. The seventh defendant, who was not named in the suit, voluntarily subjected itself to intervene in the suit and counter claimed for injunctive relief, declaratory order, damages and costs against the plaintiff for copyright infringement of its copyright protected works seized from the first defendant's premises. The fifth defendant also counter claimed against the plaintiff for constructively dismissing her. In its claim for infringement of its copyright, the plaintiff in its claim relied on the following:

(i) Schedule 1 was the statutory declaration sworn by the plaintiff's former director and chief operating officer, Mr Owatari Hideo ('PW5') pursuant to s 42 of the Copyright Act 1987;

(ii) Schedule 2 was a list of employees listing their names, jobs done, dates of completion and commencement for the creation of the copyrighted material; and

(iii) Schedule 3 contained names, National Registration Identity Card numbers, job responsibilities for map number and map reference, date of commencement and completion.

The plaintiff failed in its copyright infringement claim, because there was no prima facie evidence to show that the plaintiff was the copyright owner of the work. In the declaration sworn, PW5 said that the maps and data were completed by certain personnel. However, the plaintiff failed to exhibit the actual work carried out by these personnel and, thus, the declaration sworn was defective and did not comply with s 42(1)(a) of the Act.

The plaintiff tendered a 'skype chat' between the defendant witnesses as evidence of copyright infringement. The plaintiff produced a certificate ('exhibit P29') pursuant to s 90A E A1950 for admission of the print-out of the chat, duly signed by a digital evidence specialist from the Digital Forensic Department in Cyber Security ('PW4'). However, exhibit P29 was not a valid certificate under s 90A, due to the fact that it certified that PW4 was not the officer responsible for the management and analysis process of the computer that produced the skype chats. Furthermore, the certificate did not certify that the document was produced in the course of its ordinary use or that it was in good working order. It was also evidenced that portions of the skype chat were missing. For these reasons, the evidence of the skype chat did not aid the plaintiff in proving copyright infringement. The plaintiff failed to prove that the defendants had infringed the copyright, and the court dismissed the plaintiff's application against all defendants with costs; dismissed the fifth defendant's counter claim against plaintiff with costs; but allowed the seventh defendant's counter claim against plaintiff with costs.

New developments

On 2 February 2012, further amendments were introduced to the Evidence Act by way of section 73AA and sections 90D, 90E and 90F under the Evidence (Amendment)(No.1) Act 2012. Although these amendments do not specifically refer to computer evidence, it would operate to include computer evidence. These amendments are aimed to compliment the Mutual Assistance in Criminal Matters Act 2002. Section 73AA provides for a pre-trial agreement in writing between the parties agreeing to the admission of specified evidence. Where such agreement is signed, no proof of such evidence shall be required. This therefore operates as an opt-in proviso ensuring that the evidence

will not be challenged. The amendments under section 90D facilitate the admission in criminal proceedings of evidence obtained under the Mutual Assistance in Criminal Matters Act 2002 without further proof of any fact stated in the testimony albeit with certain safeguards. Section 90D(2) stipulates that the testimony, statement or deposition shall be taken on oath or affirmation, under an obligation to tell the truth or under caution as would be accepted, by courts in the foreign country concerned, for the purposes of giving testimony in proceedings before those courts.

Subsection (3) requires authentication of such evidence by being signed or certified by a judge, magistrate or officer in or of the foreign country to which the request was made; and bear an official or public seal of the foreign country or department. Subsection (4) provides that such certificate pursuant to subsection (3) shall be admitted in the proceedings as conclusive evidence of the facts contained in the certificate, and subsection (5) provides that judicial notice shall be taken of it. Once again, these provisions are designed to ensure that the evidence cannot be challenged by the defence. Subsection (6) provides that the testimony taken under subsection (2) may be reduced to writing or be recorded on a tape, disk or other device from which sounds or images are capable of being reproduced or may be taken by means of technology that permits the virtual presence of the person in Malaysia. Subsection (7) requires such evidence under subsection (6) to be authenticated as provided under subsection (3). Subsection (8) deems such video or testimony by other means which permits the virtual presence of the person in Malaysia, to have been given in Malaysia. This would facilitate the admission of teleconferencing or video conferencing testimony, as in the 2010 test case of a 16-year-old rape victim who was allowed to testify via live 'video link' in a Sessions Court. On an appeal on the point, the High Court held that the video link did not amount to 'recorded evidence' as it was a 'live' video link.[5] Subsection (9) clarifies that the testimony, statement or deposition need not be in the form of an affidavit; or constitute a transcript of a proceeding in a foreign court. Finally, subsection (10) ensures the admissibility of such evidence, and provides that the court has no discretion to exclude it. In relation to evidence from foreign jurisdictions, s 90F ensures its admissibility, provided it is tendered with a certificate of authorisation from the Attorney General.

A new section, s 114A, in the Evidence (Amendment) (No.2) Act 2012[6] has introduced a presumption of fact applicable in both civil and criminal proceedings in respect of publication through the internet. In order to facilitate the identification and proving of the identity of an anonymous person involved in publication through the internet subsection (1) provides that:

> (1) A person whose name, photograph or pseudonym appears on any publication depicting himself as the owner, host, administrator, editor or sub-editor, or who in any manner facilitates to publish or re-publish the publication is presumed to have published or re-published the contents of the publication unless the contrary is proved.

This means if X creates a blog in Ys name, or posts something 'offensive' or 'sensitive' on Y's web page or social network site, Y is deemed to have published it. Victims of hacking and identity theft would have to bear the evidential burden of proving otherwise.

Subsection (2) provides:

> (2) A person who is registered with a network service provider as a subscriber of a network service on which any publication originates from is presumed to be the person who published or re-published the publication unless the contrary is proved.

The provisions of this subsection has grave consequences. If a posting is found to originate from Y's account with a network service provider, Y is deemed to be the publisher unless Y is able to prove otherwise. Thus people sharing an internet account, or giving access to third parties had better beware, because the account holder will be held liable unless the contrary can be proved.

Subsection (3) provides:

> (3) Any person who has in his custody or control any computer on which any publication originates from is presumed to have published or re-published the content of the publication unless the contrary is proved.

Here again if a publication is traced to a computer either owned by or over which Y had custody and control, Y will be deemed to be the publisher of any material found on it unless Y can prove otherwise.

5 *Yuen Mei Keng, ' Rape trial: Testimony via video link okayed' , The Star, 4 February 2010.*

6 *Date of Royal Assent: 18 June 2012; date of publication in the Gazette: 22 June 2012; date of coming into force: 31 July 2012 [PU(B) 255/2012].*

Subsection (4) further provides that for the purpose of this section:

(a) "network service" and "network service provider" have the meaning assigned to them in section 6 of the Communications and Multimedia Act 1998 [Act 588]; and

(b) "publication" means a statement or a representation, whether in written, printed, pictorial, film, graphical, acoustic or other form displayed on the screen of a computer".

The section which clearly favours the prosecutor, and has caused great public anxiety, especially among social network users. The rational for the amendment was that it was difficult to trace the source of an anonymous postings because even though there was an aggrieved party, no cause of action could be pursued, as there was no evident publisher of the content. This is not necessarily so, because there are procedural means for obtaining the necessary information.

For instance, in *Stemlife Bhd. v Bristol-Myers Squibb (M) Sdn Bhd* [2008] 6 CLJ, the plaintiff applied for pre-action discovery against the defendant for defamatory postings on the defendant's web site and in an external blog linked to the defendant's web forum by two users of the forum operating under the pseudonyms 'stemlie' and 'kakalily'. The plaintiff sought a *Norwich Pharmacal*[6] order against the defendants for the identity of the users, and contended that the defendant should have the relevant information, because the users were registered with the defendant and would have provided their particulars upon registration. In granting the order sought, the High Court explained that the question before the court was not whether the defendant was liable for the same wrong against the plaintiff as that committed by the users with the pseudonyms 'stemlie' and 'kakalily', but whether the defendant facilitated their wrongdoing. There was evidence that the defendant's web site contained terms and conditions that reserved the defendant's editorial rights to edit or completely remove postings on the web site at its sole discretion without prior notice or explanation. Hence, it was found that the defendant, by providing and controlling the web site that enabled defamatory materials or hyperlinks to be posted freely with no editorial editing, clearly facilitated the wrongdoing.

With the operation of section 114, a plaintiff in a similar situation could now directly seek redress against the web site hosts. The onus would be on the defendants to use their resources to identify the bloggers of the offensive postings and join them in the proceedings and prove that they are not the publishers.

Conclusion

The provisions of s 90A Evidence Act 1950 have clearly facilitated the use of 'computer generated evidence' in the Malaysian courts. However, despite the recent amendments to the Evidence Act in 2012, it is noted that the legislature has not seen the need to amend the 'computer' specific language of the statute to the more neutral term of 'electronic' or 'digital'. As such questions of whether 'documents' from a particular equipment are 'computer generated' will continue to arise. The two major issues that arose in practice being whether a 'certificate' under subsection (2) had to be mandatorily produced in every case, and whether subsection (6) could be used to circumvent the provisions of subsection (1) have been clearly addressed by the courts.

However, equally clearly, the distinction between authenticity and admissibility has not been appreciated by the courts or by the lawyers who try to challenge the admissibility of certain 'computer generated documents'. Meanwhile, the latest amendments to the Evidence Act 1950 have far reaching consequences, because it is weighed heavily in favour of the prosecution, making the challenging of the evidence virtually impossible. It would be better if an opt-in provision similar to s 73AA could be introduced for all actions, whether civil or criminal, providing for a pre-trial agreement in writing between the parties agreeing to the admission of specified evidence at the trial.

Gita Radhakrishna, is a lecturer at the Faculty of Business & Law, Multimedia University (Melaka campus), Malaysia. She is currently undertaking her PhD research on 'The admissibility of electronic evidence in the Malaysian Courts'.

gita@mmu.edu.my

6 *Norwich Pharmacal Co v Commissioners of Customs & Excise [1974] AC 133, [1973] 2 All ER 943, [1973] 3 WLR 164, HL.*